

Confidencialidad e informatización en la Sanidad

ISABEL M^o PORTERO SÁNCHEZ
Hospital Universitario Marqués de
Valdecilla (Santander)

Dentro del campo sanitario existen, como no podía ser menos, multitud de temas que pueden llamar la atención de quien se encuentra inmerso en él. Sin duda los estrictamente clínicos ocupan el lugar preferente; pero junto a ellos, en ocasiones nos salen al encuentro algunos otros que tampoco podemos ni debemos despreciar, dada la importancia práctica que pueden adquirir en determinados momentos. Uno de estos es el de la relación que puede darse entre la confidencialidad propia de la profesión sanitaria y la aplicación de la ciencia informática en el mundo de la sanidad.

En efecto, los últimos años del presente siglo nos están confirmando numerosos avances tecnológicos con repercusión en no pocas áreas de conocimiento; no sin razón el filósofo Bilbeny¹ nos habla de una «revolución cognitiva» refiriéndose preferentemente a las ciencias tecnológico-científicas, y cómo la prueba de ello podemos verla en el paso de los medios de comunicación escritos y el nuevo hacer que supuso la radio, luego la televisión y finalmente el ordenador.

Y tal dato, que conlleva en sí la carga de algo altamente positivo, encierra igualmente sus riesgos. Se avanza mucho, nos sentimos miembros de una sociedad preparada e inteligente pero, al

mismo tiempo, contemplamos cómo se pierde sensibilidad frente a muchos problemas humanos. En concreto la posibilidad de acumular informaciones y datos en cantidades casi ilimitadas, de relacionarlas y repetir las cuantas veces sea necesario, nos conduce ante un nuevo poder social sobre el individuo, el poder informático, y al tiempo en que todo esto se produce, deviene igualmente una clara necesidad de controlar ciertos datos para proteger la intimidad de las personas.

No es de extrañar por tanto que ya hace casi un siglo apareciera en el mundo jurídico una nueva exigencia que se conoció con la expresión inglesa «right privacy», que poco a poco ha ido recibiendo refrendo legal y jurisprudencial prácticamente en todos los países civilizados².

Conviene afirmar, no obstante, que el tratamiento de datos personales por parte de los médicos se ha realizado prácticamente desde siempre; lo que ocurre es que actualmente se ve incrementado por el aumento de población, los servicios, y el cambio instrumental experimentado mediante el cual se lleva a efecto el procesamiento de los mismos. Así, hoy no se habla ya de tratamientos manuales o mecánicos de datos, sino más bien de tratamientos elec-

¹ Norbert Bilbeny. *La revolución en la ética. Anagrama. Barcelona 1997* pp. 13-17

² Esta expresión apareció como título en un artículo publicado en 1891 por Samuel D. Warren y Louis D. Brandeis en la «Harvard Law Review». En la intención de ambos autores parece que venía a ser algo equivalente a «to be let alone», derecho a permanecer al margen de intromisiones provenientes de la esfera pública y privada. Posteriormente la jurisprudencia de EE.UU. fue perfilando este derecho, e incluso llegó a plasmarse en la Declaración Universal de Derechos Humanos (art. 12) cuando declara prohibida toda «arbitrary interference with privacy». Sobre todo ello puede verse F. Rigaux. *L'elaboration "un right to privacy par la jurisprudence americane en «Revue internationale du droit comparé» 33 (1980) pp. 701-730.*

³ Puede verse sobre esto Corbella y Corbella J. *La responsabilitat del metge e des les institucions sanitàries* Discurso de ingreso en la Real Academia de Medicina de Barcelona, Barcelona 1986 pp. 45 y ss. El autor considera que la responsabilidad en el ámbito de la sanidad puede darse actualmente a 3 niveles: del médico en cuanto tal, de las instituciones sanitarias, y de la Administración de Sanidad.

⁴ La Ley General de Sanidad, de 14 de abril de 1986, desarrolla el tema del secreto profesional y la confidencialidad de la información en sus arts. 10 y 61. Cabe igualmente recordar lo dispuesto en el Código de Deontología Médica, aprobado en Londres en 1949, (arts. 43, 45 y 50) donde se señala que el secreto «cubre todo lo que llegue a conocimiento del médico en el ejercicio de su profesión, no solo lo que se le confie, sino también lo que haya podido oír o comprender... El médico debe de proteger contra toda indiscreción las fichas personales y cuantos documentos pueda conservar en relación con el enfermo».

⁵ No solo en determinados servicios específicos, como por ejemplo puede ser el de Psiquiatría, sino también en otros no estrictamente clínicos, donde los expertos informáticos, asistentes sociales etc. pueden tener alguna misión.

trónicos u automatizados que nos permite procesar informáticamente ingentes cantidades de ellos, obtener copias o enviarlas a remotos lugares, transmitir ficheros completos etc. En suma, estamos capacitados técnicamente para poder recibir y transmitir un cúmulo de información sobre cada uno de nosotros, como si de una radiografía se tratase, y de esta manera nuestro iter vital puede ser facilitado y analizado sin problemas.

Nada pues de extraordinario que desde fines de los años 50 se apliquen en el campo sanitario los modernos métodos informáticos, por las ventajas que en la práctica pueden proporcionar al personal médico y en la gestión hospitalaria, aunque la «eficacia» no sea el único criterio a tomar en cuenta, sino también la utilidad que supone su facilidad de empleo.

Así pues el ejercicio de la actividad sanitaria se ve sometido actualmente a cambios técnicos y estructurales que no podemos desconocer. Entre otras razones porque con ellos cabe incidir en el campo de la responsabilidad del personal sanitario, transformando los principios que tradicionalmente venían aplicándose en este tema³.

Ante tal situación el Derecho no solo trata de conseguir el carácter reservado para los datos que figuren en los archivos o bancos informáticos, sino también de regular cómo se consiguen y bajo qué supuestos pueden ser utilizados. De ahí que han surgido en muchos países instituciones públicas encargadas de velar porque se cumplan esta finalidad de confidencialidad: en ocasiones es un órgano administrativo especial con funciones ejecutivas (España, Francia, Austria), o bien personal que pueden asumir un papel de inspección o vigilancia (Noruega), o se trata de entidades con funciones meramente consultivas (Alemania, Canadá, Luxemburgo).

Al propio tiempo, teniendo en cuenta que es importante el «saber», el «saber ser» y el «saber hacer», los códigos éticos intentan de alguna forma limitar

posibles consecuencias perjudiciales para los usuarios; buscan evitar que las diversas profesiones se consoliden simplemente como plataformas de status, e intentan que el secreto profesional, la solidaridad, la inexistencia de prejuicios, las intervenciones realistas actúen como fundamento o base para mantener la dignidad de las diversas profesiones, y, dentro de ellas, una muy importante es la sanitaria.

En esta línea intentamos centrarnos al tratar de las confidencialidad de los datos referidos a pacientes y su tratamiento informático⁴.

LA ATENCIÓN A LA SALUD Y SU REFERENCIA EN ARCHIVOS Y BANCOS DE DATOS

Todos somos conscientes que en el campo sanitario se ha venido produciendo de un tiempo a esta parte una evolución que podríamos considerarla desde un enfoque puramente médico a otro más amplio, multidisciplinar, en el que pueden intervenir expertos en otras ciencias ajenas a las estrictas de la salud⁵. Conocemos igualmente que una labor sanitaria seriamente llevada a cabo, de manera especial en los grandes centros hospitalarios, implica un cúmulo enorme de información que puede ser utilizado no solo con fines estrictamente terapéuticos, en el puro sentido del término, sino también para otras facetas como podrían ser, por ejemplo, la investigación, y la estadística.

El tema pues de los datos socio-sanitarios parece importante de tratar, no solo por la enorme cantidad de los mismos, sino ante los riesgos que pueden sobrevenir por su utilización. Se trata de datos de los denominados «sensibles» en el sentido de tener en cuenta no solo el contexto en que se utilizan, sino también el contenido de los mismos, que puede en determinados casos (así se hace constar en el núm. 43 de la Memoria Explicativa del Convenio del Consejo de Europa de

1981) perjudicar a los derechos e intereses de los individuos. Queda pues claro que aunque la «sensibilidad» como condición no puede aplicarse a todos los datos sobre personas, sí que puede ser referida a algunos de ellos⁶.

Sobre la enorme cantidad de datos sanitarios que normalmente se emplean baste constatar los millares de historias clínicas, de diagnósticos, tratamientos, ingresos, altas y bajas, y otros tipos utilizados. Referente a posibles riesgos podemos intuirlo con solo pensar en la inclusión de dichos datos en los archivos o servicios informatizados centralizados, el acceso a los mismos, su utilización y cambio, y las filtraciones que pueden teóricamente darse en ese camino.

Parece por tanto conveniente flexibilizar acerca de las perspectivas sanitarias y jurídicas en el mundo del tratamiento automatizado de datos, máxime cuando vemos la creciente interconexión de las diversas unidades operativas que pueden intercambiar información a fin de poder suministrar prestaciones sanitarias con la mayor eficacia posible. Meditemos, a manera de ejemplo, en el flujo informático que puede darse entre un médico de asistencia extrahospitalaria con un gran centro sanitario; o entre los diferentes servicios actuantes en un hospital, considerando como tal, de acuerdo a la Ley de Coordinación Hospitalaria de 21 de julio de 1962 (art.1) «los establecimientos destinados a proporcionar una asistencia médico-clínica sin perjuicio de que pueda realizarse en ellos, además, en la medida en que se estime conveniente, medicina preventiva y de recuperación y tratamiento ambulatorio».

Es más, no faltan universidades que ya incluyen entre las disciplinas de los planes de estudios médicos el operar con la informática en cuestiones de salud. La Universidad Rene Descartes figura en Europa entre las pioneras, como antes lo había sido en los Estados Unidos la de Illinois que lo había implantado desde 1974. Y si hablamos de nuestro

país, la Agencia de Protección de Datos, en su Memoria correspondiente a 1995, reconoce que «los datos personales relativos a la salud son ya sometidos a tratamiento automatizado de modo generalizado y en gran escala, como consecuencia de la extensión sanitaria a toda la población y del valioso papel de la informática en su gestión»⁷.

LOS DATOS EN LA RELACIÓN MÉDICO-PACIENTE

Entre los pacientes y profesionales de la salud, y me refiero en concreto al médico en una perspectiva hacia el enfermo, ha de producirse necesariamente una relación de la que se derivarán una serie de datos que normalmente constarán en la historia clínica del mismo. Las reglas por las que ha de regirse este cúmulo de información son variadas, aunque frecuentemente se atienen a estos principios: interrogatorio sobre problemas biomédicos; entorno familiar, ocupacional y comunitario del paciente; valores y visión del mundo que tiene etc.

Una vez obtenida dicha información puede pasarse a lo que la doctrina suele denominar «consentimiento informado», es decir, el paciente tiene derecho a conocer con precisión su diagnóstico, tratamiento, posibles riesgos y probabilidades de éxito, derivaciones que caben a otros servicios etc. Este conocimiento informado que como sabemos aparece en la década de los cincuenta como algo corriente en el protocolo sanitario⁸ debería enmarcarse en un contexto adecuado tanto con el propio paciente como cuando haya de darse por los familiares. El médico debe mostrar que acepta bien que se le formulen preguntas adicionales, y el deseo de que sus respuestas sean claras y comprensibles, para que de esta manera el enfermo pueda en su momento tomar la decisión oportuna; no olvidemos que, como señala Haring⁹, no es infrecuente la existencia de informaciones incompletas o deformadas por diversas razones, como por ejemplo experimentos de los que no se quiere hablar, terapias especiales, o

⁶Un autor como Velázquez Bantista R. *Protección jurídica de datos personales automatizados*. Edit. Colex. Madrid 1993 pp. 26 y ss. establece 3 posibles categorías de datos referidos a las personas: 1) datos indiferentes 2) datos sensibles en relación con el contexto y 3) datos sensibles en sentido propio. Entre los primeros incluye nombre, apellidos, edad, sexo, domicilio, títulos académicos; entre los segundos los datos tributarios y sobre solvencia económica; y entre los terceros las opiniones políticas, religiosas, tendencias sexuales, origen racial etc.

⁷Madrid 1996 pg.89

⁸Se suele fijar el comienzo de los «consentimientos informados» en los Estados Unidos. Uno de los primeros casos fue tratado en *Salgo vs. Leland Stanford Jr. University Board of Trustees*, en 1957. Posteriormente siguieron otros como el *Natanson vs. Kline* en 1960 ts. Puede verse sobre esto Ruth R. Faden y Tom L. Beauchamp. *A history and theory of informed consent*. Oxford University Press. New York 1986.

⁹Bernard Haring. *Ética de la manipulación*. Herder. Barcelona 1985 pp. 28 y 148

¹⁰ Art. 10.5 donde habla al derecho a la información en términos comprensibles, de forma continuada, completa, verbal o escrita, sobre el proceso del paciente, incluyendo diagnóstico, pronóstico, alternativas terapéuticas etc. También el Real Decreto de 20 de enero de 1995 contempla el derecho del paciente incluso a que se le entregue copia de su historial clínico.

¹¹ El modelo legalista de la «hoja de consentimiento» ha sido criticado por buena parte de la doctrina. A manera de ejemplo Horward Brody. *The healers power*. Yale University Press. New Haven 1992.

¹² No faltan quienes critican que son las gentes más pobres y con menos formación los que menos preguntan. Las personas con estudios suelen a veces preguntar ¿si Vd. tuviera esta enfermedad, qué tratamiento elegiría?, o bien ¿qué haría en mi caso?. No faltan tampoco quienes dicen que los médicos pueden manipular al paciente, bastando simplemente con enfatizar determinados puntos o aspectos.

¹³ Puede consultarse sobre el particular R. Pastor Sánchez-A. López Miras-J. Gervas. *Historia clínica informatizada*. En la rev. «Medicina Clínica» núm. 103 pp. 304-309.

simplemente falta de tiempo por tener que atender a muchas personas.

Toda esta información, que se contempla en la propia Ley General de Sanidad¹⁰, cabe incluso tratarla desde dos perspectivas: una primera que vendría a suponer la base para una posterior autorización del paciente ante las intervenciones médicas que se estimen oportunas; y otra que sería la aprobación legalmente efectiva del paciente que permite al personal sanitario protegerse ante posibles demandas judiciales.

A veces la recogida y entrega de datos será voluntariamente llevada a cabo, mientras que en otras ocasiones puede ser exigida por una normal legal. En cualquier caso, habrá siempre que tener en cuenta el tipo de datos solicitados, la obligatoriedad o no de facilitarlos, la permanencia, finalidad y legalidad de la operación de recogida de los mismos etc.

Tengamos también en cuenta que en ocasiones el enfermo puede limitarse a firmar o a asentir a cuanto se le proponga, con el único fin de poder recobrar la salud. Esta manera de proceder, que a veces se ve indirectamente reflejada en la «hoja de consentimiento» y que ha dado en llamarse posición legalista del mismo¹¹, debiera ser corregida en el sentido de afirmar más que sea consecuencia de una correcta información al paciente y la humanización de la medicina. O, en otras palabras, debería basarse en la existencia de estas condiciones: posibilidad real de que el paciente comprenda bien lo que dice y tenga voluntariedad en la decisión que toma, una vez conozca la patología que padece, el plan de actuación para superarla y los riesgos posibles.

Considerar que esto pueda llevarse siempre así en la práctica cabe que muchos lo entiendan harto problemático. Se argumenta, por ejemplo, que en numerosas ocasiones los enfermos no están capacitados para entender la compleja información que se les suministra; o que solo recogen una pequeña parte

de tal información; o que la propia patología que padecen puede obstaculizar seriamente la formación de una clara voluntad, tomándose las decisiones a menudo en base a factores triviales¹².

De cualquier manera que sea, toda la información recibida del paciente deberá entrar a formar parte, en la medida que se estime necesaria, de la «historia clínica» considerada en sentido amplio como un documento en el que deben contenerse todos los datos de utilidad para el tratamiento del paciente. Por tanto deberá reunir estas características: ser lo más completa posible, permitir la comunicación interprofesional e interdisciplinar, y consecuentemente la puesta en practica de una correcta actuación asistencial. Además la «historia clínica» debiera de ser de alguna manera única, uniforme o normalizada, no muy extensa, legible y clara; dicho de otra forma, posibilitar cuanto pueda la finalidad asistencial, y también la docente e investigadora, así como algunos otros objetivos que se consideren necesarios desde un ángulo de política sanitaria. Con una concepción así de amplia podemos entender que una historia clínica contenga numerosos datos biográficos, sociales, médicos etc. del patient¹³.

EL PROCESO DE INFORMATIZACIÓN DE LOS DATOS SANITARIOS

Un proceso de informatización de historias clínicas y los datos en ellas contenidos es algo en lo que normalmente van a participar no solo los expertos de la salud sino también los informáticos. Unos y otros podrán aportar desde sus respectivos campos las ideas y necesidades que entiendan deba cubrir un «archivo» o «banco de datos»: la estructura, el tipo de datos recopilables, el procedimiento mejor de recogida de los mismos, las finalidades previstas a la hora de ponerlo en funcionamiento, los usos y medidas de seguridad a tomar etc.

Ahora bien, este proceso de informatización de datos sanitarios puede plantear algunos problemas, entre los que pudiéramos tomar a manera de ejemplo los siguientes: la concreción sobre lo que debe entenderse por «datos personales», o deducir si en ellos cabe incluir o no los informes médicos relativos a la salud de los pacientes.

La primera cuestión pues que nos asalta es la de dilucidar a qué nos referimos cuando hablamos de «datos personales». Indirectamente el art. 17 de la Propuesta de Directiva del Consejo de Europa de 27 de julio de 1990 nos dice que «salvo acuerdo libre, expreso y escrito del interesado, los Estados miembros prohibirán el tratamiento automatizado de datos que se refieran al origen racial y étnico, la opinión política, las convicciones religiosas o filosóficas, las afiliaciones sindicales, así como las informaciones relacionadas con la salud y la vida sexual». De ahí podemos entrever cuales sean aquellos datos especialmente sensibles que han de ser preservados, si bien la propia norma legal introduce inmediatamente la posibilidad de que existan excepciones a lo que acaba de estipular cuando haya «motivos importantes de orden público».

No de manera diferente se muestra la Ley Orgánica 5/1992, de 29 de octubre, que dentro de nuestra legislación viene a recoger el espíritu de aquella disposición europea en el art. 6 cuando señala que «el tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa», y admite la excepción cuando los datos se recojan de fuentes accesibles al público, o para el ejercicio propio de las funciones de la Administración en el ámbito de sus competencias.

Más difícil quizás puede aparecer el encontrar un concepto claro de lo que se deba entender como «datos sanitarios». Aquí vale de muy poco la legislación, ya que se limita a hablar de ellos pero sin determinar claramente su contenido y alcance⁴, si bien la Memoria

Explicativa de enero de 1981 a la que ya hemos hecho referencia dice en el núm. 45 que «la noción de datos de carácter personal relativos a la salud... abarca las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo», incluyendo las posibles informaciones sobre abuso de alcohol u otras drogas.

El acceso a los datos

Este aspecto es objeto igualmente de diferentes puntos de vista, ya que salvándose la confidencialidad, cabe discutir quien puede acceder a ellos, y con qué procedimiento. Así por ejemplo, sobre lo primero, no faltan los que prevén tal posibilidad para el personal sanitario, para los pacientes, e incluso para los órganos judiciales. Y sobre lo segundo pueden darse diversos métodos, como el que cada profesional pueda acceder e incluir datos en su espacio específico, sin que pueda modificar o eliminar la información de otros profesionales.

En estrecha coordinación con ello cabe hablar también del control que sin duda ha de tenerse sobre el archivo o banco de datos. Las nuevas tecnologías han revolucionado la materia referente a las garantías de protección a la intimidad de las personas, ante eventuales tratamiento de sus datos; los actuales avances técnicos permiten almacenar, tratar y realizar prospecciones sobre la información recogida en aquellos, a la vez que se está extendiendo una sensibilización social suscitada por la posibilidad de establecer perfiles a partir de las referencias que puedan obtenerse de varios bancos de datos. La inexistencia de estas circunstancias en el sector sanitario obliga a los profesionales del mismo a asumir tal realidad y a actuar en consecuencia, teniendo delante su responsabilidad ética como tal profesional de la salud (de acuerdo a sus convicciones individuales), la responsabilidad igualmente ética (ya objetiva) basada en las normas deontológicas de su profesión, y finalmente la responsabilidad frente a la sociedad general a través de las normas jurídicas que ésta se ha dado para garantizar una correcta convivencia.

⁴La Directiva 95/46 del Parlamento Europeo y del Consejo de Europa, de 24 de octubre de 1995, sobre protección de las personas físicas en lo que respecta a la informatización de sus datos personales, establece en el art. 2.a que son «datos personales» aquellos referentes a la identificación de una persona física identificada o identificable, directa o indirectamente, mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica psíquica, económica, cultural o social. Y en su art. 8 alude a los datos sanitarios como parte de los personales, sin especificar cuales sean aquellos. Como tampoco lo especifica el Convenio del Consejo de Europa de 28 de enero de 1981 (ratificado por España en 1984) que se limita a mencionar entre los personales «los relativos a la salud». Una propuesta de Resolución del Consejo de Europa, patrocinada por Francia, Italia, Noruega y algunos otros países trató en 1992 de concretar algo este tema, considerando como tales «los que tengan un vínculo evidente con el estado de salud de una persona».

¹⁵ Este texto fue sometido a debate en la Comisión Constitucional del Congreso al considerarlo redundante (ya se consagra la protección en el art. 1), pero otros defendieron su inserción. La discusión fue, en todo caso, dura y se dijo que el origen de que apareciera se encontraba en la Constitución Portuguesa.

La confidencialidad de los datos

Un tercer punto a tratar, igualmente en relación con los anteriores, es el de la confidencialidad de la información sanitaria almacenada en los archivos o bancos de datos. Buena parte de los autores, cuando tratan esta materia, consideran que el posible uso de datos médicos puede estar relacionado con fines asistenciales, estudios epidemiológicos, investigaciones clínicas, estudios retrospectivos, educación, y finalmente tratamientos estadísticos. Teniendo en cuenta todo ello, y considerando que hay una obligación de respetar la intimidad personal y familiar de los pacientes, la confidencialidad ha de asentarse por un lado el un «derecho del paciente» y por otro en una «obligación o deber del personal sanitario».

Los riesgos que pueden presentarse pueden ser varios: por ejemplo considerar la información recogida en los archivos o bancos de datos como propiedad del personal o de las instituciones sanitarias; o bien la mercantilización que es posible hacer hacia determinadas instituciones o entidades que puedan verse afectadas de alguna forma dependiendo de la información (industria farmacéutica, mutuas de accidentes laborales, empresas aseguradoras, etc. etc.). Evidentemente habrá que evitar en cuanto sea posible la quiebra de la confidencialidad y para ello no deberíamos olvidar las deficiencias que aún sufren los sistemas de documentación y archivo de muchos centros sanitarios, la carencia de una cultura profesional sobre confidencialidad, y la presión que a veces puede darse desde intereses ajenos al acto sanitario (presión política, económica, de medios de comunicación etc.). Pensemos, por ejemplo, hipotéticamente, en posibles cesiones de datos a empresarios para que puedan descartar de la contratación laboral a quienes padezcan determinadas patologías; o los que puedan intentar conseguir las entidades aseguradoras sobre enfermos crónicos o graves; o los datos personales que algunos medios de comunicación pretenden sobre personajes famosos con el fin de obtener crédito o ganancias.

Por eso, ante la proliferación de bases de datos que almacenan información sobre las personas (incluidos datos sanitarios), la legislación europea y la española han intentado establecer mecanismos de protección, en función de la tipología y características de las mismas, así como de la finalidad perseguida por quienes tienen la titularidad sobre ellas.

LA REGULACIÓN JURÍDICA DEL TRATAMIENTO DE LA INFORMACIÓN MÉDICO-SANITARIA AUTOMATIZADA

Cualquier toma de posición sobre la confidencialidad en la información sanitaria desde la perspectiva del Derecho ha de partir del principio de la dignidad de la persona como un valor a respetar. Así se reconoce en el Preámbulo y el artículo 1 de la Declaración Universal de los Derechos Humanos de 10 de diciembre de 1948, y de forma más específica en el artículo 12 cuando señala que «nadie será objeto de injerencias arbitrarias en su vida privada, su familia... ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

Igualmente, una base en nuestra legislación particular de la que hay que partir es la Constitución de 1978, que en su artículo 18.1 expresamente declara que «Se garantiza el derecho al honor y a la intimidad personal y familiar y a la propia imagen», señalando a continuación, en el núm. 4, que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»¹⁵

También hemos de tener en cuenta que una materia como la que tratamos, tan sensible, no ha podido dejar de ser objeto de regulación europea, estando nuestro país, como miembro de la UE, comprometido a adaptar su legislación a las normas que se elaboren a nivel comunitario. La Di-

rectiva 95/46, de 24 de octubre de 1995¹⁶, intenta regular la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos.

Finalmente, dentro de nuestro derecho interno, la Ley Orgánica 5/1992, de 29 de octubre, sobre regulación de la protección a los ciudadanos en el tratamiento automatizado de sus datos (LORTAD) se ocupa también del tema, de igual forma que la Ley 5/1998, de 6 de marzo, lo hace tratando de incorporar la Directiva del Parlamento Europeo de 11 de marzo de 1996 sobre protección jurídica de las bases de datos. Todo ello debido sin duda al ámbito legal en esta materia que está cobrando cada vez más una dimensión internacional.

Sobre el tratamiento de datos personales, aparte la propia noción de los mismos en relación con el campo sanitario, a lo que ya hemos hecho referencia, se dispone de forma bastante extensa que ha de entenderse como tales «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo, interconexión, así como su bloqueo, supresión o destrucción» (art. 2.b). A continuación se señala lo que se entiende por «fichero de datos», «fichero automatizado» etc., debiendo considerarse entre los datos personales aquellos de carácter sanitario (art. 8).

La legislación pues, con buen criterio, exige previamente a la creación de cualquier banco de datos personales-sanitarios una serie de condiciones: deberán los que pretendan ser titulares de los mismos determinar su estructura, el tipo de datos a recoger y el procedimiento para llevarlo a cabo, la finalidad y usos posibles de cuanto en él se almacene, las posibles cesiones, y las medidas de seguridad a adoptar sobre su contenido

y el acceso al mismo. Si se trata de bancos de datos pertenecientes a sujetos de titularidad pública, como es el caso de la mayoría de los hospitales, se exige no solo que tales cuestiones vengan especificadas en los Boletines o Diarios Oficiales correspondientes, sino también que sean notificadas a la Agencia de Protección de Datos y anotados en el Registro General de Protección de datos dependiente de ésta.

Es relativamente habitual que en el tratamiento automatizado de datos participen distintas personas físicas o jurídicas, las cuales pueden tomar parte en su almacenamiento, aplicación a los mismos de operaciones lógicas o aritméticas, su modificación o borrado, recuperación o difusión etc. Del mismo modo es posible que un concreto tratamiento pueda realizarse en nombre y por cuenta de otro, es decir, se preste un servicio consistente en un tratamiento informático; así por ejemplo no es infrecuente el que puedan implicarse en tales operaciones grabadores de datos, analistas-programadores, etc. ¿a quién se calificará como «responsable» del tratamiento?. El Convenio del Consejo de Europa, de 1981, señala como responsable del fichero a la persona natural jurídica, autoridad pública, servicio o cualquier otro organismo que, con arreglo a Derecho, sea competente para decidir la finalidad del mismo, la categoría de datos que deben registrarse y las operaciones que a éstos pueden aplicarse.

Una vez cumplimentados tales requisitos podrá comenzarse a introducir datos en los bancos o ficheros automatizados, debiendo a partir de entonces obtener el consentimiento de los pacientes con relación al tratamiento de sus datos personales y advirtiéndoles de su almacenamiento, posible cesión, derecho de acceso a los mismos, y señalándoles también las obligaciones que la entidad titular asume sobre confidencialidad y seguridad de su contenido.

La propia Directiva comunitaria a la que hemos aludido dice que «Los Estados miembros prohibirán el tratamiento de datos que revelen... datos relativos a

¹⁶ DOCE n. L 281/31, de 13 de noviembre de 1995. Esta disposición tuvo su origen cinco años antes, en 1990, en una propuesta inicial que posteriormente fue Dictaminada por el Comité Económico y Social del Parlamento Europeo.

la salud» (art. 8.1) tratando precisamente de evitar los posibles riesgos de violación al derecho de intimidad. Sin embargo en los números siguientes, ese mismo precepto viene a admitir excepciones «cuando el tratamiento de los datos 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 sea realizado por un profesional sanitario sujeto al secreto profesional, sea en virtud de la legislación nacional o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto».

Esta manera de contemplar el tratamiento de los datos sanitarios se encuentra también plasmada en diversas normas nacionales, tal como por ejemplo en las españolas. Así podemos considerarlo teniendo presente la Ley General de Sanidad (arts. 10 y 61), o la Ley Orgánica sobre el Tratamiento Automatizado de Datos de Carácter Personal (LORTAD de 29 de octubre de 1992) donde, aparte el personal sanitario, se dice que «el responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal está obligado al secreto profesional respecto de los mismos y el deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado, o, en su caso, con el responsable del mismo» (art. 10).

De modo que la «seguridad» en el contexto del tratamiento automatizado de datos podríamos contemplarla como en dos momentos: aquel en que se procede a recoger las informaciones para archivarlas, y las instalaciones donde se almacenan. Sobre lo primero cabe decir que en bastantes legislaciones se especifica que los bancos de datos se crearán y llevarán de tal manera que se impidan intrusiones indebidas (ej. ley sueca 446/1982, art. 7), indicándose que se procurará una estrategia global tendente a dotarlos de los debidos sistemas de seguridad. Nues-

tra Ley Orgánica ya citada señala al respecto que el responsable del fichero deberá adoptar las medidas técnico-organizativas necesarias para garantizar la seguridad de los datos y evitar su posible alteración o pérdida, o tratamientos no autorizados. Se prevé que un Reglamento establezca los requisitos y condiciones a exigir en los ficheros o bancos de datos para dar respuesta a la demanda europea que reconoce que «en la actualidad las bases de datos no están suficientemente protegidas en muchos Estados por la legislación vigente y, cuando existe, tal protección no es uniforme» (Directiva 96/9 CE de 11 de marzo de 1996 1º considerando).

A este respecto cabe recordar que la seguridad de la información constituye sin duda un elemento omnipresente y necesario en la sociedad moderna. Los servicios de información electrónica exigen una infraestructura segura de telecomunicaciones, unos terminales seguros y una utilización asimismo segura. Pero, al mismo tiempo, tampoco puede olvidarse que no debe haber excesos en la materia porque podría caerse en incompatibilidad con la libre circulación de información que también pretende protegerse.

Todo ello nos lleva pues a concluir que la protección de los datos médicos ha de encontrarse en el derecho a la intimidad, y que la información y confidencialidad en el ámbito sanitario no deja de ser como una expresión más del respeto a la dignidad humana. De esta forma entendemos debe interpretarse lo dispuesto en los arts. 10 y 11 de la Ley General de Sanidad, y en ese contexto hemos de ver también la proyección penal que tiene la violación del debido secreto en el vigente código penal, que dedica una rúbrica al «descubrimiento y revelación de secretos» y en concreto en el art. 199.2 dice que «el profesional que, incumpliendo sus obligaciones de sigilo o reserva, divulgue los secretos de otra persona, será castigado con penas de prisión de 1 a 4 años, multa de 12 a 24 meses, e inhabilitación especial para dicha profesión por espacio de 2 a 6 años».

Y si contemplamos la situación desde la esfera civil veremos cómo las nuevas técnicas aplicadas a la recogida y procesamiento de datos personales han relanzado la vieja idea del jurista Savatier de que todo riesgo debe tener un garante y todo daño un responsable. Por consiguiente ante los posibles perjuicios que puedan producirse en este campo no hay duda de que cabe acudir a lo dispuesto en el art. 1902 del código civil cuando determina que «el que por acción u omisión causa daño a otro interviniendo culpa o negligencia, está obligado a reparar el daño causado». Bien es verdad que si en este precepto el elemento subjetivo de la culpa aparece como base para poder conseguir una indemnización, el propio código atenúa este principio y permite actuar sobre una responsabilidad objetiva en determinados supuestos que pudieran trasladarse por analogía a la materia que comentamos (ej. el art. 1905). Tampoco deberíamos olvidar otras disposiciones que pueden llevarnos en esa dirección, tales como la Ley Orgánica de Protección Civil al Honor, la Intimidad y la Propia Imagen, de 5 de mayo de 1982, o incluso aquellas normas que existen para dar cumplimiento al párrafo 2 del art. 43 de nuestra Constitución.

En este contexto de generalización de la responsabilidad frente a una mala utilización de los datos y bancos de datos, no parece extraño que sea en la profesión sanitaria donde se prevean unas situaciones especialmente sensibles. La sociedad aspira a reglamentar las relaciones entre los profesionales de la misma y quienes soliciten sus servicios, y también a que aquellos reparen los hipotéticos daños que puedan ocasionarse con motivo de sus actuaciones profesionales independientemente de que exista error, impericia o incluso diligencia. ¿El por qué de tal situación? sin duda habría que buscar no una sino varias causas, pero entre otras se reconoce actualmente que puede deberse a una cierta despersonalización en el ejercicio de la medicina, que implica en ocasiones que el paciente no se sienta ligado personalmente a su médico y que psicoló-

gicamente se muestre en situación defensiva frente a una organización sanitaria que desborda su comprensión. Añadamos igualmente una cierta desmitificación de las profesiones liberales, frente a la fe ciega que durante mucho tiempo se tuvo en ellas, y tendremos delante algunas explicaciones.

Aún con todo cuanto hemos expuesto, el tema de la protección de la intimidad de las personas, con relación a los bancos de datos informatizados, sigue siendo objeto de discusión. Bastaría traer a colación la polémica suscitada en Alemania tras una famosa sentencia de su Corte Constitucional pronunciada en el año 1969, a partir de la cual la doctrina comenzó a hablar de dos posibles «zonas» o «esferas» a diferenciar: a) una absolutamente tutelada por la ley (que será únicamente aquella referida a la intimidad personal en sentido estricto), y b) otra relativamente tutelada (con posibilidad de utilizar alguno de sus datos según el principio de adecuación a los fines o intereses en juego).

Tal tesis fue ya en su momento criticada al comprobarse que tomando datos sueltos puede actualmente llegarse a construir un perfil de individuo (por eso la llamaron algunos «teoría del mosaico»), y que por tanto todas las zonas deberían quedar debidamente protegidas. Tampoco faltaron quienes defendieron la idea de que cada persona, según su papel social, debería ser quien decidiera cuáles de sus datos y cuáles no podrían ser objeto de protección (llamada «teoría del rol social»)¹⁷.

Puede ser igualmente esclarecedor lo dispuesto en la ya citada Recomendación del Consejo de Europa, de 23 de enero de 1981, cuando en el anexo primero viene a abarcar dentro de las garantías de protección casi todos los datos sanitarios, dice a este propósito que «abarcará a todos los bancos médicos automatizados creados con fines de tratamiento médico o de salud pública o de investigación médica en los cuales se almacenen informaciones médicas y, en su caso, informaciones sociales o

¹⁷ Puede verse sobre el particular la obra *Banche di dati e diritti della persona*, Cedam Padova 1985, en especial pp. 95-96.

¹⁸ La Agencia de Protección de Datos, en la ya citada Memoria de 1995, pp.92 ha dejado claro la inexistencia de dichos procedimientos y cómo en la práctica no se proporciona muchas veces a los pacientes la información precisa. Y si tal sucede, es evidente que el paciente difícilmente puede ejercer sus derechos en este terreno.

¹⁹ Ley italiana de 19 de noviembre de 1997 (Gazzeta Ufficiale della Repubblica de 21 de noviembre) sobre «Trattamento dei dati sensibili» sobre todo arts. 3, 5, 6 y 7. En ellos se especifica cuando pueden utilizarse, la modalidad de tratamiento informático la conservación de los mismos y su comunicación y difusión.

administrativas conexas relativas a individuos identificados o identificables». No obstante conviene no olvidar que en la práctica se suele diferenciar el tratamiento jurídico según la finalidad perseguida por quienes vayan a utilizarlos: se trate de asistencia o terapia, o a trabajos de investigación.

Tomando en consideración el primer supuesto, hoy existe una buena cantidad de programas informáticos cuya finalidad es la confección e incorporación al fichero o banco de datos de las historias clínicas. Sin entrar en pormenores que ya ha descrito la doctrina, sí conviene recordar la no coincidencia a la hora de decidir a quien pertenecen: es frecuente partir de la idea de que la información sanitaria es propiedad de la persona enferma o asistida, y únicamente si ella concede el oportuno permiso (o en su caso los familiares, cuando así esté previsto en la ley) puede revelarse; de igual forma que, con las debidas reservas, se admite la aplicación de lo que algunos denominan «privilegio terapéutico» y que consiste en poder utilizar información con fines de avance científico, o cuando exista un interés público debidamente contrastado y siempre que los datos a utilizar no sobrepasen la finalidad establecida.

Por eso el enfermo tiene derecho a saber si sobre él existe algún tratamiento de datos, la categoría del mismo, y en general cual puede ser su posible utilización. ¿Podrá dicho paciente acceder por sí mismo o por intermediación de persona autorizada a ellos?. En el Preámbulo de la Directiva ya comentada se dice que precisamente el propio interés de los pacientes y la protección de los derechos y libertades de terceros permiten a los Estados restringir dicho acceso, pudiendo exigir que se haga siempre a través de un profesional de la medicina.

En España el Real Decreto 1332/1994, de 20 de junio, no establece ninguna especialidad, por lo que el artícu-

lo 61 de la Ley General de Sanidad podría ser susceptible de aplicación de la forma más amplia¹⁸, lo que a su vez pudiera permitir el derecho de los pacientes a solicitar y obtener la rectificación o supresión de datos inexactos, incompletos o no correctos; de igual manera que podrían solicitar de las autoridades sanitarias que se transmitan dichos cambios a las personas o archivos a quien pudieran haber sido enviados. Naturalmente que cuando hablamos de cambios y rectificaciones estamos haciendo referencia a los datos puramente sociales o demográficos, ya que los datos clínicos estrictamente hablando derivan generalmente no de la información del paciente cuanto de otras fuentes como pueden ser los resultados de analíticas, radiológicos, etc., sobre éstos no deberían poder exigir los pacientes cambios o supresión, porque (aparte el posible consentimiento ya previamente por él prestado) deben de quedar todos ellos liberados para así, en todo momento, tener a disposición y proseguir con el diagnóstico y tratamiento debido.

Si el enfermo conociera que sus datos son utilizados sin respeto a la normativa legal, sí que podría solicitar el desbloqueo de los mismos o el que sean objeto de oportuno tratamiento con garantía. Otra pregunta que podríamos hacernos es la referida al tiempo que deben conservarse los datos personales sanitarios en los ficheros o bancos de datos; no hay unanimidad en la respuesta y no falta alguna legislación, como la italiana¹⁹ que dice que solo pueden serlo por un periodo no superior al que sea necesario para cumplir las obligaciones y finalidades propias de la institución y el objeto de petición de dichos datos. Entre nosotros, el artículo 4 de la Ley Orgánica de 1992 de la que ya hemos hablado señala que «serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados», y que sólo reglamentariamente podrá autorizarse en su momento la conservación en atención a valores históricos.