TELEMEDICINA Y PROTECCIÓN DE DATOS SANITARIOS

TELEMEDICINA Y PROTECCIÓN DE DATOS SANITARIOS

(ASPECTOS LEGALES Y ÉTICOS)

JAVIER SÁNCHEZ-CARO

Subdirector General y Jefe
de la Asesoría Jurídica del INSALUD

FERNANDO ABELLÁN

Letrado de la Corte de Arbitraje del Ilustre Colegio de Abogados de Madrid,
Sección de Responsabilidad Civil Sanitaria

GRANADA, 2002

Derecho Sanitario Asesores
Calle O'Donnell, 43 - 1.ºA
28009 MADRID
Tel.: 91 576 75 80 • Fax: 91 577 28 33
E-mail: dchosanitario@wanadoo.es

ISBN: 84-8444-481-3 • Depósito Legal: Gr. 196/2002

Fotocomposición, impresión y encuadernación: EDICIONES EL PARTAL, S.L.

SUMARIO

PRÓLOGO

Las nuevas tecnologías, con la aplicación generalizada de los medios informáticos, electrónicos y telemáticos, está provocando cambios muy profundos en la sociedad, a los que pocas manifestaciones del conocimiento científico pueden ser ajenos.

Las coordenadas de espacio y tiempo, elementos constantes en toda manifestación del conocimiento humano, que ponían de relieve su carácter circunstancial, condicionando toda experiencia científica, se ven hoy día desbordadas por una nueva realidad, la «sociedad tecnológica», en la que es posible acceder y transmitir el conocimiento científico sin las tradicionales servidumbres que han acompañado todo descubrimiento o innovación.

Los juristas debemos asumir que hemos pasado de la aplicación de la técnica en la sociedad, a la sociedad de las nuevas tecnologías. Hoy día, la sociedad se hace y se desarrolla en la medida que se instala en las nuevas tecnologías, la diferencia entre la sociedad y la técnica que describía Ortega y Gasset, en los años treinta en la Universidad de Verano de Santander y la sociedad de las nuevas tecnologías está en que la técnica, hasta ahora, ha venido colaborando al desarrollo social, mientras que a partir de ahora, la sociedad está inmersa en las nuevas tecnologías, componente estructural de su ser y desarrollo mismo.

Internet y las nuevas tecnologías han creado una nueva realidad que antes no existía y que lanza constantes desafíos al pensamiento.

Ese desafío que ahora se nos presenta con más fuerza, supone un nuevo reto: combinar humanismo y tecnología en una sociedad en continuo cambio.

En este nuevo ambiente, el derecho y la medicina tienen un elemento común; ambas ciencias se ocupan del hombre, se preocupan del hombre y por el hombre, por su devenir. Por lo que tiene de permanente en las distintas circunstancias de espacio y tiempo.

Para los médicos, el hombre es objeto de estudio en cuanto paciente, a los juristas les preocupa el hombre, la persona, en cuanto ser en conflicto. En ambos casos, la persona se nos presenta en un contexto, en una circunstancia histórica concreta.

Los médicos buscan el progreso en la atención de la salud de los ciudadanos; los juristas buscan la justicia en las relaciones interpersonales. Siguiendo a los filósofos griegos podríamos decir que, ambos, médicos y juristas, buscamos curar al hombre restableciendo el equilibrio y la armonía del ser humano. Ambas profesiones tienen un alto contenido ético, se preguntan constantemente sobre el concepto de persona y su dignidad y en cierto modo son también profesiones bellas, pues la belleza se identifica con el equilibrio de las cosas, con el logro de la armonía.

Este es, a mi juicio, uno de los méritos más destacados de los autores, *Javier Sánchez-Caro y Fernando Abellán,* añadir, ahora, a su larga trayectoria como juristas dedicados al estudio del Derecho Sanitario, una especial sensibilidad para transmitirnos sus conocimientos sobre un tema de gran actualidad.

La obra *«Telemedicina y protección de datos sanitarios»,* constituye una aportación científica de consulta obligada para médicos y juristas.

La prestación de servicios de asistencia sanitaria a distancia, expresión que nos permite aproximarnos a este nuevo concepto de «telemedicina», es analizada por los autores en todas sus manifestaciones; la teleasistencia, la televigilancia, la teleconsulta y la aparición de «webs» sanitarias, como manifestaciones de una nueva forma de entender los procesos asistenciales, plantean problemas éticos y jurídicos que se abordan en esta obra con un rigor, una claridad y un apoyo documental poco común.

Se presta especial atención a los problemas derivados de esta nueva forma de atender y curar al paciente, sobre todo en él ámbito de los compromisos éticos que el ejercicio de la profesión médica comporta y en la necesaria reserva y custodia de los datos personales de los pacientes que, al incorporarse a soportes informáticos, exigen un especial deber de diligencia para evitar que puedan ser conocidos por personas ajenas al proceso asistencial o no habilitadas por la Ley.

El estudio del régimen jurídico de los datos relativos a la salud, calificados por la Ley de Protección de Datos, como especialmente sensibles, constituye una muestra de la calidad científica de los autores y de la profundidad y rigor de sus conocimientos.

La obra ofrece un capítulo dedicado a formular unas conclusiones que constituyen un compendio exhaustivo de los problemas más actuales que pueden encontrar en su quehacer diario, médicos y juristas en la aplicación de las nuevas tecnologías. Su consulta y detenida reflexión constituye un auténtico «regalo» para quienes llevamos años dedicándonos a las relaciones entre el derecho y la salud.

Para terminar, porque lo importante es el trabajo al que se dedican estas líneas, *Javier Sánchez-Caro y Fernando Abellán*, han logrado plasmar en su obra *«Telemedicina y protección de datos sanitarios»,* la aspiración de todo jurista: transmitir su conocimiento con claridad, precisión y sencillez.

Madrid, 19 de noviembre de 2001

JOSÉ MARÍA ÁLVAREZ-CIENFUEGOS SUÁREZ
Magistrado del Tribunal Supremo

I
CONCEPTO DE TELEMEDICINA

I.1. ALGUNAS DEFINICIONES DE INTERÉS. EVOLUCIÓN DEL CONCEPTO DE TELEMEDICINA

La mayor parte de las definiciones clásicas del concepto de telemedicina hacen referencia al ejercicio de la medicina a distancia [1]. Dentro del elenco de estas últimas podemos comenzar destacando la de la *Organización Mundial de la Salud (OMS)*, que la considera «el suministro de servicios de atención sanitaria, en los que la distancia constituye un factor crítico, por profesionales que apelan a las tecnologías de la información y de la comunicación con objeto de intercambiar datos para hacer diagnósticos, preconizar tratamientos y prevenir enfermedades y heridas, así como para la formación permanente de los profesionales de atención a la salud y en

[1] El origen histórico de la Telemedicina se sitúa generalmente a raíz de la introducción del teléfono (1900), y más concretamente en el año 1924 con el programa de radio denominado «Radio News» en el que un médico visitaba a un paciente a través de las ondas. La primera demostración entre varios estados de Estados Unidos tuvo lugar en 1951, en la Feria Mundial de Nueva York. *Telemedicina. La salud en el siglo XXI*, Estudio Editorial, 2001 (pág. 47).

actividades de investigación y evaluación, con el fin de mejorar la salud de las personas y de las comunidades en que viven» [2].

Se entiende, por tanto, la telemedicina como la realización de una actividad sanitaria propia de situaciones en las que se produce un problema de distancia física entre el facultativo y el paciente.

En una línea conceptual parecida el doctor G. TANGALOS la define como el proceso por el que la comunicación electrónica, visual u oral es empleada para 1) proporcionar soporte diagnóstico y consultivo a los facultativos en lugares remotos; 2) asistir en la prestación, o proporcionar ésta directamente, de servicios médicos a los pacientes en lugares remotos; 3) mejorar o pulir las habilidades y conocimientos de servicios médicos en zonas remotas [3].

En un sentido más amplio se pronuncia el *Comité Permanente de Médicos Europeos*, cuando indica que «el término telemedicina

[2] Esta definición aparece recogida en el *Plan de Telemedicina del INSALUD*, editado por la Subdirección General de Coordinación Administrativa, Área de Estudios, Documentación y Coordinación Normativa. Madrid, 2000; pág. 19. Aquí se cita también otra definición incluida en el denominado documento *Marco de la Telemedicina en el INSALUD*, elaborado en 1998, que se refiere a la telemedicina como *«La utilización de las tecnologías de la información y de las comunicaciones como un medio de proveer servicios médicos, independientemente de la localización tanto de los que ofrecen el servicio, como de los pacientes que lo reciben, y la información necesaria para la actividad asistencial»*.

[3] V. Dr. ERIC G. TANGALOS, director de la División de Medicina Interna Comunitaria de la *Clínica Mayo* en Rochester, Minnesota (Estados Unidos). *Telemedicina. La salud en el siglo XXI*. Estudio Editorial. 2001 (prólogo, pág. 12).

define el ejercicio de la medicina a distancia. En la telemedicina las decisiones relacionadas con las intervenciones, el diagnóstico y el tratamiento, y las recomendaciones se basan en datos, documentos o cualquier tipo de información trasmitida por sistemas de comunicación» [4].

En términos también genéricos, prescindiendo ya del carácter remoto o no del lugar donde se realiza la actividad, la *Asociación Médica Mundial* considera que la «telemedicina es la práctica de la medicina a distancia gracias a la cual las intervenciones, el diagnóstico, las recomendaciones y las decisiones terapéuticas se fundamentan en los datos clínicos, documentos y otras informaciones transmitidas por los sistemas de comunicación» [5].

En el mismo sentido anterior, para la *Asociación Médica Americana* la telemedicina consiste en el ejercicio de la medicina desde la distancia a través de las telecomunicaciones y de tecnología interactiva de video [6].

[4] V. *Documento CP97/33*, del *Comité Permanente de Médicos Europeos*, denominado *Principios Éticos de la Telemedicina*, donde además se manifiesta que es preferible que la telemedicina se limite a situaciones en las que el médico no pueda estar físicamente presente en un plazo de tiempo razonable.

[5] V. Preámbulo de la *Toma de posición de la Asociación Médica Mundial sobre las responsabilidades y las directrices éticas ligadas a la práctica de la telemedicina*, adoptada por la 51 Asamblea, celebrada en Tel Aviv (Israel), en octubre de 1999.

[6] *Joint Report of the Council on Medical Education and Council on Medical Service, 1996 Meeting of the AMA House of Delegates, Chicago* (http://www.ama-assn.org).

Finalmente, podemos mencionar a la *Asociación Americana de Telemedicina*, que la define como la utilización de información médica remitida de un sitio a otro mediante comunicaciones electrónicas, para favorecer la salud del paciente o para proveerle cuidados y con el propósito de mejorar estos últimos [7].

Analizando las definiciones anteriores, se aprecia, tal y como sostienen DEL POZO GUERRERO y GÓMEZ AGUILERA [8], una evolución del viejo concepto de telemedicina, asociado únicamente a la utilización de las telecomunicaciones para mejorar la calidad de la atención sanitaria en zonas remotas deficientemente atendidas, hacia un nuevo concepto de telemedicina en sintonía con los términos globalidad e interoperabilidad que impone la sociedad de la información.

Para los citados autores, la telemedicina clásica dará paso a una nueva telemedicina entendida como una manera de calificar la forma de hacer y organizar los servicios para cuidar y restituir la salud de todos, en virtud de la cual se identifique precisamente a

[7] *Telemedicine Report to Congress, January 31, 1997. American Telemedicine Association* (http://www.atmeda.org).

[8] FRANCISCO DEL POZO GUERRERO y ENRIQUE J. GÓMEZ AGUILERA (Grupo Bioingeniería y Telemedicina. Universidad Politécnica de Madrid). Ver su trabajo *Telemedicina: una visión del pasado y del futuro*, publicado en la Revista *Todo Hospital* (Monográfico Telemedicina), julio-agosto 2001 (págs. 444-445). Para los citados autores el futuro nos depara una *cibercultura de la medicina*, que dará lugar a un escenario telemédico que permitirá construir entornos virtuales de colaboración, compartición y acceso a la información en medicina, desconocidos hasta el momento, y que cambiarán los modos de cooperación, trabajo y comunicación de los profesionales y de los pacientes.

la salud como el objetivo último de las tecnologías de la información y las comunicaciones [9].

Esta evolución del concepto de telemedicina es apreciada también por el profesor GONZALO HERRANZ cuando, a la vista de los últimos posicionamientos sobre la materia tanto de la Asociación Médica Mundial como del Comité Permanente de los Médicos Europeos, afirma que la idea básica que subyace es que la telemedicina es un modo más de ejercer la medicina, que se justifica tanto por su capacidad de hacer llegar a ciertos pacientes, inaccesibles de otro modo, la asistencia del médico, como por poder mejorar la calidad de la atención médica [10].

I.2. ¿QUÉ SE ENTIENDE ACTUALMENTE POR TELEMEDICINA?

Para el grupo europeo CATAI, dirigido por la catedrática española OLGA FERRER-ROCA [11], y que aboga por la necesidad de con-

[9] *Ibídem* (pág. 448), donde también se manifiesta respecto de la nueva telemedicina que en la misma *«… se va desluciendo su condición de sustantivo para convertirse en adjetivo»*.

[10] GONZALO HERRANZ RODRÍGUEZ. Ver su ponencia *Aspectos Éticos de la Telemedicina*, en el *VII Congreso Nacional de Derecho Sanitario*, celebrado en Madrid, en octubre de 2000. Ed. Fundación Mapfre Medicina 2001 (pág. 26).

[11] O. FERRER-ROCA, J.A. ABREU REYES, R. ABREU GONZÁLEZ, M. SUAREZ DELGADO, E. SOLA-RECHE. CATAI (Centro de Alta Tecnología en Análisis de la Imagen), Tenerife. Para estos autores la práctica de la telemedicina puede traer consigo fundamentalmente tres aplicaciones: posibilitar las historias clínicas electrónicas, manejar información de pacientes electrónicamente; y, en su caso,

cienciar y capacitar a los profesionales y a los ciudadanos en las nuevas tecnologías llevando a cabo un código infoético para la práctica de la telemedicina [12], el concepto de telemedicina sería muy amplio y comprendería tres aspectos distintos y complementarios que, a su vez, plantearían diferentes cuestiones:

I.2.1. **La telemedicina como una nueva forma de ejercicio de la medicina**

Dentro de la práctica médica, a través de la sociedad de la información, resulta particularmente relevante todo lo referente a la garantía de calidad de los servicios médicos, a la garantía de renovación o actualización de los conocimientos de los profesiona-

---

elaborar diagnósticos e indicar tratamientos por vía telemática. Ver artículo *Capacitación médica en la sociedad de la información. Preparando la legislación para una revolución asistencial*. Rev. Clín. Esp. 2001 (201, págs. 315-321).

[12] Algunos autores, como la doctora PETRA WILSON (Visiting Scientist European Comission. D.G. XIII), consideran conveniente la elaboración de un código infoético propio para la práctica de la telemedicina. La infoética es un término construido a semejanza del de bioética, pero con las palabras información y ética (su utilización en Europa data de 1997.). Para dicha autora la infoética consiste en los principios éticos que se invocan para sustentar la investigación, desarrollo e implementación de la información tratada tecnológicamente, dentro de lo que se denomina Sociedad de la Información. La infoética discurre por muchos y diferentes campos, tales como la filosofía (ética), lingüística, economía, ley, sociología, ciencia política, educación, religión/teología, inteligencia artificial, informática. El ámbito de trabajo de la infoética consiste en los aspectos privados/individual y público/institucional de los problemas éticos de carácter nacional, internacional y global (VIII Winter Course Catai, artículo *Infoethics–The European Perspective.* Marzo 2000).

les y a la libertad de movimiento de estos últimos consagrada por la Unión Europea.

Relacionado con esta cuestión, pero fuera del grupo CATAI, resulta de interés la diferenciación que propone G. ATIENZA MERINO [13], entre telemedicina estática o de almacenamiento y telemedicina interactiva, que se lleva a cabo por medio de imágenes móviles.

En la *telemedicina estática* los datos y las imágenes de la exploración clínica de los pacientes se almacenan en archivos que son enviados posteriormente al ordenador del especialista quien, después de estudiar el caso clínico, emite un diagnóstico y, en su caso, un tratamiento.

Y la *telemedicina interactiva* se caracterizaría por el establecimiento de sesiones de videoconferencia en tiempo real entre dos profesionales o incluso entre un médico y determinado paciente, lo que requiere una red a prueba de fallos, rápida y potente.

I.2.2. **La telemedicina como manejo electrónico de datos**

Cobra especial importancia aquí la sensibilización de médicos y usuarios sobre la validez legal de la historia clínica electrónica,

[13] G. ATIENZA MERINO (Axencia de Avaliación de Tecnoloxías Sanitarias de Galicia); ver artículo *La Telemedicina en la práctica médica*. Revista Galega de Actualidade Sanitaria (vol. 1, núm. 2, año 2001, págs. 124 a 127).

así como sobre las medidas que determinan la seguridad e intimidad de los datos sanitarios y las normativas comunitarias sobre libertad de movimiento de datos personales.

I.2.3. **Telemedicina y tecnologías de la información**

Para el citado grupo CATAI resultan necesarias normativas de control *ad hoc* que permitan la certificación de técnicas y tecnologías adecuadas en las aplicaciones de la telemedicina, y que aquellas que regulan en la actualidad los dispositivos de telecomunicaciones y de la sociedad de la información en general sean moduladas cuando se apliquen a la práctica médica.

En este trabajo nos vamos a ocupar fundamentalmente de las dos primeras acepciones o vertientes de la telemedicina, el ejercicio de la actividad médica y el manejo (tratamiento) automatizado de los datos concernientes a la salud de las personas.

II
APLICACIONES GENERALES DE LA TELEMEDICINA

Las aplicaciones básicas de la Telemedicina pueden encuadrarse en tres bloques fundamentales que son los procesos asistenciales, la gestión de pacientes y administración, y los servicios de información y formación.

II.1. PROCESOS ASISTENCIALES

Se trata de las aplicaciones directamente relacionadas con el tratamiento y cuidados que prestan los médicos a los pacientes. Dentro de estos procesos puede hablarse de las siguientes variantes:

II.1.1. **Teleasistencia**

Consiste en la interacción entre un médico y un paciente situado a distancia, normalmente aislado geográficamente y en situación de urgencia médica [14].

[14] A modo de ejemplo, cabe decir que en las prisiones situadas en lugares remotos de Estados Unidos se utiliza cada vez con más frecuencia la

II.1.2. **Televigilancia**

Se trata del seguimiento de enfermos crónicos desde el domicilio de estos últimos, mediante la recogida por vía telemática de informaciones médicas (tensión arterial, electrocardiograma, etc.). Esta forma de telemedicina se utiliza frecuentemente con pacientes que padecen enfermedades crónicas como la diabetes, hipertensión, deficiencias físicas o mujeres con embarazos de alto riesgo. En algunas ocasiones se requiere formar al propio paciente o a un familiar del mismo para la obtención y transmisión de los datos. En otros casos debe recurrirse a un enfermero u otra persona cualificada.

II.1.3. **Teleconsulta entre médicos**

Se trata de la interacción entre dos médicos, uno encargado del paciente, y otro especialista en un campo determinado. Dentro de esta modalidad podrían distinguirse dos supuestos:

II.1.3.1. *Telediagnóstico*

Consistente en la transmisión de electrocardiogramas, imágenes radiológicas, etc., remitidas por el médico generalista que atiende al

---

telemedicina para atender a los reclusos, debido al coste económico de transportar a estos últimos a las clínicas y al riesgo potencial para los ciudadanos de dicho transporte. *Congressional Telehealth Briefing, June 23, 1999, American Telemedicine Association* (http://www.atmeda.org).

paciente a otro médico especialista (radiólogo, cardiólogo, etc.), que no se encuentra físicamente en el centro asistencial.

II.1.3.2. *La segunda opinión*

En casos complejos en los que el paciente, a través del médico que le atiende directamente, desea recabar una segunda opinión médica de otro facultativo antes de someterse a una intervención de riesgo.

II.1.4. **Teleconsulta entre paciente y médico. Las «webs» sanitarias**

El paciente busca directamente la opinión de un médico con el que no ha tenido una relación previa, y que no le ha realizado un examen clínico. Es el caso frecuente de las personas que buscan consejo médico a través de las webs sanitarias. El problema de esta práctica deriva de la falta de fiabilidad, confidencialidad y seguridad de las informaciones, así como de la ausencia de garantías respecto de la identidad y cualificación del médico, como consecuencia de la falta de inmediación física entre este último y el paciente.

PARERAS propone distinguir tres niveles de consulta de casos clínicos a través de internet [15]:

[15] LLUIS G. PARERAS. Ver capítulo 3, denominado *Internet y Medicina. Presente y Futuro*, de la obra *Aseguramiento y Medicina Virtual. Los nuevos*

• Nivel inicial de consulta de cuestiones relativas a la salud, que no implican diagnóstico ni tratamiento e informan al paciente para mantenerse más sano. Para dicho autor este nivel sería absolutamente ético.

• Segunda opinión a través de internet. En la medida en que haya un médico responsable presente físicamente con el paciente, la relación de este último con el facultativo no sufre alteración.

• Y un tercer nivel consistente en la consulta directa del paciente a través de internet, práctica considerada por PARERA inaceptable éticamente en el momento actual.

No obstante, para intentar reducir los inconvenientes referidos, la Unión Europea, a través de su *Grupo de Trabajo sobre criterios de calidad para webs sanitarios* [16], ha desarrollado un documento que incluye guías sobre los citados criterios, compatibles con la mayor parte de las acreditaciones europeas en funcionamiento, las propias directivas europeas y los estándares técnicos relevantes en internet. En el documento se enuncian los siguientes principios básicos [17]:

---

desafíos (Actas del simposio celebrado en Madrid, el 17 de octubre de 2000). Ed. Fundación Sanitas y otros. Madrid, 2001 (págs. 42 y 43).

[16] Grupo perteneciente al Directorio General de la Sociedad de la Información de la Comisión Europea, cuyo trabajo está dirigido a diseñar una futura marca CE para webs sanitarios. Está integrado por 58 participantes de todos los países de la Unión Europea, además de representantes de Noruega, Suiza y Estados Unidos.

[17] *Quality Criteria for Health Related Webs*, del citado *Grupo de Trabajo sobre criterios de calidad para webs sanitarios*. Documento accesible desde la siguiente página web de la Unión Europea: *http://europa.eu.int/information_society/eeurope/ehealth/quality/draft_guidelines/text_….* Y también referido en *Diario Médico*, de fecha 15 de octubre de 2001.

• *Transparencia y honestidad del proveedor*. La persona u organización responsable de la página web debe estar perfectamente identificada, así como los objetivos y propósitos del servicio y la audiencia a la que se dirige. También debe indicarse quienes son los patrocinadores económicos.

• *Autoridad científica*. Las fuentes de información deben estar claramente identificadas: nombre y credenciales de los proveedores de la información.

• *Confidencialidad*. Los sistemas para garantizar la intimidad, seguridad y confidencialidad deben estar bien definidos.

• *Actualización de contenidos*. Las actualizaciones de la página web deben realizarse periódicamente.

• *Responsabilidad*. Los enlaces que se realicen deben cumplir con una serie de garantías de calidad y la selección de contenidos encontrarse claramente definida.

• *Accesibilidad*. La página web debe permitir que los usuarios puedan navegar sin confusiones.

Otra clasificación de las aplicaciones asistenciales de la telemedicina sería la propuesta por MONTEAGUDO, que cita las siguientes [18]:

• *Teleconsulta*, para facilitar el acceso al conocimiento y consejo de un experto remoto. Puede referirse a una especialidad concreta, como en los casos de telerradiología, telepatología, telecardiología y telelaboratorio, o constituir una plataforma de uso general.

[18] V. JOSÉ LUÍS MONTEAGUDO. Revista *Informática y Salud*, núm. 29 (enero/febrero 2001), artículo denominado *Telemedicina* (págs. 1.499-1.500).

• *Trabajo cooperativo*, cuando se establece una conexión en red de grupos de profesionales que comparten recursos de conocimiento, bases de datos, e informaciones para ayuda en la toma de decisiones. Una subclase sería el telediagnóstico cooperativo.

• *Telepresencia*, que supone la asistencia de un profesional sanitario remoto a un paciente, como en el caso de telediagnóstico mediante sistemas de videoconferencia en tiempo real.

• *Telemonitorización*, que hace referencia a vigilancia remota de parámetros fisiológicos y biométricos de un paciente. Es el supuesto de la telemonitorización fetal de embarazadas de alto riesgo.

• *Teleasistencia*, que alude a la provisión de cuidados de salud a pacientes en entornos de vida diaria, como en el caso de los ancianos que viven en su hogar. Normalmente es interactiva e incluye telealarmas.

• *Telecirugía*, que hace uso de la telerrobótica, la visión artificial y la realidad virtual.

II.2. GESTIÓN DE PACIENTES Y ADMINISTRACIÓN

Citas, peticiones de pruebas analíticas y radiológicas, intercambio de información electrónica entre profesionales (informes interconsulta entre atención primaria y atención especializada, etc.), acceso a la historia clínica compartida del área de salud, de manera que cada facultativo pueda acceder a la información en el momento y de la forma en que la necesite [19].

[19] *Plan de Telemedicina del INSALUD*; ob.cit. (pág. 27). Aquí se distingue, al hablar del acceso a la historia clínica compartido, entre la posibilidad de

II.3. SERVICIOS DE INFORMACIÓN Y FORMACIÓN TANTO A CIUDADANOS COMO A PROFESIONALES SANITARIOS

Transmisión de contenidos sobre la salud especialmente a través de internet.

Los sistemas de salud pueden utilizar herramientas de teleformación y de apoyo a la toma de decisiones para sus profesionales, y facilitar contenidos informativos y servicios para los ciudadanos [20].

---

obtener una visión horizontal por el médico de Atención Primaria, que le permita conocer la evolución de los diferentes episodios sufridos por el paciente, y una visión vertical por el especialista, que le permita consultar toda la información de detalle de un episodio concreto.

[20] ENRIQUE PALAU. Revista *Administración Sanitaria*; artículo *Telemedicina*: *un intento de aproximación desde lo sanitario*. Vol. V, núm 19, julio-septiembre 2001.

III

TELEMEDICINA COMO FORMA DE EJERCICIO DE LA MEDICINA. ASPECTOS ÉTICOS

Puede decirse que los aspectos éticos que subyacen a la práctica de la telemedicina son, esencialmente, los que confluyen en el ejercicio de la medicina convencional [21]. En ambos casos se trata, lógicamente, de atender y curar al paciente.

No obstante, por razón de la utilización en telemedicina de sofisticados aparatos técnicos y complejos sistemas de información, que sin duda potencian las posibilidades de asistencia a los pacientes en general, pero también los riesgos para estos últimos, se hace preciso ahondar de forma adicional en algunas cuestiones específicas y singulares del ejercicio de la telemedicina.

A esta tarea han dedicado sus esfuerzos algunas asociaciones internacionales y grupos de expertos del ámbito médico, que han formulado sus recomendaciones sobre la materia, destacando entre estas últimas las de la *Asociación Médica Mundial*

[21] V. PETRA WILSON. *An overview of legal issues in European Telemedicine.* Octubre, 1998, pág. 1.

(AMM) (1.999) [22] y las del *Comité Permanente de Médicos Europeos* (1.996) [23], de las que pueden extraerse las siguientes líneas básicas:

III.1. PARTICULARIDADES DE LA RELACIÓN MÉDICO-PACIENTE EN TELEMEDICINA

A la hora de reflexionar sobre la relación médico paciente en telemedicina, el primer principio importante que puede extraerse de las declaraciones internacionales mencionadas consiste en que la utilización de la telemedicina debe ser excepcional y circunscribirse nada más que a los casos en los que el médico no pueda, dentro de un retraso aceptable y en las condiciones de seguridad requeridas, estar presente físicamente [24].

En otras palabras, no debe prescindirse, si es posible, de la relación de contacto físico y personal entre el médico y el paciente, que se considera preferible a la telemedicina y, desde luego, el uso

[22] *Toma de posición de la Asociación Médica Mundial sobre las responsabilidades y las directrices éticas ligadas a la práctica de la* telemedicina. Adoptada por la 51 Asamblea general de la AMM, Tel Aviv (Israel), octubre 1999. Ver traducción de esta declaración publicada en *Actualidad del Derecho Sanitario*, núm. 62, junio 2000, págs. 481 a 484.

[23] *Principios Éticos de la Telemedicina*. Comité Permanente de Médicos Europeos. Markku Aarimaa, 28 de noviembre de 1996.

[24] Ver punto 8 del documento de la AMM.

de esta última no debe afectar negativamente a la relación personal médico/paciente [25].

Sentada la premisa anterior, y sin perjuicio de reconocer la utilidad de muchos de los servicios de asistencia que posibilita la telemedicina y el hecho de que la misma debe estar abierta a todos los médicos más allá de las fronteras nacionales [26], para la Asociación Médica Mundial lo más aconsejable sería que el paciente no pudiera beneficiarse directamente de una consulta por telemedicina salvo que se dieran las siguientes condiciones [27]:

• Que el médico y el paciente dispongan de elementos de identificación recíproca fiables [28].

• Que exista una previa relación profesional médico-paciente [29].

[25] Ver apartado *Relación médico/paciente* del documento del Comité Permanente, donde se dice que *«Es preferible que todos los pacientes consulten al médico cara a cara, y que la telemedicina se limite a situaciones en las que el médico no pueda estar físicamente presente en un plazo de tiempo razonable»*.

[26] En el apartado *Autorización-Competencia* del documento anterior, se indica que las posibilidades que ofrece la telemedicina deben estar al alcance de todos los médicos.

[27] Ver puntos 7, 9 y 10 del texto de la AMM.

[28] En igual sentido en el citado apartado *Relación médico/paciente* del documento del Comité Permanente, se considera esencial que el médico y el paciente se puedan identificar mutuamente con toda seguridad cuando tenga lugar la consulta telemédica.

[29] En el mismo apartado que se acaba de citar se manifiesta que *«Normalmente una consulta telemédica directa sólo debería tener lugar si el médico tiene una relación profesional con el paciente o tiene conocimiento suficiente del problema en cuestión, de manera que el médico pueda emitir un juicio clínico conveniente y justificado»*.

• Que el médico tenga un conocimiento suficiente del problema en cuestión, de modo que pueda ejercer un juicio clínico apropiado y justificable. Queda a salvo, lógicamente, el supuesto de urgencia en que el médico tiene que basar su juicio en informaciones incompletas, debiendo estar en estos casos constituido el factor determinante de su opinión o tratamiento médico por la propia naturaleza de la urgencia.

III.2. RESPONSABILIDAD MÉDICA Y TELEMEDICINA

Se parte del principio de que el médico debe ser totalmente independiente y libre para elegir o rechazar la telemedicina [30].

III.2.1. Requisitos para practicar la telemedicina

Seguidamente, se establecen una serie de premisas para que el médico pueda utilizar la telemedicina evitando incurrir en responsabilidades:

a) Que únicamente recurra a ella en función del mejor interés del paciente. Es decir, el uso de la telemedicina se legitima por el beneficio al paciente, pero nunca por la mayor comodidad del médico.

[30] Puntos 11 al 15 del documento de la AMM.

b) Que haya obtenido el consentimiento del paciente, previa identificación del mismo, y que, con el fin de evitar los riesgos de fuga de información inherentes a las comunicaciones electrónicas, se haya asegurado de que fueron adoptadas las normas de seguridad para garantizar la confidencialidad del paciente, en un doble sentido [31]:

• Los datos relativos al paciente y otras informaciones que le conciernen no pueden ser transmitidos a un médico o a otro profesional de la salud más que a petición del paciente o con su consentimiento, y en la medida en que él determine.

• Las informaciones que se transmitan deben referirse al problema médico concreto de que se trate.

Por su parte, PETRA WILSON [32], en aras de procurar al paciente la autonomía referida, considera que el médico debe informar de forma completa sobre el uso de la herramienta telemática de que se trate, el proceso telemático (incluida su

[31] V. Punto 17 de la declaración de la AMM. Y apartado *Ética médica, consentimiento del paciente y secreto médico*, del documento del Comité Permanente donde se dice que *«Las normas habituales en materia de confidencialidad y seguridad se aplican también a los documentos que se utilizan en telemedicina. Sólo pueden utilizarse los métodos de archivo y transmisión cuando se garantice el secreto y la seguridad.*

Los datos del paciente y las demás informaciones sólo pueden facilitarse a otro médico o profesional sanitario a petición o con el consentimiento informado (permiso) del paciente, y de la manera que éste apruebe. Estos datos deben estar relacionados con el problema de que se trate».

[32] PETRA WILSON. *An overview of legal issues in European Telemedicine*. ob. Cit. Octubre 1998 (pág. 2).

seguridad) y las implicaciones que su utilización conlleve para la salud del paciente.

También debe informar al paciente de las razones profesionales que le llevan a utilizar medios telemáticos, en detrimento de otros medios convencionales.

c) Que esté preparado para participar, en caso de necesidad, en el seguimiento del tratamiento.

d) Que en el supuesto de intervención en el proceso asistencial de telemedicina de personal no médico que realice tareas de búsqueda o transmisión de datos, con fines de control u otros, que tenga seguridad el médico de que la formación y competencia de este personal auxiliar permite una utilización ética adecuada de la telemedicina [33].

e) Que guarde un dossier apropiado de sus pacientes en el que todos los aspectos concernientes a cada caso sean adecuadamente documentados, tratando de garantizar la perennidad de las informaciones, así como su fidelidad con el original. [34]

[33] En el apartado *Calidad, seguridad y protección en telemedicina* del documento del Comité Permanente se manifiesta que *«el médico debe asegurarse, cuando realiza intervenciones médicas a distancia, de la presencia de un personal suficiente y convenientemente formado que atienda al enfermo y le preste asistencia permanente»*.

[34] V. Punto 23 del texto de la AMM y apartado *Historial del paciente* del documento del Comité Permanente, donde se dice que *«Todos los médicos que practican la telemedicina deben llevar un historial completo del paciente y to-*

f) Que el médico se encuentre autorizado para ejercer en el país en que se halle establecido y sea competente en su especialidad médica; y también, en el caso de que atienda directamente por medio de telemedicina a un paciente de otro país, que cuente con dicha autorización para ejercer en este último lugar [35].

Para GONZALO HERRANZ, la obligación de obtener la necesaria autorización en los lugares de residencia y de ejercicio significa que la práctica de la telemedicina ha de someterse plenamente a las normas éticas vigentes en los respectivos territorios. Como dice dicho autor, no es admisible una telemedicina desvinculada de las comunidades deontológicas de origen y destino o, al menos, de una regulación internacional [36].

---

dos los casos deben estar convenientemente documentados. También debe consignarse la manera de identificar al paciente, así como la cantidad y la calidad de los datos y del resto de la información que se recibe. Las conclusiones, las recomendaciones y los servicios de telemedicina que se efectúen deberán estar convenientemente documentados».

[35] V. Punto 22 del documento de la AMM, donde se excepciona de la obligación de autorización el supuesto en que el médico utilice un sistema mundialmente homologado. También en el apartado *Autorización–Competencia* de la declaración del Comité Permanente se prescribe que *«Los médicos que practican la telemedicina deben estar autorizados para ejercer la telemedicina en el país o el Estado donde se encuentren y deben ser competentes en su especialidad. Para que un médico practique la telemedicina directamente con el paciente, debe estar autorizado a ejercer la medicina en el Estado donde resida habitualmente el paciente, o el servicio debe aprobarse a escala internacional».*

[36] GONZALO HERRANZ RODRÍGUEZ. Ver su citada ponencia *Aspectos Éticos de la Telemedicina*, en el *VII Congreso Nacional de Derecho Sanitario*, celebrado en Madrid, en octubre de 2000. Ed. Fund. Mapfre Medicina, 2001 (pág. 27).

III.2.2. ¿Cuándo debe abstenerse el médico de practicar la telemedicina?

Asimismo, existen una serie de supuestos en los que el médico debe rechazar su participación en telemedicina:

• Cuando no tenga los conocimientos, la capacidad, las informaciones o los datos suficientes del paciente para poder formular adecuadamente su punto de vista [37].

• Cuando no esté seguro de que la eficacia y calidad del equipamiento que necesita son suficientes y que éste cumple la normativa establecida [38].

[37] En el apartado *Calidad, seguridad y protección en telemedicina*, del documento del Comité Permanente, se establece que *«el médico debe evaluar atentamente los datos y el resto de la información que recibe. El médico sólo puede dar su opinión, dar recomendaciones o tomar decisiones si la calidad y la cantidad de los datos o del resto de la información que recibe es suficiente y está relacionada con el caso en cuestión»*. Asimismo, en el caso de urgencia (apartado *Relación médico-paciente*) se determina que el juicio del médico *«debe basarse en una información casi completa, pero entonces el peligro para la salud del enfermo será el factor determinante para dar consejo o tratamiento»*.

[38] V. Punto 19 del documento de la AMM, en el que también se indica que para cada una de las interacciones efectuadas en el marco de la telemedicina habría que establecer un protocolo que indique las medidas a adoptar en caso de defectos del material o de aparición de problemas en casa del paciente.

En la declaración del Comité Permanente se afirma abiertamente (apartado *Calidad, seguridad y protección en telemedicina*) que *«un médico que practique telemedicina es responsable de la buena calidad de sus servicios. No puede utilizar la telemedicina sin comprobar que el equipo necesario para dar este tipo de servicio tiene la calidad adecuada y funciona correctamente»*.

• En los casos como el de la televigilancia, en los que el paciente asume la responsabilidad de recoger los datos y transmitirlos al médico, cuando no tenga seguridad de que el paciente está bien formado en los procedimientos necesarios, de que tiene capacidad física suficiente y de que comprende bien la importancia del papel que le toca desempeñar [39].

III.2.3. **La responsabilidad del médico tele-experto**

Puede matizarse también la responsabilidad según sea la actuación del médico en cada supuesto, y así se contemplan dos situaciones distintas:

a) Respecto del médico que asiste al paciente directamente por medio de telemedicina.

Evidentemente asume la responsabilidad del caso, especialmente del diagnóstico, los consejos, los planes de tratamiento y las intervenciones médicas directas [40]. Y también sigue siendo respon-

[39] V. Punto 16 del texto de la AMM, donde además se dice que la misma actitud debería prevalecer cuando se trata de un miembro de la familia u otro auxiliar implicado en la práctica de la telemedicina.

[40] En la declaración del Comité Permanente (apartado *Responsabilidad del médico*) se indica que cuando el médico practica la telemedicina directamente con el paciente, aquél asume la responsabilidad del caso en cuestión.

sable del tratamiento y del diagnóstico del paciente en el caso de que solicite la opinión de otro médico (tele-experto) [41].

b) Respecto del médico tele-experto que es consultado por otro colega, siendo este último quien tiene contacto directo con el paciente.

Aquí el médico tele-experto es libre de aceptar o no la consulta y por ello responsable de la calidad de los consejos que proporcione al médico actuante. Debe precisar las condiciones exigidas para su eficacia, ya que tiene el derecho a determinar si la información que se le transmite es suficiente o no para dar una opinión fundada.

Ahora bien, como decíamos anteriormente, y matiza el profesor GONZÁLO HERRANZ, el médico que pide la opinión de otro colega retiene la responsabilidad del tratamiento y a él corresponde decidir, con el consentimiento del paciente, el uso que debe hacerse de las opiniones o recomendaciones del colega consultado, es decir, del tele-experto [42].

[41] En igual sentido en el apartado *Responsabilidad del médico* del documento del Comité Permanente, se proclama que *«el médico que pide a otro médico su opinión seguirá siendo responsable del tratamiento y de las demás decisiones y recomendaciones que se hagan al paciente»*.

[42] GONZALO HERRANZ RODRÍGUEZ. Ver su citada ponencia *Aspectos Éticos de la Telemedicina*, en el *VII Congreso Nacional de Derecho Sanitario*, celebrado en Madrid, en octubre de 2000. Ed. Fund. Mapfre Medicina, 2001 (pág. 29).

Asimismo, debe evaluar cuidadosamente los datos y otras informaciones que reciba y sólo puede dar su opinión médica, hacer recomendaciones o adoptar decisiones si recibe datos y otras informaciones cuyo número y calidad sean suficientes y apropiados [43].

Finalmente, tiene obligación de registrar en un dossier los consejos que dé, así como los datos y otras informaciones en las que se hubieran fundado [44].

III.3. LEX ARTIS Y TELEMEDICINA

El uso de las nuevas herramientas tecnológicas dentro del campo sanitario va a originar, a buen seguro, nuevos fenómenos de responsabilidad médica y ello no solo por razón de los especiales deberes de confidencialidad a que obliga el tratamiento automatizado de los datos sobre la salud, sino también a consecuencia de la redefinición de la *«lex artis»* que se producirá en el tratamiento de muchas enfermedades.

En este sentido, PETRA WILSON considera que la generalización de la telemedicina como elemento de diagnóstico puede hacer incurrir en responsabilidades al médico que, teniendo a su alcance medios telemáticos necesarios y adecuados para el tratamiento de

[43] V. Punto 20 de la declaración de la AMM.
[44] V. Punto 24 de la misma declaración antes citada.

un paciente, no los empleara a su debido tiempo perjudicando con ello a este último [45].

La citada autora hace hincapié también en la importancia en telemedicina de tener presente la normativa para la protección de consumidores respecto de los contratos a distancia, pensando sobre todo en aquellas situaciones en las que se produce una relación directa entre el médico que presta servicios telemáticos y el paciente que los recibe, sin existir una mediación entre ambos de otro médico que se encuentre físicamente con el paciente. En estos casos PETRA WILSON considera que lo que estará haciendo en realidad el paciente es contratar a distancia con un proveedor de servicios de salud, que tendrá que cumplir con los requisitos y obligaciones que se contienen en la Directiva europea sobre protección de consumidores con respecto a los contratos a distancia [46].

Por su parte, FERRER ROCA y otros [47], entienden que la mala praxis debida a un empleo defectuoso de las técnicas propias de

[45] V. PETRA WILSON. *An overview of legal issues in European Telemedicine*. Ob. cit., pág. 9. La citada autora considera que los problemas de daños a los pacientes por el uso de la telemedicina podrán ser tratados al amparo de la normativa europea sobre productos defectuosos (Directiva del Consejo 85/374/EEC) y sobre aparatos médicos (Directiva del Consejo 93/42/EEC).

[46] Directiva 97/7/EC, sobre protección de los consumidores con respecto a contratos a distancia.

[47] O. FERRER-ROCA, J.A. ABREU REYES, R. ABREU GONZÁLEZ, M. SUAREZ DELGADO, E. SOLA-RECHE. CATAI (Centro de Alta Tecnología en Análisis de la Imagen), Tenerife. Ver artículo *Capacitación médica en la sociedad de la información. Preparando la legislación para una revolución asistencial*. Rev. Clín. Esp. 2001 (201, págs. 315-321).

la telemedicina puede originar responsabilidad por el acto médico, ya sea por falta de capacidad del médico, ya sea por un uso inadecuado.

Para los citados autores la práctica adecuada de una medicina a distancia no queda totalmente garantizada con un código deontológico de buena práctica profesional, ya que éste por si mismo no recogerá los aspectos técnicos que el médico debe manejar para identificar los límites de su conocimiento y que servirán para poder determinar si su conducta es o no negligente.

Como consecuencia de lo anterior, y apoyándose en lo establecido en la Directiva europea de comercio electrónico [48], estiman necesario apostar, además de por una activa formación de los médicos y sanitarios en general, porque se produzca una clara guía colegial en la adecuación y elaboración de códigos de conducta para la sociedad de la información.

Se hace necesario para el médico, en definitiva, una permanente actualización de sus conocimientos y habilidades que, como proclama el Código Deontológico [49], constituye un deber individual del médico y un compromiso de todas las organizaciones y autoridades que intervienen en la regulación de la profesión.

[48] Directiva 2000/31/CE, de 8 de junio de 2000, del Parlamento y del Consejo relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior. El art. 16 de esta Directiva exhorta a las organizaciones y organismos profesionales a elaborar códigos de conducta en el ámbito comunitario.

[49] V. Art. 21.1 del Código de Ética y Deontología Médica, de 1999, de la Organización Médica Colegial (OMC).

Y con respecto al aparataje e infraestructura utilizada en telemedicina, los autores referidos consideran necesaria la promulgación de normativas de control «ad hoc», en dos líneas [50]:

• Por un lado, normativas que permitan la certificación de técnicas y tecnologías adecuadas en las aplicaciones de telemedicina (dispositivos médicos de diagnóstico, control y/o tratamiento a distancia).

• Y por otro lado, respecto de aquellas normativas que regulan actualmente los dispositivos de telecomunicaciones de la sociedad de la información en general, que las mismas sean moduladas o adaptadas cuando se apliquen a la práctica médica.

En tanto estos aspectos no queden suficientemente regulados y aclarados es responsabilidad del médico saber cuál es su límite de actuación, ya que, como recoge el Código Deontológico, el médico está obligado solamente a utilizar prácticas validadas [51].

[50] Los autores mencionados del grupo europeo CATAI entienden que mientras estos aspectos no queden cubiertos con suficiente amplitud en directivas específicas sobre los dispositivos médicos de diagnóstico, control y/o tratamiento a distancia, es responsabilidad del médico saber cuál es su límite de actuación. También consideran que el análisis y evaluación de estas herramientas no puede dejarse en manos de técnicos sin conocimientos médicos, por lo que los médicos habrán de capacitarse para los futuros retos que les brindan las nuevas tecnologías, y potenciarse, además, estudios intermedios (Bioingeniería, Telemedicina, Informática Médica).

[51] V. Art. 29.6 del citado Código de Ética y Deontología Médica de la OMC.

Finalmente, podemos citar la opinión de BENEDICT STANBERRY [52] que se muestra claramente a favor del establecimiento de códigos

[52] BENEDICT STANBERRY, Director del *Centre for Law Ethics and Risk in Telemedicine*, Cardiff, Gales, Gran Bretaña. V. artículo *Law, Ethics and Risk in Telemedicine*, dentro del trabajo donde se recogen las ponencias del VIII Curso de Invierno del CATAI, La Laguna (Tenerife), abril 2000 (págs. 137 a 140).

El citado autor plantea también otro tipo de problemas como son los de jurisdicción aplicable en caso de exigencia de responsabilidades por daños. BENEDICT STANBERRY describe el caso de Estados Unidos en donde las cuestiones de jurisdicción han sido una de las barreras clave para el desarrollo de la telemedicina. Afirma el citado autor que el problema en este país es que un médico que practique la medicina debe tener licencia para practicarla en el estado concreto en que trabaja. Las denominadas Actas de Práctica Médica promulgadas por cada Estado han sido creadas para proteger a los ciudadanos del Estado concreto de que se trate de individuos que ejerzan la medicina sin licencia. En consonancia con lo anterior, los seguros por mala práctica cubren al médico sólo en el Estado en el que él ejerce. Por tanto, un teleconsultante desarrollando servicios de telemedicina más allá del Estado en que trabaja puede correr el riesgo, no solo de practicar la medicina sin ningún tipo de seguro de responsabilidad (lo que se conoce como «practising bare»), sino también de practicarla ilegalmente desde el momento en que asume que cuando diagnostica, trata o prescribe para un paciente (por medios telemáticos) está practicando realmente medicina en el Estado en que dicho paciente se encuentra.

Esta situación puede ser también extrapolable en el marco de la Unión Europea en la medida en que las titulaciones médicas no estén homologadas. Para el citado autor todavía no está claro qué ley es la aplicable en el caso de una consulta transfronteriza, existiendo la posibilidad de que en caso de reclamaciones los pacientes elijan el país de los afectados donde más les convenga por la sensibilidad de su sistema judicial a la cuestión (es lo que se conoce como «forum shopping»).

No obstante, debe recordarse que en la Directiva comunitaria de Comercio Electrónico (2000/31/CE) se determina que, en caso de litigio, es de aplicación la legislación del país donde se asienta el proveedor de los servicios (en este caso sería el médico consultado).

deontológicos específicos de actuación en telemedicina al afirmar que, encontrándose todavía la telemedicina en su infancia, no se conoce todavía qué es o qué debería ser una «práctica aceptada» en esta materia, debido a que muy pocos colegios o asociaciones profesionales han publicado guías oficiales para sus miembros.

III.4. EL DEBATE ÉTICO SOBRE LA VIRTUALIDAD DEL PRINCIPIO DE INMEDIACIÓN MÉDICO-PACIENTE, Y SOBRE LA MEDICINA FUNDAMENTADA EN LA EXPERIENCIA FRENTE A LA DENOMINADA MEDICINA BASADA EN LA EVIDENCIA [53]

El debate ético que suscita la práctica de la telemedicina, entendida ésta en su vertiente de ejercicio de la práctica médica, consiste en analizar si la misma debe ceñirse exclusivamente a los casos en los que media una situación de urgencia, un problema de distancia física (lugar remoto), o si, por el contrario, puede admitirse también el ejercicio de la telemedicina como una alternativa a la medicina convencional justificada por razones de agilidad, mayor seguridad en el diagnóstico, reducción de costes, etc.

Está en juego aquí la relevancia que se considere debe darse al principio de inmediación entre médico y paciente, al contacto

[53] Cabe significar que no nos parece acertada la expresión medicina basada en la «evidencia» desde el momento en que la medicina no es una ciencia exacta. Lo contrario conduciría a considerar que la medicina conlleva siempre una obligación de resultado. Por esta razón sería, a nuestro juicio, más adecuada la expresión de medicina basada en pruebas.

personal y físico entre ambos, que desde Hipócrates hasta nuestros días ha venido siendo sinónimo de un actuar correcto [54].

Para GONZALO HERRANZ, desde el punto de vista deontológico, no es posible una relación médico-paciente conforme a la ética si se apoya exclusivamente en recursos telemédicos. Para dicho autor, estos últimos constituyen un suplemento, no un sustituto, del necesario encuentro directo, cara a cara, entre médico y paciente. La ética profesional exige que, en algún momento de la relación profesional entre médico y paciente –cuanto antes mejor– se establezca un contacto inmediato, personal, que permita realizar la historia clínica y la correspondiente exploración física [55].

En la misma línea, ARTHUR M. HOUSE opina que siempre es mejor la relación personal médico-paciente, si bien, cuando la dis-

[54] El art. 18.1, del Código de Ética y Deontología Médica, de 1999, de la Organización Médica Colegial, establece que *«todos los pacientes tienen derecho a una atención médica de calidad humana científica. El médico tiene la responsabilidad de prestarla, cualquiera que sea la modalidad de su práctica profesional y se compromete a emplear los recursos de la ciencia médica de manera adecuada a su paciente, según el arte médico, los conocimientos científicos vigentes y las posibilidades a su alcance»*.

[55] GONZALO HERRANZ RODRÍGUEZ. *Aspectos Éticos de la Telemedicina*, ob. cit. (pág. 36). Dicho autor se apoya en la alusión del *Código de Ética y Deontología Médica* de 1999, de la Organización Médica Colegial, que en su art. 22.1 establece que no es ético el ejercicio de la medicina mediante consultas exclusivamente por carta, teléfono, radio, prensa o internet. También indica que, en sentido similar, se pronuncia el Código de los médicos alemanes y el de la Asociación Médica Americana, y que esta doctrina está además refrendada por la Declaración de la Asociación Médica Mundial y por las Directrices del Comité Permanente de los Médicos Europeos.

tancia impide que dicha relación se produzca, la telemedicina constituye un elemento idóneo para el diagnóstico y el tratamiento [56].

OLGA FERRER-ROCA si bien reconoce que la práctica médica sin examen clínico directo del paciente es contraria a la ética médica, considera que hay dos claras excepciones a la citada regla:

a) El caso de los especialistas médicos que diagnostican y practican la medicina sin un contacto directo con el paciente, por ejemplo, radiólogos, anatomopatólogos, especialistas de laboratorio.

b) El caso de las áreas aisladas, insulares o rurales, atendidas por médicos generales y con falta de especialistas [57].

Por otro lado, quienes abogan por considerar la telemedicina como una alternativa o incluso, en algunos casos, como una superación del ejercicio de la medicina tradicional que impone la modernidad, apuestan al mismo tiempo por la preponderancia de la denominada *«medicina basada en la evidencia»*, esto es, en pruebas, frente a la *«medicina personalista o tradicional»* en la que el diag-

[56] ARTHUR M. HOUSE, catedrático de la Universidad de Terranova (Canadá) y gobernador de la provincia de Terranova y Labrador, considerado uno de los pioneros de la telemedicina en el mundo. *Ciclo Primavera de la Salud*, dedicado a la Telemedicina y organizado en Madrid por la Universidad Complutense (*Diario 16*, de 8 de junio de 2000).

[57] Prof. Dr. OLGA FERRER-ROCA (responsable de la Cátedra de Telemedicina de la UNESCO ubicada en la Universidad de la Laguna, Tenerife). *Telemedicina*. Ed. Panamericana. Mayo 2001 (pág.179).

nóstico se realiza partiendo de la experiencia personal obtenida por el médico a partir del contacto directo con el paciente en cuestión, y con la de muchos pacientes a los que trató con anterioridad.

Los partidarios de la citada medicina basada en la evidencia fundamentan la virtud de la misma en las ventajas de la estadística frente a la apreciación personal o subjetiva del facultativo, es decir, en el análisis numérico de casos similares ocurridos con anterioridad y en la comprobación de sus resultados. De esta forma, según la corriente mencionada, el diagnóstico médico deja de ser fruto del riesgo individual, de la capacidad o de la formación del médico o del personal sanitario, y se convierte en la comprobación automatizada, accediendo por medios informáticos a una base de datos, de multitud de diagnósticos, petición de pruebas y prescripción de tratamientos previos de otros pacientes anteriores que presentaban síntomas similares [58].

Siguiendo a DEL POZO GUERRERO y a GÓMEZ AGUILERA, a medida que la medicina continúe su evolución usando las nuevas tecnologías emergentes parece imperativo que los protocolos clínicos actuales cambien hacia nuevos protocolos telemédicos, basados tanto en los nuevos procedimientos tecnológicos como en la

[58] V. AMÉRIGO, J.A. y SUÁREZ GARCÍA, Eugenio. *Telemedicina – La salud en el siglo XXI*. (ob. cit.). Para estos autores *«la telemedicina será la nueva forma de practicar la medicina. La observación en la que se basó Hipócrates dará paso a las mediciones automatizadas de nuestros esquemas vitales. La experiencia dará paso a una medicina basada en la evidencia»* (pág. 29). Estudio Editorial 2001.

práctica de la medicina *on-line* y en la oferta de servicios para el telecuidado de la salud [59].

Ahora bien, como indica SIMON WALLACE, el gran reto para los partidarios de esta tendencia reside en conseguir la aceptación por parte de los médicos del uso habitual de los protocolos como manera ordinaria de la práctica médica, y en permitir su disponibilidad de forma electrónica desde el lugar de trabajo, concretamente en plena consulta [60].

En igual sentido opina MONTEAGUDO PEÑA, para quien el primer factor de resistencia apreciado por los expertos para la implan-

[59] FRANCISCO DEL POZO GUERRERO y ENRIQUE J. GÓMEZ AGUILERA. *Telemedicina: una visión del pasado y del futuro*, ob. cit. (pág. 450). Para los citados autores *«El uso generalizado de bases de datos que dispensen servicios de información médica en web cambiará la forma en la toma de decisiones para el cuidado de los pacientes. El aumento imparable de redes globales, protocolos clínicos estandarizados para la cibermedicina y la existencia de 'ciberclínicos' especializados, podría tener como consecuencia a corto plazo la denominada venta de conocimientos médicos»*.

[60] SIMON WALLACE. V. Capítulo 3, *La tecnología de la información y la modernización de los sistemas sanitarios*, de la obra *La tecnología de la información: impacto en la política y gestión sanitaria del siglo XXI (Actas del simposio celebrado en Madrid, el 7 de octubre de 1999)*. JOAN JOSEP ARTELLS I HERRERO, JULIÁN RUÍZ FERRÁN y AURORA BERRA DE UNAMUNO. Madrid, 2000.

Refiriéndose a la situación en Inglaterra, WALLACE afirma que existe un gran número de protocolos disponibles que hasta ahora han tendido más a acumular el polvo de las estanterías que a formar parte de la práctica médica habitual. Para el citado autor la disponibilidad y facilidad del acceso que procuran las tecnologías de la información es una potente posibilidad de generalizar su utilización (pág. 51).

tación de los sistemas de telemedicina es la falta de aceptación por los profesionales médicos de la introducción de cualquier innovación en sanidad. La cultura médica es conservadora y cauta especialmente en lo que se refiere a tecnologías que, como la telemedicina, pueden alterar la relación médico-paciente [61].

Sin duda, unos de los problemas a los que se enfrenta este modo de entender el ejercicio de la medicina es el hecho conocido y admitido por todos de que la medicina no es una ciencia exacta, y que por ello la objetivación del diagnóstico médico por medios informáticos no garantiza el acierto, ya que corre el riesgo de obviar algunos aspectos, no apreciables a primera vista, que pueden resultar esenciales y que quizás sólo pueda ofrecer la experiencia personal y continuada del médico con el paciente.

[61] JOSÉ LUIS MONTEAGUDO PEÑA (Jefe del Área de Investigación en Telemedicina y Sociedad de la Información del Instituto de Salud Carlos III, de Madrid). Ver su trabajo *Modelos de implantación de telemedicina. Impulsores y barreras*, incluido en la Revista *Todo Salud*, julio-agosto 2001 (págs. 457-459). El citado autor indica también otros factores clave que actúan como barrera de la telemedicina: la falta de datos sobre evaluación de las aplicaciones de telemedicina que sirvan de base para la toma de decisiones; la ausencia de protocolos y normas de trabajo para la integración de las aplicaciones de telemedicina en la práctica sanitaria; las cuestiones legales relacionadas con la regulación de la práctica clínica (protección contra demandas por mala práctica); los aspectos de seguridad de datos y confidencialidad; la falta de infraestructuras apropiadas de telecomunicación o los costes de instalación y operación; la adecuación de las estructuras administrativas y organizativas de las instituciones sanitarias actuales; la madurez tecnológica del entorno (garantías sobre la fiabilidad, seguridad, acceso y disponibilidad del servicio); y los aspectos de financiación.

Por esta razón, pudiera pensarse que la postura más acertada sobre esta materia consista en tratar de compaginar las ventajas de las dos formas de entender el ejercicio de la medicina, es decir, conjugar los medios técnicos con la experiencia personal.

IV
TELEMEDICINA COMO MANEJO ELECTRÓNICO DE DATOS SOBRE LA SALUD

Otro de los aspectos trascendentales a la hora de abordar la problemática que suscita la telemedicina es el derivado del tratamiento automatizado de los datos personales sobre la salud del paciente, que han de discurrir por los sistemas de comunicación y almacenarse con las garantías adecuadas.

IV.1. LA PROTECCIÓN DE LOS DATOS PERSONALES. ASPECTOS GENERALES

IV.1.1. Principios inspiradores en el ámbito europeo

La *«Carta de los Derechos Fundamentales de la Unión Europea»*, proclamada en diciembre de 2.000, dedica expresamente un precepto a la protección de datos de carácter personal, configurándolo como un derecho de toda persona respecto de los datos de dicho carácter que la conciernan y estableciendo, además, que los mismos habrán de tratarse de modo leal, para fines concretos y

sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo que prevea la ley [62].

Los antecedentes de declaraciones internacionales en materia de protección de datos son numerosos [63], si bien, dentro del ámbito

[62] *Carta de los Derechos Fundamentales de la Unión Europea*, proclamada por el Parlamento Europeo, el Consejo y la Comisión, y hecha en Niza, el 7 de diciembre de 2000 (Diario Oficial de las Comunidades Europeas, de 18 de diciembre de 2000. C 364). En el art. 8 de este texto se reconoce, además, el derecho de toda persona a acceder a los datos recogidos que la conciernan y a su rectificación. También se indica que el respeto de estas normas quedará sujeto al control de una autoridad independiente.

[63] V. PILAR JIMÉNEZ RIUS, Letrada del Tribunal de Cuentas, Revista *Actualidad Administrativa* (La Ley) núm. 26, semana 25 junio al 1 julio de 2001, artículo *Antecedentes legislativos de la nueva Ley Orgánica de Protección de Datos Personales*; págs. 965 a 1.003. La citada autora alude a los siguientes antecedentes:

a) Declaración Universal de los Derechos Humanos adoptada y proclamada por la 183.ª Asamblea General de la ONU, el 10 de diciembre de 1948 (arts. 12 y 19).

b) Pacto Internacional de Derechos Civiles y Políticos hecho en Nueva York, el 19 de diciembre de 1966 (arts. 17.1 y 17.2).

c) Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales realizado en Roma el 14 de noviembre de 1950 (arts. 8.1 y 8.2).

d) Resolución 509, de 1968, de la Asamblea del Consejo de Europa, sobre los derechos humanos y los nuevos logros científicos y técnicos.

e) Resoluciones del Consejo de Europa de 1973 y 1974, relativas, la primera, a la protección de las personas respecto a los bancos de datos electrónicos en el sector privado, y la segunda, a la protección de las personas respecto a los bancos electrónicos en el sector público.

f) Recomendaciones del Consejo de Europa relativas a la protección de datos personales, entre las que destaca en materia sanitaria la Recomendación R(97)5, de 13 de febrero, relativa a la protección de datos sanitarios.

europeo, la norma de referencia es la directiva comunitaria del año 1995, dedicada a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos [64]. De la citada norma podrían extraerse los siguientes principios en materia de tratamiento y protección de datos:

g) Recomendaciones de la Organización para la Cooperación y Desarrollo de Europa (OCDE), de las que destacan la relativa a la circulación internacional de datos personales para la protección de la intimidad (septiembre 80); y la relativa a la seguridad de los sistemas de información (noviembre 92).

h) Convenio 108, de 28 de enero de 1981, del Consejo de Europa, relativo a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

i) Recomendación 81/679/CEE, de la Comisión, de 29 de julio de 1981, relativa al Convenio del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

j) Recomendación de la ONU relativa al tratamiento automatizado de datos personales, de 14 de diciembre de 1990.

k) Tratado de la Unión Europea. Artículo 6 modificado por el Tratado de Ámsterdam en 1997.

l) Directiva 95/46/CEE, del Parlamento Europeo y del Consejo de Europa, de 24 de octubre de 1995, relativa a la protección de personas físicas con relación al tratamiento de datos personales y a la libre circulación de estos datos.

m) Directiva 97/66 del Parlamento y del Consejo de Europa, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

n) Tratado Constitutivo de la Comunidad Europea. Artículo 286 introducido por el Tratado de Ámsterdam.

o) Propuesta (4) de Reglamento del Parlamento Europeo y del Consejo de Europa sobre la protección de personas físicas en lo que respecta al tratamiento de datos personales por las Instituciones y Organismos de la Comunidad Europea y sobre la libre circulación de estos datos (14 de julio de 1999).

p) Carta de los Derechos Fundamentales de la Unión Europea, de diciembre de 2000 (art. 8).

[64] Directiva 95/46/CE, antes citada.

IV.1.1.1. *Principio de limitación de objetivos*

Los datos deben recogerse con un objetivo específico y posteriormente tratarse o transferirse únicamente en una medida que no sea incompatible con la finalidad de su obtención [65].

No obstante, pueden establecerse excepciones a la norma anterior para la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas, etc. [66].

IV.1.1.2. *Principio de proporcionalidad y de calidad de los datos*

Los datos deben ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se tra-

[65] V. Art. 6.1, b) de la citada Directiva donde se dice que los Estados miembros dispondrán que los datos personales sean *«recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas»*.

[66] Estas excepciones se detallan en el art. 13.1 de la Directiva mencionada, donde además se citan la salvaguardia de un interés económico y financiero importante de un Estado miembro o de la Unión Europea (incluidos los asuntos monetarios, presupuestarios y fiscales); una función de control o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública; y la protección del interesado o de los derechos y libertades de otras personas.

ten posteriormente. Además, tienen que ser exactos y, cuando se precise, actualizados [67].

IV.1.1.3. *Principio de transparencia*

Es obligado informar a los interesados sobre el objetivo del tratamiento, sobre la identidad del responsable del mismo y, en su caso, de su representante, y sobre cualquier otro elemento preciso para garantizar un trato leal [68].

El principio de transparencia conlleva la existencia de unos derechos de acceso, rectificación y oposición, que se concretan en el derecho del interesado a obtener una copia de todos los datos relativos a su persona, en el derecho a que se rectifiquen aquellos datos personales que resulten ser inexactos, y en el derecho, en determinadas situaciones, a oponerse al tratamiento de los mis-

[67] V. Art. 6.1, c) y d) de la misma Directiva, donde también se manifiesta que *«deberán tomarse las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados»*.

[68] Ver también art. 10 de la Directiva, en cuyo apartado c), se indica que habrá de informarse también de lo siguiente: *«los destinatarios o las categorías de destinatarios de los datos, – el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado»*.

mos [69]. Lógicamente, con las excepciones referidas más arriba al tratar sobre el principio de limitación de objetivos.

IV.1.1.4. *Principio de confidencialidad y seguridad del tratamiento*

El responsable del tratamiento tiene obligación de tomar las medidas técnicas y organizativas que sean necesarias para conseguir un nivel de seguridad adecuado que evite los riesgos del tratamiento, es decir, que permita la protección de los datos personales contra la destrucción accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados (en particular cuando el tratamiento incluya la transmisión de datos dentro de una red), y contra cualquier otro tratamiento ilícito de los datos personales.

En este sentido, las personas que actúen bajo la autoridad del responsable o encargado del tratamiento, incluido este último, no deben tratar los datos salvo por instrucción del responsable del tratamiento [70].

[69] V. Arts. 12, 13 y 14 de la Directiva.

[70] V. Art. 16 de la Directiva, y también el art. 25.1 de la misma, donde se dice que *«los Estados miembros dispondrán que la transferencia a un país tercero de los datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado»*.

IV.2. LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA CONSTITUCIÓN ESPAÑOLA

IV.2.1. La llamada libertad informática

La protección de los datos sobre la salud dentro de nuestro ordenamiento jurídico tiene su máximo exponente en la Constitución Española donde se proclama 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» [71].

Algunos pronunciamientos del Tribunal Constitucional sobre este precepto han dado pie a que se hable de la *libertad informática* (también llamada derecho a la autodeterminación informativa) como un nuevo derecho o libertad fundamental de carácter autónomo respecto del derecho a la intimidad personal y familiar, dirigido a hacer frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos [72].

[71] V. Art. 18.4 de la Constitución Española de 1978, que establece 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»*.

[72] V. Sentencia del Tribunal Constitucional 254/1993, de 20 de julio.

V. también ALBERTO ANDÉREZ GONZÁLEZ (Asesor Jurídico del Gobierno de Navarra y Letrado de la Administración de la Seguridad Social), en *Informe Seis – La Seguridad y confidencialidad de la información clínica.* capítulo *Aspectos legales de la seguridad y confidencialidad en la información clínica.* Sociedad Española de Información de la Salud. Pamplona, 2000, pág. 159. El citado autor se hace eco del debate doctrinal en torno a si el precepto citado configura un

Como tiene dicho el Tribunal Constitucional en la Sentencia de noviembre de 2.000, que resolvió el Recurso de Inconstitucionalidad contra la Ley Orgánica de Protección de Datos de Carácter Personal (en adelante LOPD), la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad, y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es así el derecho a controlar el uso de los mismos datos insertos en un programa informático («habeas data») [73].

---

derecho fundamental distinto al propio derecho a la intimidad personal y familiar (consagrado en el apartado 1 del mismo artículo), o si por el contrario dicho precepto se limita a la afirmación de un derecho de carácter instrumental o accesorio respecto del derecho a la intimidad y demás derechos fundamentales, derecho que vendría delimitado por el propio legislador ordinario (se trataría así de un derecho de configuración legal) a través del establecimiento de los límites impuestos a la utilización de la informática como modo de contribuir a la garantía de aquellos derechos fundamentales.

[73] Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. Esta sentencia resolvió el Recurso de Inconstitucionalidad interpuesto por el Defensor del Pueblo contra algunos incisos de los artículos 21.1 y 24.1 y 24.2, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Las consecuencias de esta sentencia son, de un lado, y respecto de la cesión de datos entre las Administraciones Públicas prevista en el art. 21.1, que restringe dicha posibilidad al ejercicio de las mismas competencias o al tratamiento posterior con fines históricos, estadísticos o científicos. En consecuencia, fuera de las excepciones contempladas con carácter general en el art. 11.2 LOPD y de las específicas del art. 21.1 y 21.2 del mismo texto, será siempre necesario el consentimiento de las personas afectadas por los datos para que las Administraciones Públicas puedan cederse los datos entre sí, salvo que expresamente lo excepcione una norma con rango de ley. Por otro lado, con la decla-

IV.2.2. **El derecho fundamental a la intimidad y el derecho fundamental a la protección de datos. Dos conceptos distintos**

IV.2.2.1. *Contenidos diferentes de ambos derechos*

Podríamos hablar, por tanto, por un lado, de un derecho fun-

---

ración de inconstitucionalidad de los incisos del apartado 1 del art. 24, lo que se desprende es que el derecho de información al ciudadano reconocido en el art. 5.1 y 2, únicamente podrá ser excepcionado por las Administraciones Públicas, cuando dicha información pueda afectar a la Defensa Nacional, a la seguridad pública, o a la persecución de una infracción de tipo penal. Finalmente, se suprime todo el apartado 2 del art. 24, por lo que las únicas excepciones específicas que las Administraciones Públicas podrán alegar para el ejercicio de los derechos de acceso, rectificación y cancelación por los ciudadanos, serán las reguladas en el art. 23 (peligro para la defensa del Estado o la seguridad pública, protección de los derechos de terceros, investigaciones, cumplimiento de obligaciones tributarias).

Con relación a este asunto de las excepciones, JAVIER SÁNCHEZ-CARO considera que el Tribunal Constitucional no niega en realidad la posibilidad de que haya de hacerse en algún momento una ponderación de los bienes o derechos en juego, sino que niega que dicha ponderación pueda hacerse por la Administración con una cláusula tan genérica como la prevista en el citado apartado 2 del art. 24 de la LOPD (mediante una mera resolución motivada). No obstante, el citado autor entiende que ha de tenerse en cuenta la dificultad de articular en una Ley los presupuestos y condiciones de la restricción en cada caso posible. Por esta razón indica que *«El riesgo de la sentencia, en nuestra opinión, es abocar al legislador a un casuismo de difícil descripción, pues no hay nada tan complejo como captar o aprehender una realidad multiforme y variopinta»*. Ver su artículo *Ley de Protección de Datos e innovaciones tecnológicas farmacéuticas. Revista de Administración Sanitaria.* Volumen V, Núm. 19, julio-septiembre 2001 (págs. 141 a 143).

damental a la intimidad personal y familiar [74] y, por otro lado, de un derecho fundamental a la protección de datos [75]. La diferencia entre ambos sería que mientras el primero está dirigido a proteger a la persona frente a cualquier invasión que pueda realizarse en el ámbito de su vida personal y familiar que la misma desee excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad [76]; el segundo persigue garantizar a esa persona un poder de control o disposición sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para su dignidad y derecho [77].

[74] Art. 18.1 de la Constitución Española, donde *«se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen»*.

[75] Art. 18.4, también de la Carta Magna, anteriormente reproducido.

[76] Se trataría del *«poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido»* (Ver Sentencias del Tribunal Constitucional 73/1982, de 2 de diciembre; 110/1984, de 26 de noviembre; 89/1987, de 3 de junio; 231/1988, de 2 de diciembre; 197/1991, de 17 de octubre; 134/1999, de 15 de julio, 144/1999, de 22 de julio; y 115/2000, de 10 de mayo).

[77] MIGUEL ÁNGEL DAVARA RODRÍGUEZ distingue entre «datos públicos» (conocidos por cualquiera) y «datos privados» (conocidos por voluntad del titular o en circunstancias especiales y tasadas por las leyes). Los datos privados los divide en «íntimos» (el titular debe proporcionarlos regularmente en cumplimiento de sus obligaciones cívicas) y «secretos» (el titular no está obligado a proporcionarlos salvo casos excepcionales). Asimismo, los datos secretos, también llamados sensibles, los subdivide en «secretos profundos» y «secretos reservados», siendo estos últimos los únicos que quedan reservados en todas las ocasiones y ante cualquier circunstancia. *Manual de Derecho Informático*. Ed. Aranzadi. (3.ª ed. Septiembre 2001) págs 50 a 53.

Al mismo tiempo, este poder de control, característico del derecho fundamental a la protección de datos, consiste en atribuir a su titular un haz de facultades jurídicas para imponer a terceros la realización u omisión de determinados comportamientos (obligación de informar sobre los datos, rectificación de los mismos, cancelación, etc.).

La concreción jurídica de este poder de control o disposición consistiría, fundamentalmente, en el ejercicio de las cinco facultades siguientes [78]:

1. La facultad de consentir la recogida, la obtención y el acceso de los datos personales.

2. La facultad de consentir su posterior almacenamiento y tratamiento.

3. La facultad de consentir su uso o usos posibles por un tercero, sea el Estado o un particular.

4. La facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo.

5. Y la facultad de poder oponerse a esa posesión y usos, requiriendo a quien corresponda que ponga fin a la posesión

[78] Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre (fundamento jurídico séptimo).

y empleo de los datos, previa exigencia de que le informe de qué datos posee sobre su persona y qué destino han tenido. Esta facultad alcanza también a la posibilidad de exigir que los datos sean rectificados o cancelados.

IV.2.2.2. *Distinto objeto de protección*

También por razón del distinto objeto de protección podemos encontrar diferencias entre ambos derechos, ya que, siguiendo al Tribunal Constitucional, el objeto de tutela del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, y ello precisamente porque su objeto no es sólo la intimidad [79].

Matiza incluso el citado Tribunal que los datos amparados por el derecho fundamental a la protección de datos son «todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».

[79] Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. Continúa el Tribunal afirmando que *«el derecho fundamental a la protección de datos alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos»*.

Evidentemente, los datos relativos a la salud de la persona deben entenderse comprendidos dentro del paraguas de protección de este derecho, aún en el caso de que, en algunos supuestos, pudiera considerarse que su conocimiento o difusión no afectara realmente a la vida privada o íntima de la persona en cuestión, y ello por la razón antes comentada de que la protección de los datos de carácter personal no se detiene exclusivamente en los datos de carácter íntimo, sino que va mas allá abarcando a todos los de carácter personal que identifiquen o permitan identificar a la persona.

IV.2.3. *Límites del derecho fundamental a la protección de datos de carácter personal*

Lógicamente, los límites al citado derecho han de venir dictados por la coexistencia del mismo con otros derechos y bienes jurídicos de rango constitucional.

En este sentido, el Tribunal Constitucional cita en su mencionada Sentencia de noviembre de 2000 [80], la seguridad y defensa del Estado, la persecución y castigo del delito, la intimidad de las personas, e incluso la distribución equitativa del sostenimiento del gasto público y las actividades de control en materia tributaria [81].

[80] V. Fundamento jurídico noveno de la citada Sentencia.

[81] Sentencias del Tribunal Constitucional 110/1984 y 143/1994.

IV.3. LA PROTECCIÓN DE LOS DATOS SOBRE LA SALUD DE LAS PERSONAS

IV.3.1. Concepto de datos sanitarios

En cuanto a qué debe entenderse por datos relativos a la salud, y siguiendo al profesor MURILLO DE LA CUEVA [82], la citada expresión abarcaría tanto a los datos de carácter médico como a aquellos otros que guarden relación con la salud.

Quedarían comprendidos, por tanto, todos aquellos datos que tienen que ver con el cuerpo humano, como la sexualidad, la raza, el código genético, pero además los antecedentes familiares, los hábitos de vida, de alimentación y consumo, así como las enfermedades actuales, pasadas o futuras previsibles, bien sean de tipo físico o psíquico; y las informaciones relativas al abuso de alcohol o al consumo de drogas [83]. En definitiva, abarcaría todos los

[82] PABLO LUCAS MURILLO DE LA CUEVA, catedrático de Derecho Constitucional. Ver su ponencia sobre *La publicidad de los archivos judiciales y la confidencialidad de los datos sanitarios*, dentro del VII Congreso Nacional de Derecho Sanitario, organizado por la Asociación Española de Derecho Sanitario; Madrid, octubre de 2000. Ed. Fund. Mapfre Medicina, 2001 (pág. 81).

[83] V. Apartado 45 de la Memoria Explicativa del *Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal*, hecho en Estrasburgo y ratificado por España el 27 de enero de 1984. En dicho apartado se definen los datos de carácter personal relativos a la salud como *«las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo»*, pudiendo tratarse de informaciones sobre un individuo de

datos que de alguna forma se refieran a la salud tanto de individuos con buena salud, enfermos o fallecidos [84].

Igualmente, deben considerarse expresamente incluidos dentro del concepto de los datos de salud de las personas, los datos psicológicos y referentes a la salud mental [85], bien deriven expresamente de historiales médicos (de un determinado tratamiento psicológico o psiquiátrico), bien provengan de encuestas, y en este último supuesto por considerar que, en cualquier caso, se trata de datos referentes a la salud de las personas, que conciernen directamente a su salud mental o se encuentran estrechamente relacionados con esta última [86].

---

buena salud, enfermo o fallecido. Añade el citado apartado 45 que *«debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas»*.

Y también, *Recomendación R (97) 5, del Comité de Ministros del Consejo de Europa* a los Estados miembros relativa a la protección de los datos médicos, en la que se afirma que *«la expresión datos médicos hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como a las informaciones genéticas»*.

[84] Recomendación R (81) I, referida a la reglamentación aplicable a los bancos de datos médicos automatizados.

[85] La Recomendación R (91) 15, del Comité de Ministros del Consejo de Europa, en materia de estudios epidemiológicos en el ámbito de la salud mental, hace hincapié en la necesidad de establecer las garantías necesarias para la protección de los datos referentes a este tipo de trastornos.

[86] V. Memoria de 1999, de la Agencia de Protección de Datos (aptdo. 3.2.5.3 sobre *Naturaleza de los datos psicológicos a efectos de su tratamiento*).

Los datos de la salud tienen, además, la consideración de datos sujetos a un régimen especial de protección, de tal forma que no pueden tratarse automáticamente a menos que el derecho interno prevea garantías adecuadas [87].

Aunque fuera del ámbito europeo que aquí tratamos, resulta de interés también mencionar lo recogido al respecto por la ley de confidencialidad de los datos sanitarios estadounidense [88], que contempla un concepto de datos sanitarios muy amplio, que abarca incluso los aspectos económicos relacionados con la prestación de la asistencia sanitaria.

De esta forma, en la citada ley se definen los datos sanitarios como toda información, bien oral, bien grabada en cualquier forma o medio que haya sido creada o recibida por un proveedor de servicios de salud, plan de salud, autoridad pública de salud, empresario, compañía de seguros de vida, escuela o universidad, o entidad encargada del tratamiento de datos de salud; que se refiera a la salud física o mental, o a alguna circunstancia de la salud de una persona en el pasado, presente o futuro; a la provisión de cuidados de salud personales; o al pago de los servicios de salud

[87] V. Art. 8 de la *Directiva 95/46/CE 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*.

También art. 6 del citado Convenio 108 del Consejo de Europa.

[88] *Standards for Privacy of Individually Identifiable Health Information*, del *Department of Health and Human Service*, ley vigente en Estados Unidos de América desde primeros de 2001, y que puede consultarse en la página web siguiente: *http://aspe.hhs.gov/admnsimp/final/PvcPre01.htm.*

que hubiera realizado una persona en el pasado, que se lleve a cabo en el presente o vaya a realizarse en el futuro.

Siguiendo al magistrado COLLADO GARCÍA-LAJARA [89] puede distinguirse entre datos médicos y datos genéticos. Los primeros serían los que hacen referencia a todos los datos de carácter personal relativos a la salud de una persona, afectando igualmente a los datos manifiesta y estrechamente relacionados con la salud. Y los segundos, a los que nos referiremos expresamente más abajo, serían los datos de cualquier tipo relacionados con los caracteres hereditarios de un individuo o que, vinculados a los mismos, compongan el patrimonio de un grupo de individuos emparentados; y todos los datos relativos a intercambios de información genética (genes) de un individuo o línea genética, con relación a cualquier aspecto de la salud o de una enfermedad, constituyan o no un carácter identificable.

IV.3.2. **Estatus de los datos sanitarios en el ámbito europeo**

Conforme expone el *Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías* [90], en su dictamen para la Comisión

[89] ENRIQUE COLLADO GARCÍA-LAJARA, *Protección de datos de carácter personal (legislación, comentarios, concordancias y jurisprudencia)*, Ed. Comares. Granada 2000., pág. 25.

[90] Se trata de un organismo independiente formado por doce miembros que asesora al Consejo, Comisión y Parlamento europeos proporcionando dictámenes éticos a proyectos susceptibles de recibir financiación comunitaria.

Europea, de 30 de julio de 1999, bajo la rúbrica *Principios Éticos de la Sanidad en la Sociedad de la Información* [91], los datos sobre la salud personal afectan a la identidad y a la vida privada de los individuos y son, por ello, extremadamente sensibles. Consecuentemente, el estatus de estos datos está estrechamente ligado a su condición de elementos que conforman la personalidad, no debiendo ser tratados como meros objetos de transacción comercial.

Por este motivo, su recogida y proceso debe estar presidida por el principio de uso legítimo, en el sentido de que la recogida y manejo de los datos sobre la salud debe obedecer estrictamente al propósito legítimo que justifique su utilización (que será normalmente la protección de la salud), sin que en ningún caso terceras personas puedan tener acceso directo a los mismos.

[91] *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. Para este grupo los principios de la Convención Europea de Derechos Humanos, las reglas de la Convención del Consejo de Europa para la protección de los individuos con relación al tratamiento automatizado de datos personales y, especialmente, la Directiva Europea 95/46/EC, para la protección de los datos personales, son fuentes esenciales a tener en cuenta a la hora de tratar los aspectos éticos de la salud en la Sociedad de la Información.

Además, el Grupo de Expertos considera deseable la promulgación de una Directiva específica sobre protección de datos médicos, dentro del marco de la actual Directiva sobre protección de datos personales, para tratar las cuestiones particulares que se derivan del uso de datos sobre la salud en la Sociedad de la Información.

IV.3.2.1. *Valores en conflicto*

Ahondando sobre esta cuestión debe decirse que para el citado Grupo Europeo las innovaciones tecnológicas en la sanidad conllevan siempre una serie de valores en conflicto:

1. *Efectividad versus confidencialidad*: la necesidad de los profesionales de conocer y compartir los datos personales de la salud del paciente, en orden a procurarle unos cuidados de calidad, crea una situación de secreto compartido que puede comprometer la confidencialidad.

2. *Intimidad versus beneficio social (solidaridad)*: la preservación a ultranza de la intimidad puede estar enfrentada con ciertos beneficios colectivos (investigación, mejora de la administración y planificación, prevención, etc.) que favorecen a la larga a la comunidad.

3. *Control de calidad versus autonomía profesional*: algunos profesionales entienden que los controles de calidad (protocolos, guías clínicas, pautas clínicas, etc.) pueden a la postre restringir o disminuir la autonomía profesional.

4. *Eficiencia versus beneficiencia (hacer el bien)*: la beneficiencia indica que hay que dar el mejor cuidado posible a cada paciente, pero este objetivo puede resultar muy caro e irrealizable. En un contexto de recursos limitados, dar a unos pacientes cuidados muy caros podría privar a otros pacientes de cuidados mucho más básicos y necesa-

rios; el segundo mejor tratamiento puede ser, a veces, el más apropiado.

IV.3.2.2. *Principio Éticos*

Además, en este documento del citado Grupo Europeo se enuncian como principios éticos a tener en cuenta a la hora de hablar de los conflictos de valores citados [92]:

1. *Dignidad Humana*: como fundamento de las condiciones para la intimidad, confidencialidad y secreto médico.

2. *Autonomía*: como fundamento de las condiciones para la autodeterminación y participación.

3. *Justicia*: como fundamento de las condiciones para una distribución equitativa de recursos limitados.

4. *Beneficiencia y no maleficiencia*: como fundamento para procurar anticipar beneficios frente a riesgos previsibles.

5. *Solidaridad*: como fundamento del derecho de cada uno a la protección de su salud, con especial atención a los grupos más vulnerables de la sociedad.

92 Ver apartado 1.5.3 (*Ethical principles*), del documento referido.

La autonomía de los pacientes frente a la obtención de sus datos sobre la salud, la confidencialidad de estos últimos y la seguridad en la transmisión electrónica de los mismos de un sitio a otro, son cuestiones esenciales a la hora de tratar sobre el estatus de los datos sobre la salud, que el mencionado Grupo Europeo aborda con profusión.

IV.3.2.3. *La autonomía de los pacientes frente a la obtención de sus datos sobre la salud*

En el dictamen aludido del Grupo Europeo de Ética se enuncian cuatro principios a tener en cuenta en materia de autonomía de las personas con respecto a los datos sobre su salud [93]:

1.—*Prioridad de la obtención a través del propio interesado.* Siempre que resulte posible los datos sobre la salud de los ciudadanos deben obtenerse directamente de estos últimos.

2.—*Control de los datos por el afectado*. La autonomía incluye el derecho de los ciudadanos a conocer y a determinar qué datos personales sobre su salud se van a recoger y registrar, y a conocer quién los va a utilizar y para qué propósitos, y también su derecho a que se corrijan los citados datos cuando sea necesario.

[93] Ver apartado 2.3 (*Self-determination*), del mismo documento.

3.—*Derecho de oposición al uso de datos personales*. Los ciudadanos tienen derecho a oponerse al uso de sus datos para otras finalidades no establecidas por ley.

4.—*Necesidad de justificar los usos sociales de los datos*. El uso de los datos personales sobre la salud para finalidades que puedan beneficiar al conjunto de la sociedad debe estar justificado en el contexto de los derechos que se acaban de referir más arriba.

IV.3.2.4. *Confidencialidad de los datos sobre la salud*

El Convenio de Oviedo de 1.997 [94], relativo a los derechos humanos y la biomedicina, proclama el derecho de toda persona a que se respete su vida privada cuando se trate de informaciones relativas a la salud.

Asimismo, con relación al problema de la confidencialidad de los datos sobre la salud, el *Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías* en su mencionado dictamen establece los siguientes postulados [95]:

1.—*Consentimiento Informado.* El respeto a la vida privada, como Derecho Humano, requiere que la confidencialidad de los

[94] V. Art. 10.1, del citado Convenio, de aplicación directa en España desde el primero de enero de 2000 (publicado el Instrumento de ratificación en el B.O.E. núm. 251, de 20 de octubre de 1999).

[95] Ver apartado 2.2 (*Confidenciality/privacy*), del documento referido.

datos sobre la salud personal esté garantizada en todo momento. Esto conlleva también que, en principio, es obligado obtener el consentimiento informado del paciente para la recogida y cesión de dichos datos.

2.—*Fijación de límites de acceso a la información*. La obtención y acceso a los datos sobre la salud personal está restringida a los facultativos que realizan el tratamiento medico y a aquellas terceras personas (facultativos que no realizan el tratamiento, personal sanitario y social, personal de administración, etc.) que puedan demostrar un uso legítimo.

3.—*Ámbito, extensión e importancia del secreto médico*. Todos los usuarios legítimos de los datos personales sobre la salud tienen una obligación de confidencialidad equivalente a la obligación profesional del secreto médico. Las excepciones a esta obligación deben limitarse y establecerse por normas legales.

El secreto médico es una cuestión central para la confianza y estimación del sistema de salud, no sólo para el interés particular de cada persona. La confianza es un valor ético fundamental por si mismo.

Asimismo, no debe olvidarse que el respeto por la confidencialidad de los datos sobre la salud continúa después de la muerte de la persona afectada.

Por otro lado, debe significarse que como consecuencia de la

incidencia de la Directiva europea sobre protección de datos [96], se ha producido una ampliación de los sujetos tradicionales con obligación de confidencialidad en el campo de los datos sobre la salud, en cuanto que dicha obligación se hace recaer en cualquier persona física o jurídica que tenga acceso a la información del paciente. En consecuencia, además de afectar al médico y a las personas de su equipo, tanto sanitarios como personal de administración, incumbirá también al responsable y/o encargado del tratamiento de los datos, y al proveedor del servicio de telecomunicaciones que comparte la información.

IV.3.2.5. *La seguridad en la transmisión de los datos sobre la salud*

Como indicábamos al principio, al abordar el *Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías* el estatus de los datos sanitarios, hacía hincapié en su condición de elementos de la personalidad del individuo, descartando que pudieran ser tratados como meros objetos de transacción comercial.

Pues bien, la citada naturaleza de los datos sobre la salud conlleva realizar importantes esfuerzos en materia de seguridad para evitar que los mismos puedan utilizarse indebidamente. En este

[96] Directiva 95/46/CE del Parlamento Europeo 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 (Traspuesta a nuestro derecho interno en virtud de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal).

sentido, el dictamen del Grupo referido manifiesta al respecto lo siguiente [97]:

1.—*La seguridad como imperativo ético*. La seguridad en la información y en las comunicaciones por medios telemáticos, por lo que se refiere a los datos sobre la salud, es un imperativo ético para garantizar el respeto a los derechos humanos y libertades del individuo, en particular la confidencialidad de sus datos y su confianza en la utilización para fines médicos de los citados sistemas de información y comunicación.

2.—*Encriptación y redes cerradas*. El respeto a la seguridad requiere el uso de tecnología de encriptación apropiada, el empleo de redes cerradas para la transmisión de los datos personales de la salud y medidas organizativas para mantener la seguridad [98].

3.—*Respeto a los estándares de seguridad europea*. Debido a la importancia de la seguridad de los datos personales sobre la salud, los estándares de seguridad europea deberían observarse en cualquier lugar en donde se pudiera producir una transferencia electrónica de datos identificables.

[97] Ver apartado 2.6 (*Security*).

[98] Como indica el prof. Dr. ALAIN POMPIDOU (miembro del Parlamento Europeo y Presidente del Gabinete Asesor de las Opciones Científicas y Tecnológicas), cuando viaja por la red la información del paciente, ésta debe mantenerse en el anonimato debiéndose asegurar los mecanismos necesarios para tal fin, incluyendo la encriptación. V. prólogo de la obra *«Telemedicina»* de OLGA FERRER-ROCA; ob. cit. Mayo 2001 (págs V y VI).

4.—*Control de los sistemas de información*. Si consideramos que la medicina es un campo ético seguro, los sistemas de información y comunicación por medios telemáticos deben ser rigurosamente controlados.

Como afirma PETRA WILSON [99], cuando el médico utiliza herramientas telemáticas, tiene que asegurar al paciente que el medio que emplea o por el que transmite a otro la información sobre el tratamiento es seguro frente a quienes pudieran desear interceptar la comunicación.

Sobre esta cuestión la mencionada autora PETRA WILSON [100] considera que resulta de especial utilidad el mecanismo de la firma electrónica, en cuanto herramienta adecuada para asegurar la confidencialidad, integridad y autenticidad en la transmisión de los datos sobre la salud, que permite además verificar la autoría del documento que se transmite y que dicho documento no ha sido alterado.

La firma electrónica es un mecanismo para conseguir, en redes informáticas abiertas, la seguridad de la identidad del sujeto que emite un mensaje y la integridad del contenido del mismo (es decir, que éste no ha sido modificado) [101].

[99] PETRA WILSON. *An overview of legal issues in European Telemedicine*. ob. Cit. Octubre 1998 (pág. 3).

[100] *Ibídem* (pág. 4).

[101] V. Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

IV.3.2.5. **Los datos genéticos**

Dentro de los datos sobre la salud de las personas, los datos genéticos son objeto de una especial protección en cuanto consisten en informaciones muy específicas no solo respecto del individuo en cuestión objeto de examen, sino también sobre los miembros de su familia consanguínea. Esta circunstancia les hace susceptibles de generar importantes repercusiones en el estilo de vida de los individuos e, incluso, de poder condicionar sus opciones reproductivas [102].

Conscientes de esta especial sensibilidad de los datos genéticos y en aras de su mejor protección, se promulgó la *Declaración Universal sobre el Genoma y Derechos Humanos* de la UNESCO [103], por la que se prohíbe toda discriminación por ra-

[102] Ver «considerandos» de la *Propuesta de Resolución del Parlamento Europeo sobre las repercusiones sociales, jurídicas, éticas y económicas de la genética humana*, de 24 de julio de 2001, elaborada por la *Comisión Temporal sobre Genética Humana y Otras Nuevas Tecnologías de la Medicina Moderna*. Esta Propuesta se muestra de acuerdo con el dictamen comentado del Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías, en el sentido de que se elabore una Directiva específica en materia de protección de los datos personales sobre la salud. En el apartado 19 de la Propuesta de Resolución se afirma que dicha propuesta no debe limitarse a la enunciación de principios generales extraídos del conjunto de derechos fundamentales, sino que debe establecer los mecanismos de identificación, clasificación y control de los análisis genéticos de forma suficiente para evitar su utilización abusiva, impidiendo que puedan favorecer la aparición de criterios inquietantes de *«normalidad genética»*.

[103] Aprobada por la XXIX Comisión de la Conferencia General de la UNESCO, en París, el 11 de noviembre de 1997.

zones genéticas y se establece la obligación de proteger la confidencialidad de los datos genéticos asociados a una persona identificable [104].

En igual sentido de prohibir cualquier discriminación por razones genéticas se pronuncian también la *Carta de los Derechos Fundamentales de la Unión Europea* [105] y el *Convenio de Oviedo sobre los Derechos Humanos y la Biomedicina* [106], donde se limita muy claramente la posibilidad de realizar prospecciones genéticas de individuos a supuestos que tengan que ver con la protección de la salud de las personas o con la investigación médica [107].

La utilización de la información genética personal y el acceso a la misma por parte de terceros debe basarse en la protección de la integridad personal del individuo, es decir, en exigencias efectivas de protección de su salud, excluyendo cualquier otra finalidad como pudiera ser la evaluación de un individuo en el marco de un contrato de trabajo o de seguros [108].

[104] V. Art. 7 de la citada Declaración donde se dice que *«Se deberá proteger en las condiciones estipuladas por ley la confidencialidad de los datos genéticos asociados con una persona identificable, conservados o tratados con fines de investigación o cualquier otra finalidad»*.

[105] V. Arts. 8 y 21 de este documento.

[106] V. Arts. 11, 12 y 13 del Convenio.

[107] El art. 12 del Convenio establece que *«Sólo 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»*.

[108] Ver apartado 17 de la citada Propuesta de Resolución del Parlamento

De igual forma, cualquier regulación sobre el uso y acceso a la información genética (para la salud o investigación médica) debe fundamentarse en la previa necesidad de obtener el consentimiento del afectado, aunque no exclusivamente en este requisito, debido a que en situación de paro laboral, es conocida la predisposición a aceptar cualquier tipo de condición para obtener un empleo, pudiéndose convertir en este caso el consentimiento en el efecto de una necesidad material y no en una manifestación de libertad. Por esta razón, se hace preciso promover políticas institucionales de información y concienciación de la opinión pública sobre todo lo referente al uso de la información genética y, además, establecer políticas generales de control social [109].

Asimismo, se debe restringir al máximo la posibilidad de recurrir a los datos genéticos para realizar evaluaciones prospectivas de las personas, ya que, por ejemplo, reducir las posibilidades de cualquier persona para contratar un seguro de vida o enfermedad podría dar lugar a una organización social que clasificara a los in-

---

Europeo, y también apartado 22 del mismo texto donde se dice que *«… las compañías de seguros no deben tener derecho a pedir, antes o después de la negociación de un contrato de seguro, que se lleve a cabo un análisis genético ni a que se comuniquen los resultados de los análisis genéticos ya efectuados; … los análisis genéticos no deben convertirse en una condición previa a la negociación de un contrato de seguro y … las compañías de seguros no pueden pretender que se les informe acerca de los datos genéticos que conozca el asegurado»*.

[109] V. Apartado 25 de la citada Propuesta. En el apartado 27 se indica que no pueden aceptarse políticas de apropiación privada de datos genéticos aunque vayan acompañadas de garantías formales de protección de los derechos de las personas merced al carácter anónimo de los datos.

dividuos en función de su predisposición genética, estableciendo jerarquías sociales con arreglo a dicho criterio, lo que a la postre supondría una reducción de la ciudadanía y la negación del derecho fundamental a la salud [110].

En definitiva, debe hacerse todo lo posible desde los Estados para proteger el *secreto genético*, garantizando que, cuando se realice un análisis genético, los resultados se utilicen con fines benéficos, tanto para los pacientes considerados individualmente, como para la sociedad en su conjunto [111].

Como dice ÁLVAREZ-CIENFUEGOS, la enorme potencialidad descriptiva de la genética respecto de eventuales comportamientos de futuro en un determinado grupo de personas hace que el derecho al *secreto genético*, hoy día incorporado masivamente a soportes informáticos, sea un bien codiciado desde la perspectiva de empresas de negocios, compañías aseguradoras, entidades de colocación, y desde las mismas Administraciones públicas. Por esta razón, el citado autor manifiesta que el uso de la información genética fuera de la estricta finalidad asistencial puede plantear en

[110] V. Apartado 21 del mismo texto en el que se dice que las citadas evaluaciones genéticas ofrecen representaciones distorsionadas de las personas en cuanto ignoran la relación decisiva de los datos genéticos con las proteínas y el entorno.

[111] V. Apartado 27 de la Propuesta donde se admite la posibilidad de excepcionar el principio general del secreto genético en los casos de utilización de las huellas digitales genéticas, conservadas en los bancos de datos de ADN, para identificar y capturar delincuentes.

un futuro inmediato problemas éticos y jurídicos de extraordinaria complejidad [112].

Por último, debemos aludir, aunque sea brevemente, a la Directiva europea relativa a la protección jurídica de las invenciones biotecnológicas, en la que, respecto a los datos genéticos, se dice que el simple descubrimiento de la secuencia completa o parcial de un gen no puede constituir una invención patentable [113].

No obstante, como también se indica en la citada directiva y tiene manifestado el Tribunal de Justicia de las Comunidades Europeas, sí será posible solicitar una patente para aquellas invenciones que asocien un elemento natural (por ejemplo, la secuencia de un gen) a un procedimiento técnico que permita aislarlo o producirlo con miras a su aplicación industrial [114].

[112] JOSÉ MARÍA ÁLVAREZ-CIENFUEGOS SUÁREZ. *La aplicación de la firma electrónica y la protección de datos relativos a la salud*. Revista *Actualidad Informática Aranzadi*, dirigida por MIGUEL ÁNGEL DAVARA, núm. 39, abril de 2001 (págs. 4 y 5). Manifiesta también el citado autor que *«El almacenamiento y manejo institucional —sea o no en el sistema público de salud— de millones de datos genéticos relativos a un gran número de ciudadanos constituye hoy día una amenaza que se ve incrementada por la facilidad de su transmisión a través de sistemas electrónicos»*.

[113] V. Art. 5, de la *Directiva 98/44/CE del Parlamento Europeo y del Consejo, de 6 de julio de 1998, relativa a la protección jurídica de las invenciones biotecnológicas*.

[114] *Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 9 de octubre de 2001* (asunto C-377/98), que avala la directiva anterior. En el apartado 74 se dice lo siguiente: *«Esta distinción se aplica a las investigaciones relativas a la secuencia o a la secuencia parcial de genes humanos. El resultado de dichas investigaciones sólo puede dar lugar a la concesión de una*

IV.4. LA PROTECCIÓN DE LOS DATOS SOBRE LA SALUD EN EL DERECHO ESPAÑOL

No existe actualmente en el Derecho Español una norma sanitaria específica que aborde las peculiaridades del tratamiento automatizado de los datos sobre la salud, por lo que se hace necesario acudir directamente a la propia Constitución [115] y a diversas disposiciones contenidas en las normas generales sobre tratamiento automatizado de datos personales, fundamentalmente a la ley sobre protección de datos personales [116] y al reglamento de medidas de seguridad [117].

---

patente si la solicitud va acompañada, por un lado, de una descripción del método original de secuenciación que ha hecho posible la invención y, por otro lado, de una memoria sobre la aplicación industrial que se dará a dichas investigaciones, tal como precisa el artículo 5, apartado 3, de la Directiva. Si no existe dicha aplicación, no se trata de una invención, sino del descubrimiento de una secuencia de ADN que, como tal, no es patentable».

Continua el Tribunal en el apartado 75 siguiente: *«De esta forma, la protección contemplada en la Directiva se refiere al resultado de una actividad inventiva de carácter científico o técnico y se extiende a los datos biológicos que existan en estado natural en el ser humano en la medida necesaria para obtener y explotar una determinada aplicación industrial».*

[115] V. Art. 18.4 de la Constitución Española anteriormente citado.

[116] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

[117] 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.

Otras normas de interés son el Real Decreto 1.332/1994, de 20 de junio; el Real Decreto Ley 14/1999, del 17 de septiembre, de firma electrónica y la Orden Ministerial del Ministerio de Fomento, de 21 de febrero de 2000, por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

Dentro de las leyes sanitarias genéricas podríamos destacar quizás el precepto de la ley general de sanidad [118] que establece que todos tienen derecho a la confidencialidad de toda la información relacionada con su proceso y con su estancia en las instituciones sanitarias públicas y privadas que colaboren con el sistema público; y también aquél que prescribe que las Administraciones Sanitarias, para la consecución de sus objetivos relacionados con la salud individual y colectiva, y de acuerdo con sus competencias, crearán los registros y elaborarán los análisis de información necesarios para el conocimiento de las distintas situaciones de las que puedan derivarse acciones de intervención de la autoridad sanitaria [119]. Finalmente, puede citarse el precepto del Convenio de Oviedo de 1.997 [120], relativo a los derechos humanos y la biomedicina, que proclama el derecho de toda persona a que se respete su vida privada cuando se trate de informaciones relativas a su salud.

[118] V. Art. 10.3 de la Ley 14/1986, de 25 de abril, General de Sanidad.

[119] Art. 23 de la misma ley.

Igualmente, puede citarse el art. 1 de la Ley Orgánica 3/1986, de 14 de abril, sobre Medidas Especiales en materia de salud pública, donde se prevé que, al objeto de proteger la salud pública y prevenir su pérdida o deterioro, las autoridades sanitarias de las distintas Administraciones Públicas podrán, dentro del ámbito de sus competencias, adoptar las medidas previstas en la Ley cuando así lo exijan razones sanitarias de urgencia o necesidad (reconocimiento, tratamiento, hospitalización o control de enfermos).

[120] V. Art. 10.1 del citado Convenio, de aplicación directa en España desde el primero de enero de 2000 (publicado el Instrumento de ratificación en el B.O.E. núm. 251, de 20 de octubre de 1999).

IV.4.1. **Principios básicos de la ley de protección de datos (LOPD) aplicados al mundo sanitario** [121]

Como establece esta norma en su primer artículo, la misma tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.

El objeto de aplicación de la ley está constituido por los datos de carácter personal registrados en soporte físico (no necesariamente en ficheros automatizados) que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado [122].

[121] La ley Orgánica 15/1999 (en adelante LOPD), es la trasposición a nuestro derecho de la Directiva 95/46/CEE, sobre protección de datos y libre circulación de los mismos y tiene su antecedente inmediato en la Ley Orgánica 5/1992 sobre la regulación del tratamiento automatizado de datos de carácter personal (conocida como LORTAD).

[122] V. Art. 2.1 de la LOPD y 2.2.a) donde se excluye de la aplicación de la ley a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. Respecto a los ficheros manuales, como es el caso de la mayoría de las historias clínicas, debe tenerse en cuenta que la Disposición adicional primera de la ley confiere un plazo de 12 años a contar desde el 24 de octubre de 1995 (es decir, hasta el 24 de octubre de 2007) para su adecuación a la citada norma (deberán automatizarse), sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Ver también, MAR MARTÍNEZ SÁNCHEZ (Subdirectora Registro General Protección de Datos), en su ponencia *La Ley Orgánica 15/1999, de 13 de diciembre y la inscripción de ficheros (archivos del profesional sanitario)*, expuesta en el *VII Congreso Nacional de Derecho Sanitario*, celebrado en Madrid, en octubre de 2000. La citada autora manifiesta que estarían excluidos de los principios

Se prevén igualmente mecanismos de protección frente a las actuaciones contrarias a la ley, que pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos [123], sin perjuicio del derecho de aquellos a percibir una indemnización en los casos en que el incumplimiento de la ley les hubiera originado daño o lesión en sus bienes o derechos [124].

La ley contiene una serie de principios básicos que determinan una correcta protección de datos y constituyen al mismo tiempo una garantía de los ciudadanos.

Los citados principios pueden estructurarse de la siguiente forma [125]:

IV.4.1.1. *Principio de información en la recogida de los datos* [126]

El titular del fichero tiene la obligación de informar al afectado cuando se recaban los datos, de manera tal que este último

---

de protección de la Ley el tratamiento de datos efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, como por ejemplo la correspondencia y la llevanza de un repertorio de direcciones. Ed. Fund. Mapfre Medicina, 2001 (pág. 92).

123 Art. 18 LOPD.

124 Art. 19 LOPD.

125 V. *Cuaderno sobre protección de datos*, suplemento julio 2001 de la revista OTROSÍ, editada por el Ilustre Colegio de Abogados de Madrid.

126 V. Art. 5 de la norma referida.

En sintonía con este precepto, la *Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid*, en su art. 6, y bajo

pueda conocer esencialmente quién, cómo y para qué se tratan sus datos [127].

De forma expresa debe informar de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición [128].

Persiste también el derecho de información a favor del interesado aún en el caso de que sus datos no se obtengan directamente de él, salvo en los supuestos en que una ley prevea lo contrario [129].

---

la rúbrica *Derecho de información en la recogida de datos de carácter personal*, dice lo siguiente: *«Los interesados cuyos datos personales sean objeto de tratamiento deberán ser previamente informados de modo expreso, preciso e inequívoco de los extremos señalados en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, en la forma y condiciones establecidas en ese mismo artículo»*.

[127] Esto supone que el interesado debe ser informado con carácter previo al tratamiento de sus datos y de modo expreso, preciso e inequívoco de los siguientes extremos (art. 5.1 LOPD):

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

[128] V. Apartado d), del citado art. 5.1 de la LOPD.

[129] Conforme previene el art. 5.4 de la LOPD, si los datos no se recaban directamente del propio interesado, y salvo que la ley disponga otra cosa o hubiera sido informado con anterioridad, aquél deberá ser informado de la misma

IV.4.1.2. *Principio de consentimiento del interesado* [130]

La norma general en materia de protección de datos es que debe obtenerse el consentimiento inequívoco del afectado para que se recojan sus datos, salvo en casos excepcionales previstos en la ley [131].

Debe significarse, además, que el consentimiento puede ser revocado, siempre que exista una causa que lo justifique y siempre que no se atribuyan efectos retroactivos a dicha revocación [132].

---

forma que en el caso anterior (y dentro del plazo de los tres meses siguientes a la recogida de los datos) de los siguientes extremos:

a) Del contenido del tratamiento.

b) De la procedencia de los datos.

c) De lo indicado en las letras a), d) y e) del aptdo. 5.1.

[130] V. Art. 6 de la citada LOPD.

[131] El art. 6.1 de la LOPD establece la excepción consistente en que una ley disponga otra cosa; y el art. 6.2 del mismo texto legal indica lo siguiente: *«No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para proteger un interés vital del interesado en los términos de artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles a público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado».*

[132] V. Art. 6.3 de la LOPD.

Por lo que se refiere a los datos sobre la salud, para analizar la necesidad de recabar el consentimiento del paciente deben distinguirse dos supuestos:

IV.4.1.2.1. *Obtención y tratamiento de los datos sobre la salud*

Con relación a estos datos la ley exige que el afectado consienta expresamente el hecho de que los mismos puedan ser recabados, tratados y cedidos, salvo que, por razones de interés general, lo disponga una ley [133]. Pero, además, la norma contempla otras dos excepciones a la exigencia del consentimiento en el caso de los datos sanitarios, que son las siguientes:

- Se permite el tratamiento de los citados datos cuando el mismo 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 [134].

[133] V. Art. 7.3 de la citada ley.

[134] V. Art. 7.6 de mismo texto legal. Con relación a los incapaces se dice también en el párrafo segundo de este apartado lo siguiente: *«También podrán ser objeto de tratamiento los datos a 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»*.

- La segunda excepción deriva de la necesidad de habilitar a las Administraciones públicas en el correcto ejercicio de sus funciones y competencias [135], pero también a los centros sanitarios privados, pues la citada excepción del consentimiento afecta tanto a las Instituciones y centros sanitarios públicos como a los privados y a los profesionales correspondientes, que podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratadas en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad [136].

En estos dos casos comentados podría entenderse que basta el consentimiento previo que se deriva, expresa o tácitamente, de la relación de los usuarios con los centros sanitarios y profesionales, para admitir también el tratamiento de los datos de esos usuarios o pacientes sin necesidad de que presten un consentimiento aparte y específico al respecto [137].

[135] V. Art. 6.2 de la LOPD.

[136] V. Art. 8 de la LOPD y 23 y concordantes de la Ley General de Sanidad. El art. 8 de la Ley Orgánica de protección de datos de carácter personal dice lo siguiente: *«Datos relativos a la salud. Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, 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 tratadas en los mismos de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad»*.

[137] Como indica JAVIER SÁNCHEZ-CARO *«... el tratamiento de los datos parte ya de una relación constituida en la que es excepcional no contar con la voluntad de los interesados»*. Exceptúanse situaciones tales como la urgencia o

No obstante lo anterior, la citada interpretación no es en absoluto pacífica ya que hay algunos autores que discrepan de la misma al considerar que sí es preciso recabar el consentimiento del paciente para la obtención de sus datos. Entre estos últimos se encuentra VIZCAÍNO CALDERÓN, quien considera que la excepción del consentimiento referida la permite la LOPD respecto del tratamiento en sí de los datos, pero no respecto de la fase inicial previa que sería la recogida de los mismos, para la que el citado autor piensa que debe seguirse la norma general del consentimiento expreso del afectado [138].

---

la incapacidad, que están previstas legalmente en el artículo 10 de la Ley General de Sanidad. V. Artículo *Ley de Protección de Datos e innovaciones tecnológicas farmacéuticas*. *Revista de Administración Sanitaria*, julio-septiembre 2001. Ob. cit. (pág. 139).

V. también del mismo autor y de JESÚS SÁNCHEZ-CARO, *El Médico y la Intimidad*, Editorial Díaz de Santos, Madrid, julio 2001 (págs. 136 y 137).

[138] MIGUEL VIZCAÍNO CALDERÓN. *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*. Ed. Cívitas, Primera Edición, 2001 (págs. 134 a 138). El citado autor considera que la excepción del consentimiento del referido art. 8 de la LOPD habilita para el tratamiento cuando dice *«… podrán proceder al tratamiento…»*, pero que dicho precepto no se pronuncia sin embargo respecto de la recogida de los datos, sin que, a su juicio, pueda comprender la expresión «tratamiento» la de «recogida»; todo ello sin perjuicio de reconocer la confusión de la Ley a la hora de perfilar las fronteras entre ambos conceptos.

No obstante, frente al planteamiento de este autor, debe recordarse que en el apartado c) del artículo 3 de la LOPD, se define el tratamiento de datos como *«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»*. Es decir, se incluye expresamente la «recogida» como actividad comprendida dentro del concepto de tratamiento.

IV.4.1.2.2. *La cesión o comunicación de datos sobre la salud a tercero*

Para la cesión de datos la LOPD contempla dos requisitos [139]: el primero, que la cesión lo sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario; y el segundo, que se obtenga el previo consentimiento del interesado.

El primero de los requisitos no admite excepciones, pero el segundo sí, y entre las mismas se encuentra expresamente contemplado el caso de los datos relativos a la salud respecto de los que la ley indica que no será preciso el consentimiento para la cesión de los mismos a terceros cuando dicha cesión sea necesaria para solucionar una urgencia médica o para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica [140].

Esta remisión legislativa de la citada norma, a juicio del magistrado ÁLVAREZ-CIENFUEGOS SUÁREZ, constituye una clara insuficiencia de la LOPD para contemplar las crecientes y complejas garantías que exige el tratamiento de los datos relativos a la salud de los ciudadanos mediante sistemas electrónicos, razón por la que

[139] Art. 11.1 LOPD.

[140] V. Art. 11.2, f) LOPD, que exime de la prestación 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»*.

dicho autor se muestra partidario de la urgente publicación de una norma específica que contemple, junto a los datos incorporados a las historias clínicas tradicionales, el tratamiento de otros datos relativos a la salud derivados de la investigación genética, de los avances de la biotecnología y de la clonación terapéutica [141].

Por otro lado, la ley establece que no se considerará comunicación de datos el acceso de un tercero (encargado del tratamiento) a los mismos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento [142]. Como indica ALBERTO ANDÉREZ GONZÁLEZ [143] la afirmación contenida en este precepto constituye en realidad una habilitación para la posible contratación externa del tratamiento de datos de carácter personal, sin necesidad de consentimiento del afectado. No obstante, conviene recordar que esta posibilidad queda sometida por la ley a las siguientes condiciones formales [144]:

[141] JOSÉ MARÍA ÁLVAREZ-CIENFUEGOS SUÁREZ. *La aplicación de la firma electrónica y la protección de datos relativos a la salud*. ob. cit. (pág. 4).

[142] V. Art. 12.1 de la LOPD. Asimismo, conviene recordar las definiciones de responsable del fichero y de encargado del tratamiento, que incluye la ley en su artículo 3. De esta forma, el «*responsable del fichero*» es la «*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*». Por su parte, el «*encargado del tratamiento*» es «*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*».

[143] ALBERTO ANDÉREZ GONZÁLEZ; *Informe Seis – La Seguridad y confidencialidad de la información clínica.* capítulo *Aspectos legales de la seguridad y confidencialidad en la información clínica*. Sociedad Española de Información de la Salud. ob. cit.; Pamplona, 2000, pág. 169 y 170.

[144] V. Art. 12, apartados 2 y 3, de la LOPD.

- Constancia en contrato escrito o en alguna otra forma que permita acreditar su celebración y contenido.
- Necesidad de pactar expresamente determinadas obligaciones del encargado del tratamiento. Este último no podrá aplicar o utilizar los datos con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
- Estipulación en el contrato del compromiso de adoptar las medidas de seguridad previstas legalmente.
- Obligación de destrucción o devolución de los datos al responsable del tratamiento una vez cumplida la prestación contractual.

IV.4.1.2.3. *Principio de calidad de los datos*

Es condición para que puedan recogerse datos de carácter personal el que los mismos resulten adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido [145].

La ley determina también que los datos deben ser exactos y puestos al día, de forma que respondan con veracidad a la situación actual de interesado, asociando su conservación a la necesidad de su tratamiento en virtud de la finalidad para la que se recabaron, ya que cuando hayan dejado de ser necesarios o pertinentes deberán ser cancelados [146].

[145] V. Art. 4 de la misma ley.

[146] No obstante, en el ámbito sanitario la cancelación de los datos sanita-

En el ámbito sanitario conviene recordar que la historia clínica, sea manual o electrónica, tiene su razón de ser en facilitar la asistencia sanitaria al ciudadano y que, por tanto, la naturaleza de la información que se incluye en la misma ha de ser acorde con el citado objetivo, debiéndose recoger exclusivamente toda la información clínica necesaria para asegurar, bajo un criterio médico, el conocimiento veraz, exacto y actualizado del estado de salud del paciente, por parte de los sanitarios que le atienden [147].

IV.4.1.2.4. *Principio de datos especialmente protegidos*

La ley incluye dentro de esta categoría a los datos relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual [148].

Respecto de los datos sanitarios este régimen de especial protección se concreta, básicamente, en que los mismos sólo podrán ser recabados, tratados y cedidos en los términos que se han de-

---

rios no está exenta de algunos inconvenientes derivados de la necesidad de conservar información para poder realizar estudios epidemiológicos y de salud pública. En este sentido, en el párrafo tercero del apartado 5, del artículo 4 de la LOPD, se dice lo siguiente: *«Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos»*.

147 V. JAVIER SÁNCHEZ-CARO y FERNANDO ABELLÁN. *La Historia Clínica*. Fundación Salud 2000, mayo 2000 (págs. 11 y 12).

148 V. Art. 7 de la LOPD.

jado referidos anteriormente a la hora de tratar sobre el principio de consentimiento. Y también en el hecho de que los citados datos son merecedores de la adopción de medidas técnicas de seguridad de nivel elevado, de las que se trata más adelante.

IV.4.2. **Derechos básicos de los ciudadanos en materia de protección de datos sobre la salud** [149]

IV.4.2.1. *El derecho de acceso a la información clínica*

Al objeto de que los ciudadanos puedan conocer en todo momento la información que sobre los mismos se haya podido recabar, e incluso conseguir que se rectifique o cancele, en su caso, la LOPD configura una serie de derechos, independientes entre sí [150].

[149] Como se indica en el trabajo *Cuaderno sobre protección de datos* (suplemento julio 2001 de la revista *otrosí*), anteriormente citado (pág. 7), el ejercicio de derechos viene regulado en el Título III de la LOPD, en el capítulo IV del Real Decreto 1.332/1994, de 20 de junio, por el que se desarrollan algunos aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos Personales (subsistente en virtud de la Disposición transitoria tercera de la LOPD, en tanto no se oponga a lo dispuesto en aquélla). También son de interés (si bien han de entenderse derogadas, pero son importantes porque marcan la línea interpretativa de la Agencia de Protección de Datos) las normas 1.ª y siguientes 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.

[150] En el mismo trabajo citado se recuerda que el correcto ejercicio de los derechos de los interesados, cuyos datos sean objeto de tratamiento por parte del

El primero de los citados derechos es el de acceso, que en terminología de la LOPD consiste en el derecho del interesado a solicitar y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, así como sobre el origen de dichos datos, y de las comunicaciones realizadas o que se prevén hacer de los mismos [151].

---

responsable del fichero, requiere del cumplimiento de una serie de requisitos formales, como es el envío por el interesado de una solicitud dirigida al responsable del fichero que contenga los siguientes aspectos (*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. Norma primera, apartado 3)*:

• Nombre y apellidos del interesado, a efectos de su identificación.

• Una fotocopia del DNI (o cualquier otro medio admitido en derecho) que acredite su identidad.

• En los casos en que excepcionalmente se admita, supuestos de incapacidad legal o minoría de edad, deberá proporcionarse los datos anteriormente indicados de la persona que represente legalmente al interesado.

• Petición en que se concreta la solicitud.

• Indicación de un domicilio a efectos de notificaciones.

• Fecha y firma del interesado.

• Documentos acreditativos de la petición que formula, en su caso.

El ejercicio de estos derechos no comportará ningún gasto para el interesado, es decir, se ejercerán de forma gratuita, sin que el responsable del fichero pueda, en principio, solicitar contraprestación alguna.

El responsable del tratamiento deberá contestar al interesado tanto en los casos en que consten datos del solicitante en el fichero como si no fuera así, debiendo solicitar la subsanación de los requisitos formales de la solicitud en caso de inexactitud.

[151] V. Art. 15.1 de la LOPD. En el apartado 3 de este mismo precepto se indica que *«el derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes»*.

Ahora bien, en el ámbito sanitario cuando hablamos del derecho de acceso a los datos personales nos estamos refiriendo a un tipo de información peculiar como es la información clínica, donde la regla general es que la asistencia sanitaria prestada a un ciudadano es la única razón que justifica el acceso a la misma. Cualquier otra razón de acceso a la información debe responder a un interés legítimo susceptible de protección y estar convenientemente motivada [152].

Apostando por este carácter restrictivo del acceso a la información clínica, la ley general de sanidad de 1986 establece que la historia clínica estará a disposición de los enfermos y de los facultativos que directamente estén implicados en el diagnóstico y el tratamiento del enfermo, así como a efectos de inspección médica o para fines científicos, debiendo quedar plenamente garantizado 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 [153].

Por lo que se refiere al acceso a la información clínica por los profesionales médicos, debe partirse de que la citada LOPD sienta la norma de que el tratamiento de los datos relativos a la salud habrá de realizarse por un profesional sanitario sujeto a secreto

[152] V. JAVIER SÁNCHEZ-CARO y FERNANDO ABELLÁN. *La Historia Clínica*. ob. cit. (págs. 41 a 59).

[153] V. Art. 61 de la Ley 14/1986, de 25 de abril, General de Sanidad, donde además se dice que *«los poderes públicos adoptarán las medidas precisas para garantizar dichos derechos y deberes»*.

profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto [154].

No obstante, como afirma ANDÉREZ GONZÁLEZ [155] esta última mención no está exenta de algunas dudas interpretativas pues es difícil determinar quiénes son esas otras personas con obligación de secreto equivalente a la de los profesionales sanitarios, ya que en el Derecho español no es pacífica la cuestión relativa a respecto de qué actividades cabe afirmar un deber secreto profesional en sentido estricto [156]. En cualquier caso, para el citado autor parece

[154] V. Art. 7.6 de la LOPD y, también, art. 10.3 de la citada Ley General de Sanidad en el que se indica que todos tienen derecho a la confidencialidad de toda la información relacionada con su proceso y con su estancia en las instituciones sanitarias.

[155] ALBERTO ANDÉREZ GONZÁLEZ. *Informe Seis–La Seguridad y confidencialidad de la información clínica.* capítulo *Aspectos legales de la seguridad y confidencialidad en la información clínica*. Sociedad Española de Información de la Salud. ob. cit.; Pamplona, 2000, pág. 167 y 168.

Para el magistrado JOSÉ MARÍA ÁLVAREZ-CIENFUEGOS SUÁREZ, falta en nuestro ordenamiento una norma con rango de Ley que regule el secreto profesional en el ámbito médico. El citado autor considera que la mención que se hace al mismo en la Ley General de Sanidad implica un reconocimiento de carácter asistencial pero se hace preciso una regulación del secreto médico desde la perspectiva de garantía de los pacientes. *II Master en Derecho Sanitario*. Universidad Complutense de Madrid, noviembre 2001.

[156] Para tratar de solucionar esta cuestión en la *Proposición de Ley del Senado 124/000002 sobre Derechos de información concernientes a la salud y la autonomía del paciente, y la documentación clínica* (20 de febrero de 2001), se incluye una previsión específica respecto del personal que accede en uso de sus competencias a cualquier clase de datos de la historia clínica, estableciendo para el mismo la obligación de guardar secreto.

ineludible en el modelo organizativo actual admitir un cierto grado de acceso, aunque sea limitado, a colectivos profesionales no afectados por un deber de secreto profesional en sentido estricto.

Las dificultades de compaginar el derecho a la intimidad de los afectados respecto a la información relativa a su salud con otros intereses generales como los estudios epidemiológicos, las situaciones de riesgo grave para la salud de la colectividad, la investigación y los ensayos clínicos hace aconsejable la promulgación de una normativa sanitaria específica que regule todos los aspectos relacionados con la información clínica.

En esta línea de trabajo llevó a cabo su labor el *Grupo de Expertos en Información y Documentación Clínica* [157], reunidos en el año 1997 a instancia del Ministerio de Sanidad y Consumo, elaborando unos criterios generales sobre la materia que, en sus aspectos generales, están siendo recogidos en las iniciativas legislativas actualmente en curso, y cuyos postulados básicos en materia de acceso a la información clínica son los siguientes [158]:

[157] *Grupo de Expertos en Información y Documentación Clínica. Documento Final*. Madrid, 26 de noviembre de 1997. Subsecretaría de Sanidad y Consumo, Ministerio de Sanidad y Consumo, Madrid, 1998.

[158] V. *Proposición de Ley del Senado 124/000002 sobre Derechos de información concernientes a la salud y la autonomía del paciente, y la documentación clínica...*

IV.4.2.1.1. *Acceso por los facultativos y profesionales*

Los profesionales asistenciales del centro que están implicados en el diagnóstico o el tratamiento del enfermo deben tener acceso a la historia clínica.

IV.4.2.1.2. *Acceso por el personal de administración de los centros*

El personal que se ocupa de las tareas de administración y gestión de los centros sanitarios puede acceder sólo a los datos de la historia clínica relacionados con las mencionadas funciones.

IV.4.2.1.3. *Acceso por el paciente*

El paciente tiene derecho a acceder a la documentación de la historia clínica y a obtener una copia de los datos que figuran en ella. Ahora bien, este acceso nunca puede ejercitarse en perjuicio del derecho de terceros a la confidencialidad de los datos de los mismos que figuran en la mencionada documentación, cuando hayan sido recogidos en interés terapéutico del paciente, ni del derecho de los profesionales que han intervenido en su elaboración, que pueden invocar la reserva de sus observaciones, apreciaciones o anotaciones subjetivas [159].

[159] En la citada proposición de Ley se prevé respecto de los pacientes fallecidos, que se facilite el acceso a la historia clínica a las personas a él vinculadas, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente, constituyéndose el centro sanitario en garante de la información.

IV.4.2.1.4. *Otros supuestos de acceso*

Se puede acceder a la historia clínica con finalidades judiciales, epidemiológicas, de seguridad o salud pública, de investigación o docencia [160]. Igualmente, el personal al servicio de la Administración sanitaria que ejerce funciones de inspección puede acceder a las historias clínicas a fin de comprobar la calidad de la asistencia, el cumplimiento de los derechos del paciente o cualquiera otra obligación del centro en relación con los pacientes o la Administración sanitaria.

IV.4.2.2. *Los derechos de rectificación y cancelación de la información sanitaria*

Los derechos de rectificación y cancelación conceden la posibilidad al interesado de exigir al responsable del fichero que cumpla con el principio de calidad de datos, pudiendo instarle a rectificar aquellos cuyo tratamiento no se ajuste a las previsiones de la ley, y en particular cuando los mismos resulten ser inexactos o incompletos; o a cancelarlos cuando hayan dejado de ser necesarios para la finalidad para la cual hubieran sido registrados [161]. El objetivo último es que los datos se mantengan de forma adecua-

[160] Con sujeción a lo establecido en la LOPD, en la Ley General de Sanidad y en las disposiciones concordantes.

[161] V. Art. 4.5 de la LOPD.

da, pertinente y no excesiva en relación con el ámbito y las finalidades legítimas para las que se recogieron [162].

Por lo que se refiere a los datos sanitarios, y a la posibilidad de ejercicio de los derechos de rectificación y cancelación de los mismos, su conservación debe asegurarse, total o parcialmente, al menos durante el tiempo razonablemente necesario para alcanzar el propósito concreto que justificó su recogida y que debe ser, cuando menos, aquel que, bajo un criterio médico, se establezca en el centro o área sanitaria para la asistencia del paciente en el curso de la enfermedad que justificó la creación de la documentación clínica [163].

[162] V. *Cuaderno sobre protección de datos* (suplemento julio 2001 de la revista *otrosí*), pág. 8, donde se resume lo dispuesto en el art. 16 y s.s. de la LOPD, indicándose además que se trata de dos derechos personalísimos e independientes que exigen las mismas formalidades de identificación y representación que el derecho de acceso, que deben ejercitarse por el interesado en persona, de forma gratuita, mediante solicitud o petición dirigida al responsable del fichero, formulada mediante cualquier medio que garantice la identificación del afectado y con los requisitos formales aludidos a la hora de hablar del derecho de acceso. Por otro lado, aunque la ley establece la posibilidad de que el responsable del fichero se oponga a la solicitud de rectificación o cancelación cuando existan causas justificadas, el citado responsable tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación en el plazo de 10 días, tal y como establece el art. 16.1 de la LOPD.

[163] V. *Documento Final, del Grupo de Expertos en Información y Documentación Clínica*. ob. cit. (págs. 25 y 26).

Asimismo, debe significarse que la conservación de la documentación clínica debe garantizar la preservación de la información y no necesariamente el soporte original [164].

[164] V. *Proposición de Ley del Senado 124/000002*, anteriormente citada donde se indica que la documentación clínica deberá mantenerse un mínimo de cinco años para cada proceso asistencial, desde la fecha del alta de dicho proceso.

Por lo que se refiere al *plazo conservación de la información clínica* resulta de interés destacar lo dispuesto por las dos siguientes normas autonómicas:

La *Ley 21/2000, de Cataluña, sobre los derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica*, indica que la historia clínica se ha de conservar como mínimo hasta veinte años desde la muerte del paciente (pudiéndose, no obstante, destruir los documentos no relevantes para la asistencia, transcurridos dos años desde la última atención al paciente), y dentro de ella, junto con los datos de identificación del paciente: las hojas de consentimiento informado, los informes de alta, los informes quirúrgicos y el registro de parto, los datos relativos a la anestesia, los informes de exploraciones complementarias y los informes de necropsia.

La *Ley gallega de 8 mayo de 2001, reguladora del consentimiento informado y de la historia clínica de los pacientes*, prescribe la conservación por tiempo indefinido de determinada información, entre la que se encuentran los informes de anestesia, informes de alta, hojas de consentimiento informado, etc., permitiendo que el resto de la información menos importante se conserve, como mínimo, hasta que transcurran cinco años desde la última asistencia prestada al paciente o desde su fallecimiento.

Decreto 45/1998, de 17 de marzo, del País Vasco, por el que se establece el contenido y se regula la valoración, conservación y expurgo de los documentos del Registro de Actividades Clínicas de los Servicios de Urgencias de los Hospitales y de las Historias Clínicas Hospitalarias. Se prevén plazos de conservación mínimos de dos y cinco años, e indefinido, en función del tipo de documento.

Orden de 14 de septiembre de 2001, de la Consellería de Sanidad por la que se normalizan los documentos básicos de la historia clínica hospitalaria de la Comunidad Valenciana y se regula su conservación. Como norma general se establece un plazo de conservación de cinco años desde la fecha del último episodio asistencial, si bien se prevé la conservación indefinida de determinados documentos.

No obstante, además del motivo de la atención al paciente, pueden existir otros intereses legítimos de epidemiología, de investigación o de organización y funcionamiento del Sistema Nacional de Salud que justifiquen la conservación de la documentación clínica. En estos casos, siempre que sea compatible con los fines perseguidos, deben tratarse los datos anónimamente al objeto de impedir la identificación directa o indirecta de los sujetos implicados [165].

IV.4.2.3. *Derecho de oposición a la obtención de la información sanitaria*

El derecho de oposición consistiría en la posibilidad para el afectado de negarse a la continuación del tratamiento de sus datos personales [166].

El ejercicio de este derecho se refiere a los casos en que, no siendo necesario el consentimiento del afectado para el tratamiento de sus datos de carácter personal (como ocurre respecto de los datos sobre la salud cuando su tratamiento resulte preciso para la prevención o para el diagnóstico médicos, etc. [167]) existan motivos

[165] V. *Proposición de Ley del Senado 124/000002 y ar. 4, apdo 5.º, párrafo 3.º, anteriormente reproducido.*

[166] V. *Cuaderno sobre protección de datos* (suplemento julio 2001 de la revista *OTROSÍ*), ob. cit.; pág. 9.

[167] Art. 7.6 de la LOPD.

fundados y legítimos para que dicha persona formule su oposición, atendiendo a su circunstancia particular, y siempre que una ley no disponga lo contrario [168].

No obstante, como afirma MARTÍN-CASALLO, en la práctica apenas se darán con relación al dato sanitario supuestos de ejercicio del derecho de oposición dada la finalidad de curación que, en último término, busca su tratamiento. Incluso, manifiesta el citado autor que, 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 intimidad [169].

IV.4.3. **La seguridad de los datos sanitarios**

Como afirma MARTÍNEZ SÁNCHEZ [170], la protección de los derechos y libertades de las personas en relación al tratamiento automatizado de sus datos personales implica necesariamente adoptar

[168] V. Art. 6.4 de la LOPD, donde además se dice que en el supuesto citado el responsable del fichero excluirá del tratamiento los datos relativos al afectado. El ejercicio de este derecho será gratuito para el interesado.

[169] JUAN JOSÉ MARTÍN-CASALLO LÓPEZ (Fiscal de Sala del Tribunal Supremo). Ver su ponencia *Derechos de acceso, rectificación y cancelación de los datos sanitarios en la LOPD*, dentro del *VII Congreso Nacional de Derecho Sanitario*, celebrado en octubre de 2000. Ed. Fund. Mapfre Medicina, 2001 (pág. 58).

[170] MAR MARTÍNEZ SÁNCHEZ. Ver su artículo *Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.* Revista *Actualidad Informática Aranzadi*, dirigida por MIGUEL ÁNGEL DAVARA. núm. 35, abril de 2000.

medidas técnicas y organizativas apropiadas para garantizar la seguridad y confidencialidad de la información [171].

IV.4.3.1. *El Reglamento de medidas de seguridad*

El responsable del fichero (y, en su caso, el encargado del tratamiento) debe adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar 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 [172]. Como ya hemos visto anteriormente, la naturaleza de la información sobre la salud es la de datos especialmente protegidos [173].

[171] Como dice la citada autora, el artículo 7 del *Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*; los artículos 16 y 17 de la *Directiva 95/46/CE, 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*; y el artículo 4 de la *Directiva 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y protección de la intimidad en el sector de las telecomunicaciones*, establecen la obligación del responsable del tratamiento de aplicar las medidas de seguridad técnicas y de organización adecuadas para la protección de los datos personales.

[172] V. Art. 9 de la LOPD, en cuyo apartado 2 se dice que no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respeto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

[173] Art. 7.3 de la LOPD.

La norma que contiene las medidas de seguridad generales a adoptar en materia de protección de datos personales, es el citado Reglamento de medidas de seguridad de 1999 [174]. En esta norma se clasifican las medidas de seguridad exigibles en tres niveles: básico, medio y alto, que se disponen de forma acumulativa, de tal forma que todos los ficheros deben cumplir las previsiones establecidas para el nivel básico y además las vinculadas a los niveles medio y, en su caso, alto en el supuesto de que el fichero en cuestión contenga datos de los que obligan a su adopción [175].

[174] 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.

Cabe decir que este Reglamento en su Disposición transitoria única, y respecto de los sistemas de información que se encontraban en funcionamiento a su entrada en vigor (26 de junio de 1999), contemplaba un plazo de dos años para que se implantaran las medidas de seguridad de nivel alto (requeridas para los datos sobre la salud), prorrogable por otro más, en caso de existir dificultades de orden tecnológico. Pues bien, por apreciarse precisamente dificultades del carácter mencionado la citada prórroga fue dispuesta mediante Acuerdo de Consejo de Ministros de 22 de junio de 2001 (Resolución de 22 de junio de 2001, de la Subsecretaría del Ministerio de Justicia. BOE, núm. 151, de 25 de junio de 2001).

[175] Las medidas de seguridad que contiene el Reglamento son las siguientes:

Nivel de seguridad básico

Es el aplicable a todos los ficheros que contengan datos de carácter personal y requiere la implantación de las siguientes medidas de seguridad:

• Elaboración de un documento de seguridad (art. 8);

• Definición de las funciones y obligaciones del personal (art. 9);

• Creación de un Registro de incidencias (art. 10);

• Establecimiento de un procedimiento de identificación y autenticación para los accesos al sistema de información (art. 11);

• Establecimiento igualmente de un control de acceso que evite la obtención de información no autorizada (art. 12);

El Reglamento cataloga los ficheros que contengan datos de salud como merecedores de la adopción de medidas de nivel alto,

---

• Fijación de un procedimiento de gestión de soportes (art. 13), y

• Determinación de procedimientos para la realización de copias de respaldo y recuperación de datos (art. 14).

Cabe señalar que el plazo para la implantación de dichas medidas finalizó el pasado 26 de marzo de 2000, por disposición del Real Decreto 195/2000, que vino a ampliar el primer plazo concedido.

Nivel de seguridad medio

Deberá aplicarse a los ficheros automatizados que contengan datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros y a aquellos cuyo funcionamiento se rija por lo dispuesto en el artículo 29 de la LOPD.

Las medidas a aplicar en estos ficheros son, además de las señaladas para el nivel básico, las siguientes:

• La designación de un responsable de seguridad (art.16);

• La realización de un auditoria de los sistemas de información e instalaciones de tratamiento de datos, al menos, cada dos años (art. 17), y

• Establecimiento de un control de acceso físico a los locales donde se encuentren ubicados los sistemas de información (art. 19).

El plazo para implantar las medidas de seguridad correspondientes al nivel medio finalizó el pasado 26 de junio de 2000.

Nivel de seguridad alto

Las medidas de seguridad de nivel alto deberán reunirlas aquellos ficheros que contengan datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, así como los que se hayan recabado para fines policiales sin consentimiento de los afectados. Deberán adoptarse las siguientes, además de las medidas previstas para los otros niveles (básico y medio):

• Cifrado u otro mecanismo similar para la distribución de soportes que contengan datos (art. 23);

• Establecimiento de mayores controles en el Registro de accesos (art. 24);

• Conservación de las copias de respaldo y recuperación en un lugar diferente de aquél en el que se encuentren los equipos informáticos (art. 25). Y;

• Cifrado o adopción de medidas similares en la transmisión de datos a tra-

lo que constituye el grado máximo de seguridad exigible [176]. Asimismo, la citada norma exige la elaboración de un documento de seguridad, de obligado cumplimiento para todo el personal con acceso a los datos, y donde se regulen todos los aspectos relacionados con la seguridad (medidas, normas, procedimientos, reglas, funciones del personal, respuesta ante incidencias, etc.) [177].

---

vés de redes de telecomunicaciones de forma que se garantice que la información no sea inteligible ni manipulada por terceros (art. 26).

En cuanto al plazo para su implantación véase lo manifestado en la nota anterior.

[176] V. Art. 4.3 del citado Reglamento, donde se dice: *«Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto»*.

[177] V. Art. 8.2 del Reglamento, que establece el contenido mínimo del *documento de seguridad*, citando *«los siguientes aspectos:*

a) *Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.*

b) *Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.*

c) *Funciones y obligaciones del personal.*

d) *Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.*

e) *Procedimiento de notificación, gestión y respuesta ante las incidencias.*

f) *Los procedimientos de realización de copias de respaldo y de recuperación de los datos»*.

Por su parte, el art. 15 del mismo texto, establece que en los casos en que sea preciso adoptar las medidas de seguridad de nivel medio, el documento de seguridad deberá contener, además de lo anterior, la identificación del responsable de seguridad, los controles periódicos y las medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado.

Entre las medidas técnicas que conlleva el nivel alto de protección aplicable a los datos sanitarios destaca la de la obligatoriedad del cifrado (o cualquier otro mecanismo similar) de estos últimos, tanto en la distribución de los soportes informáticos donde se encuentren dichos datos, como en la transmisión de los últimos a través de redes de comunicaciones, todo ello al objeto de garantizar que la información no sea inteligible ni manipulable por terceros [178].

También resulta obligado para los datos sanitarios la llevanza de un *Registro de accesos*, en el que se guarde, de cada acceso, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si fue autorizado o denegado [179]. Además, en estos casos el período mínimo de conservación de los datos registrados será de dos años [180].

IV.4.3.2. *La firma electrónica*

El instrumento jurídico incorporado a nuestro Derecho interno que posibilita la preservación de la integridad y autenticidad de

[178] V. Arts. 23 y 26 del Reglamento.

[179] V. Art. 24 del Reglamento, donde se dice, además, que los mecanismos que permiten el registro de los datos estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso, la desactivación de los mismos. Este responsable tendrá que revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados, al menos, una vez al mes.

[180] V. Art. 24.4 del citado Reglamento, si bien habrá de tenerse en cuenta los plazos mínimos que se establezcan por la normativa sanitaria para la conservación, en cada caso, de la información clínica.

la información en las transmisiones electrónicas de datos, así como la identidad del remitente, es la firma electrónica [181].

Como indica GARCÍA MÁS las firmas electrónicas son unos mecanismos o instrumentos utilizados para conseguir, en redes informáticas abiertas, la seguridad de la identidad del sujeto que emite un mensaje y el contenido del mismo. Para ello se parte de la ayuda de la criptografía, es decir, de la encriptación o enmascaración de la información [182].

Pues bien, ÁLVAREZ-CIENFUEGOS considera que precisamente la implantación de la firma electrónica en el mundo sanitario cons-

[181] Decreto-Ley 14/1999, de 17 de septiembre sobre firma electrónica. En su art. 2.a), se define la firma electrónica como *«… el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge»*. Y en el apartado b) del mismo precepto se indica que la *firma electrónica avanzada* es *«… la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos»*.

Asimismo, el art. 3 establece que *«la firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales»*.

[182] FRANCISCO JAVIER GARCÍA MÁS. *La firma electrónica: Directiva y Real Decreto-Ley 14/1999, de 17 de septiembre*. Revista *Actualidad Civil Aranzadi*, núm. 18, semana 1 al 7 de mayo de 2000.

tituye todo un reto para los servicios de salud, dada la especial sensibilidad de los datos relativos a la salud de los ciudadanos y debido a que, para permitir su circulación electrónica, se requiere, además de unas estrictas medidas de seguridad para evitar accesos no autorizados, una perfecta identificación de los usuarios [183].

Además, para conseguir dicha finalidad, es preciso que el Estado, en cumplimiento de lo establecido por la *Directiva europea sobre la firma electrónica*, vele y controle el hecho de que los proveedores de servicios de certificación y los organismos nacionales competentes en materia de acreditación y supervisión cumplan la normativa sobre protección de datos [184].

IV.4.3.3. *Una posibilidad de autorregulación: los códigos tipo*

La LOPD contempla la posibilidad de que los responsables de los ficheros y tratamientos puedan ampliar o adecuar a las pecu-

[183] JOSÉ MARÍA ÁLVAREZ-CIENFUEGOS SUÁREZ. *La aplicación de la firma electrónica y la protección de datos relativos a la salud*. ob. cit… En este trabajo el citado autor concluye que *«La Ley de Protección de Datos de 1999, concebida como una garantía general y básica de la intimidad de los ciudadanos, en los términos que ha reconocido recientemente el Tribunal Constitucional en sus Sentencias de 30 de noviembre de 2000, al proclamar el derecho de los ciudadanos a la 'libertad informática', resulta insuficiente para una adecuada protección de los datos relativos a la salud de las personas, siendo necesario la publicación de una ley que, de forma específica, contemple esta protección»*.

[184] V. Art. 8, de la *Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica*.

liaridades del sector en el que operan, las previsiones normativas sobre protección de datos personales que, no obstante, habrán de respetarse plenamente [185].

En este sentido, como afirma RUBÍ NAVARRETE, los códigos tipo son códigos deontológicos o de buena práctica profesional elaborados por los responsables del tratamiento de datos personales para ampliar o facilitar el cumplimiento de las obligaciones establecidas en la normativa sobre protección de datos personales, incrementar las garantías de los ciudadanos y el ejercicio de sus derechos, reforzar las estructuras organizativas y técnicas en el tratamiento de aquéllos y, en particular, las medidas de seguridad; o contemplar procedimientos específicos para la tutela de los principios y derechos exigibles en esta materia [186].

[185] Art. 32 de la LOPD: *«Códigos Tipo. 1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las 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 las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.*

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél».

[186] JESÚS RUBÍ NAVARRETE. *Los códigos tipo: la alternativa de la autorregulación*. Revista *Actualidad Informática Aranzadi*, dirigida por MIGUEL ÁNGEL DAVARA; núm. 35, abril de 2000.

Los códigos tipo deben ser depositados o inscritos en el Registro General de Protección de Datos y, cuando proceda, en el de la Comunidad Autónoma correspondiente, que podrán denegar la inscripción de los mismos cuando consideren que no se ajustan a las disposiciones legales y reglamentarias sobre la materia [187].

Su aplicación al campo sanitario es perfectamente posible, tanto en el ámbito privado como en el público, ya que la regulación de la LOPD sobre esta materia es flexible y permite que puedan adaptarse a las necesidades de una sola empresa o de la totalidad o parte de un sector empresarial o profesional, sin distinción del carácter público o privado del responsable del fichero.

IV.4.3.4. *Medidas de seguridad específicas del ámbito sanitario*

Para hallar un catálogo de medidas de seguridad expresamente concebidas para el ámbito sanitario debemos acudir a la *Recomendación del Comité de Ministros del Consejo de Europa sobre protección de datos médicos* [188], donde se indica que, en orden a asegurar la confidencialidad, integridad y exactitud de los datos procesados, así como la protección de los pacientes, se habrán de

[187] V. art. 32.3 de la LOPD y art. 18.2 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

[188] *Recomendación R (97) 5, del Comité de Ministros del Consejo de Europa* a los Estados miembros relativa a la protección de los datos médicos.

tomar medidas apropiadas que permitan la consecución de los siguientes objetivos [189]:

a) *Control de entrada a las instalaciones*.—Se debe impedir que cualquier persona no autorizada tenga acceso a las instalaciones de procesamiento de datos personales.

b) *Control del soporte de los datos*.—Debe impedirse que el soporte de los datos sea leído, copiado, alterado o retirado por personas no autorizadas.

c) *Control de memoria.*—Existe igualmente obligación de impedir la introducción no autorizada de datos en el sistema de información, y cualquier consulta, modificación o borrado no autorizados de datos personales procesados.

d) *Control de utilización.*—Hay que impedir que los sistemas de procesamiento automatizado de datos sean usados por personas no autorizadas a través de equipos de transmisión de datos.

e) *Control de acceso.*—Teniendo en cuenta, por un lado, el acceso selectivo a los datos y, por otro, la seguridad de los datos médicos, debe asegurarse que el diseño del sistema

189 Ver apartado 9 de la citada Recomendación, donde se dice también que *«Estas medidas asegurarán un nivel apropiado de seguridad, teniendo en cuenta, de una parte, el estado de la técnica y, de otra, la naturaleza sensible de los datos médicos y la evaluación de los riesgos potenciales»*.

de procesamiento, como norma general, sea tal que permita la separación de:

- Identificadores y datos relativos a la identidad de las personas.
- Datos administrativos.
- Datos médicos.
- Datos sociales.
- Datos genéticos.

f) *Control de comunicación.*—Tiene que garantizarse la posibilidad de comprobar y verificar qué personas u órganos se pueden comunicar los datos a través de equipos de transmisión.

g) *Control de introducción de datos.*— Debe garantizarse igualmente que es posible comprobar y establecer a posteriori quién ha tenido acceso al sistema y qué datos personales han sido introducidos en el mismo, cuándo y por quién.

h) *Control de transporte.*—Debe impedirse la lectura, copia, alteración o borrado no autorizados de datos personales y el traslado de soportes de datos.

i) *Control de disponibilidad.*—Tienen que salvaguardarse los datos mediante copias de seguridad.

Fuera del ámbito europeo, el *Departamento de Salud de los*

Estados Unidos [190] ha establecido los estándares electrónicos para transmitir datos y ha fijado los requisitos mínimos que deben cumplir las consultas de los médicos para asegurar la confidencialidad y seguridad de toda la información médica. Entre los requisitos exigidos se establece la obligación de utilizar software de encriptación para transmitir cualquier dato referido al estado de salud de un paciente a través de internet. Se establecen también medidas especiales de identificación (firma digital), tecnologías que aseguren niveles de acceso según los cargos y responsabilidades (servicio de admisiones, enfermería, asistencia médica, etc.), sistemas para reconocer quién y por qué entra en un archivo informático, prestando especial atención a las obligaciones del encargado del mantenimiento de la seguridad y a la conservación de los datos [191].

[190] *Department of Health and Human Service.*

[191] JOSÉ MARÍA ÁLVAREZ-CIENFUEGOS SUÁREZ. *La aplicación de la firma electrónica y la protección de datos relativos a la salud*. ob. cit. El autor da cuenta además de que estas normas, que son efectivas desde el mes de enero del año 2001, prevén la elaboración de formatos comunes para la transmisión electrónica de datos entre entidades aseguradoras, proveedores de asistencias sanitarias y hospitales. Asimismo, se recoge la previsión de sancionar con fuertes multas a quienes ignoren las normas, exigiéndose un especial deber de diligencia activa en el mantenimiento del software.

Esta ley, denominada *Standards for Privacy of Individually Identifiable Health Information*, puede consultarse en la página web: *http://aspe.hhs.gov/admnsimp/final/PvcPre01.htm*.

IV.4.4. **Consideración especial de la protección de datos en el campo de las técnicas de reproducción humana asistida**

Como ejemplo del refuerzo de las medidas de protección de datos por razón de la especialidad médica, significamos el caso de las técnicas de reproducción humana asistida, donde la trasgresión del derecho a la intimidad de los datos personales de los usuarios puede acarrear a estos últimos y a su descendencia, perjuicios especialmente graves.

Confidencialidad de la información. La ley sobre técnicas de reproducción asistida [192], consciente de la importancia extrema de garantizar la confidencialidad de la información manejada por los centros y servicios sanitarios especializados en este campo médico, dada su enorme trascendencia para la preservación de la intimidad personal y familiar de los usuarios de las técnicas y de su posible descendencia, contiene una serie de previsiones en materia de protección de datos, que deben implementarse respecto de las recogidas por la normativa general, que operan como sistema de mínimos [193].

[192] Ley 35/1988, de 22 de noviembre, sobre Técnicas de Reproducción Asistida.

[193] De este modo, el art. 4.5, del citado Real Decreto 994/1999, al referirse a la aplicación de los niveles de seguridad previstos en el Reglamento, establece lo siguiente: *«Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes»*.

En este sentido, la ley mencionada hace hincapié en la necesidad de respetar la confidencialidad de la información cuando establece que todos los datos relativos a la utilización de estas técnicas deberán recogerse en historias clínicas individuales, que deberán ser tratadas con las reservas exigibles, y con estricto secreto de la identidad de los donantes, de la esterilidad de los usuarios y de las circunstancias que concurran en el origen de los hijos así nacidos [194].

De igual forma, el Reglamento de donantes prevé expresamente que la información recogida en la historia clínica de los usuarios, la correspondiente al proceso de selección de donantes, así como toda aquella información individualizada contenida en los registros, sea recogida, tratada y custodiada en la más estricta confidencialidad, debiendo producirse dicha custodia de acuerdo con lo establecido en la Ley General de Sanidad y en la normativa sobre protección de datos [195].

[194] V. Art. 2.5 de la ley referida. También es de interés en la materia el art. 19.3 de la misma ley que dice lo siguiente: *«Los equipos médicos recogerán en una historia clínica, a custodiar con el debido secreto y protección, todas las referencias exigibles sobre los donantes y usuarios, así como los consentimientos firmados para la realización de la donación o de las técnicas»*.

[195] Real Decreto 412/1996, de 1 de marzo, por el que se establecen los protocolos obligatorios de estudio de los donantes y usuarios relacionados con las técnicas de reproducción humana asistida, y se regula la creación y organización del Registro Nacional de Donantes de Gametos y Preembriones con fines de reproducción humana.

El art. 9 de esta norma dice lo siguiente: *«La información recogida en la historia clínica de usuarios de las técnicas de reproducción asistida, la correspondiente al proceso de selección de donantes, así como toda aquella informa-*

En consonancia con las previsiones anteriores, la violación del secreto de la identidad de los donantes hace incurrir en responsabilidades legales a los equipos biomédicos y a la dirección de los centros o servicios en los que trabajen [196], y está considerada una infracción muy grave [197].

Excepciones al deber de secreto. Existen, sin embargo, dos supuestos excepcionales en los que la ley permite revelar la identidad de los donantes [198]:

• En circunstancias extraordinarias que comporten un comprobado peligro para la vida del hijo, siempre que la revelación sea indispensable para evitar el peligro citado.

---

ción individualizada contenida en el Registro Nacional de Donantes de Gametos y Preembriones, tanto en la Base Central como en los centros y servicios autorizados, serán recogidos, tratados y custodiados en la más estricta confidencialidad, debiendo producirse esta custodia conforme a lo dispuesto por la Ley General de Sanidad, en los artículos 2, 5, 7, 19, 20 y Disposición final tercera de la Ley sobre Técnicas de Reproducción Asistida, y artículos 7 y 8 de la LORTAD. Ello sin menoscabo de las condiciones de información establecidas por la Ley sobre Técnicas de Reproducción Asistida para los nacidos por la aplicación de estas técnicas y de las circunstancias extraordinarias de ruptura del deber de secreto expresamente establecidas por la Ley de Medidas Urgentes para la Salud Pública y por la propia Ley sobre Técnicas de Reproducción Asistida, en aquellos casos en que fueran de aplicación».

196 Art. 19.2 de la Ley sobre Técnicas de Reproducción Asistida.

197 Art. 20.2, B), j), de la misma ley.

198 Art. 5.5 de la ley.

• Cuando proceda con arreglo a las leyes procesales penales, siempre que la revelación sea indispensable para conseguir el fin legal propuesto.

En ninguno de ambos casos la revelación de la identidad implicará determinación legal de filiación. Siempre tendrá carácter restringido y no podrá conllevar publicidad de la identidad del donante.

Con independencia de las excepciones anteriores, en estos supuestos en los que las técnicas de reproducción van precedidas de una donación de gametos o embriones, la ley admite un supuesto adicional, aunque más limitado, de acceso a la citada información cuando afirma que los hijos, por sí o por sus representantes legales, tienen derecho a obtener información general de los donantes que no incluya su identidad. Este derecho se reconoce también a la receptora de los gametos [199].

Contenido de la información. Por lo que se refiere al derecho de información de los usuarios, debe recordarse que la mencionada Ley sobre Técnicas de Reproducción Asistida establece que debe informarse de cuantas consideraciones de carácter biológico, jurídico, ético o económico se relacionan con las técnicas, recayendo la responsabilidad de facilitar esta información sobre los equipos médicos y los responsables de los centros o servicios sanitarios [200].

[199] *Ibídem*.
[200] V. Art. 2.2 de la citada ley.

Lógicamente, de acuerdo con lo establecido en la LOPD [201], y muy especialmente en los casos en que los datos personales de los donantes y usuarios de las técnicas de reproducción vayan a incorporarse a un Banco de datos, entre la información jurídica a transmitir a los afectados debe encontrarse también la relativa al tratamiento de sus datos personales, con las particularidades que para el caso de los donantes de gametos y embriones se contemplan en la Ley sobre Técnicas de Reproducción Asistida.

Calidad de los datos y registro de los mismos. El principio de calidad de los datos está presente también en la normativa sobre reproducción humana, al contemplarse como infracción grave la omisión de datos, consentimientos y referencias exigidas por la ley, así como la falta de realización de la historia clínica [202].

En el campo de la reproducción se prevé legalmente la existencia de un registro oficial de datos personales conocido como el *Registro Nacional de Donantes de Gametos y Preembriones con fines de reproducción humana* [203].

[201] Art. 5 de la LOPD.

[202] V. Art. 20.2, A), c), de la Ley sobre Técnicas de Reproducción Humana Asistida.

[203] Su creación responde a lo previsto en la Disposición final tercera de la Ley sobre Técnicas de Reproducción Asistida, donde se dice que dicho registro será informatizado, que habrá de contar con las garantías precisas de secreto, y que la información habrá de guardarse en forma de clave. En el apartado a) de esta disposición se indica que *«El Registro Nacional consignará, asimismo, cada hijo nacido de los distintos donantes, la identidad de las parejas o mujeres receptoras, y su localización territorial en cada momento, siempre que sea posible»*.

No obstante, la norma que regula su creación y organización es el citado Real Decreto 412/1996.

Se trata de un registro único formado por las bases de datos de cada centro o servicio autorizado por la Comunidad Autónoma respectiva, mediante su agregación en una Base Central administrada por el Ministerio de Sanidad y Consumo [204].

El Reglamento sobre los requisitos de autorización y homologación de los centros y servicios sanitarios relacionados con las técnicas de reproducción asistida [205] prevé que los bancos de semen, los centros de inseminación artificial y los de fecundación «in vitro» y bancos de preembriones, remitan al Registro la información que se determina, a su vez, en el Reglamento por el que se establecen los protocolos obligatorios de estudio de los donantes y usuarios relacionados con las técnicas de reproducción humana asistida [206].

Por su parte, los propios centros o servicios sanitarios pueden llevar los registros internos que resulten adecuados para la mejor calidad de la prestación asistencial. En este sentido, como indican G. CALDERÓN y G. TOMKINS [207], en los laboratorios de fecundación

[204] V. Art. 8 del citado Real Decreto 412/1996, en cuyo apartado 1 se establece que *«Cada centro o servicio se conectará a la Base Central del Registro tras comunicación de la Administración sanitaria de la Comunidad Autónoma correspondiente a la Base Central»*.

[205] Se trata del Real Decreto 413/1996, de 1 de marzo, por el que se establecen los requisitos técnicos y funcionales precisos para la autorización y homologación de los centros y servicios sanitarios relacionados con las técnicas de reproducción humana asistida (V. Art. 14.3).

[206] Real Decreto 412/1996.

[207] G. CALDERÓN y G. TOMKINS. Ver capítulo *El laboratorio de fecundación in vitro. Condiciones de calidad actuales* (pág. 95 a 97), dentro de la obra *Reproducción asistida del siglo XXI*, Vol. 6, Núm. 2, año 2000, de la colección

«in vitro» es de máxima importancia mantener un *Registro diario*, en el que se anote un registro de datos por cada tipo de paciente tratado de forma separada, FIV, receptoras, donantes y ciclos de descongelación, todo ello con el fin de que pueda detectarse de forma inmediata cualquier cambio en los resultados (variaciones en la tasa de embarazo o implantación de los embriones).

Medidas de seguridad. Por lo que se refiere a las medidas de seguridad específicas en esta especialidad médica, la ley es muy clara al dictaminar la forma en que debe guardarse la información en los Bancos respectivos de los centros o servicios de reproducción asistida y en el Registro Nacional de Donantes: ha de ser en clave [208], precisando además el Reglamento de los donantes, que los datos de identificación personal del donante y el resto de la información sobre el mismo (número de embriones obtenidos con

---

Cuadernos de Medicina Reproductiva, editada por ANTONIO PELLICER y CARLOS SIMÓN. Ed. Panamericana, nov. 2000. Según los autores mencionados, en el citado Registro diario *«se anotarán, entre otras cosas:*

1. *Nombre del paciente.*
2. *Edad.*
3. *Número de ovocitos recuperados y fecundados.*
4. *Técnica de inseminación utilizada.*
5. *Número de embriones congelados y estadio.*
6. *Número de embriones transferidos.*
7. *Embarazo.*
8. *Número de sacos y latidos cardiacos fetales.*
9. *Comentarios».*

[208] V. Art. 5.5 de la Ley 35/1988, sobre Técnicas de Reproducción Asistida.

sus gametos, receptoras, etc.) habrán de estar relacionados por medio de un número clave interno [209].

Así pues, recapitulando lo que se acaba de referir y lo establecido en el mencionado Reglamento general de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal [210], y con relación a los datos sanitarios sobre los donantes que manejan los centros y servicios de reproducción asistida, nos encontramos con que, por un lado y dada su naturaleza de datos especialmente protegidos, deben conservarse (y, en su caso, transmitirse) cifrados y, por otro lado, la información sobre la identidad personal de los donantes y el resto de datos vinculados a la donación de estos últimos deben estar separados entre sí y relacionados bajo un número clave interno y secreto [211].

[209] El art. 8.2 del Real Decreto 412/1996, establece que el registro individual de cada donante aceptado contendrá sus datos de identificación personal y, además, relacionados con dicho registro individual a través de un número de clave interno, constarán también *«los siguientes datos:*

a) *Número de preembriones obtenidos con sus gametos e identificación de las personas de las que procedan cada uno de los gametos del otro sexo.*

b) *Identificación de receptores de la donación de gametos, sean por técnica de inseminación artificial o mediante FIV con gameto de receptor.*

c) *Identificación de la mujer/es receptora/s de los preembriones obtenidos.*

d) *Datos de identificación de los recién nacidos vivos, incluidas incidencias detectadas tras el nacimiento.*

e) *Partos de recién nacidos muertos.*

f) *Interrupción de embarazo por malformación o enfermedad fetal de origen genético o por otras causas».*

[210] Nos referimos al citado Real Decreto 994/1999, de 11 de junio.

[211] El sistema de clave es el previsto también en materia de trasplantes de órganos y tejidos, tal y como se indica en el Real Decreto 2070/1999, de 30 de

Por último, y como medida de seguridad adicional propia de este campo médico, debe decirse que el mencionado Reglamento sobre autorización y homologación de los centros y servicios sanitarios relacionados con las técnicas de reproducción asistida, exige expresamente a los Bancos de semen, laboratorios de semen para capacitación espermática, centros de inseminación artificial, centros de fecundación «in vitro» y bancos de embriones, que garanticen los controles de información y que cuenten con áreas de almacenamiento y archivo dotadas de sistema de protección contra robos [212].

IV.4.5. **El caso de los datos sobre la salud fallado por el Tribunal Constitucional** [213]

El Tribunal Constitucional tuvo ocasión de pronunciarse sobre un recurso de amparo [214] referido al caso de una empresa que man-

---

diciembre, donde se indica que los centros de extracción habrán de disponer de un registro de acceso restringido y confidencial donde se recojan los datos necesarios que permitan identificar las extracciones realizadas, los órganos obtenidos y el destino de los mismos, con las correspondientes claves alfanuméricas que garanticen el anonimato y confidencialidad, y que permita, en caso necesario, el adecuado seguimiento de los órganos de un mismo donante (ver arts. 5 y 12 g).

También se indica en esta norma que en la historia clínica del receptor se recogerán los datos necesarios que permitan identificar al donante, al órgano y al centro hospitalario del que procede el órgano trasplantado, con las correspondientes claves alfanuméricas que garanticen el anonimato y la confidencialidad (art. 15.3).

212 V. Arts. 4.1, 4.3, 6.1, 9 y 11.3 del aludido Real Decreto 413/1996.

213 V. Sentencia núm. 202/99, del Tribunal Constitucional, de 8 de noviembre de 1999.

214 Fundamentado en el art. 18 de la Constitución Española.

tenía un fichero con datos de sus trabajadores, al que denominaba «absentismo con baja médica» y en el que se consignaban además de las correspondientes fechas de baja y alta laboral, el motivo de la baja (enfermedad común o accidente laboral), los días durante los cuales se prolongó la situación de incapacidad laboral y el diagnóstico médico.

A la vista del citado contenido del fichero, en contraste con su denominación, se hacía patente que, no obstante los datos consignados en el mismo, su mantenimiento por la empresa no estaba precisamente dirigido a la preservación de la salud de los trabajadores sino al control del absentismo laboral, y que por ello su creación y actualización, frente a lo pretendido por la empresa, no podía ampararse en la existencia de un interés general amparado por la ley de protección de datos [215], sino en un interés particular de la empresa.

Por este motivo, para el Tribunal, el tratamiento y conservación en soporte informático de los referidos datos atinentes a la salud de los trabajadores, prescindiendo del consentimiento expreso de los afectados, debía calificarse como una medida inadecuada y desproporcionada que conculcaba el derecho a la intimidad y a la libertad informática del titular de la información, en este caso, de los propios trabajadores [216].

[215] Entonces la LORTAD de 1992.

[216] Ver fundamento jurídico 4.º, de la citada resolución.

IV.4.6. **La agencia de protección de datos. su actuación en el campo sanitario**

IV.4.6.1. *Naturaleza y cometido de la Agencia de Protección de Datos*

La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con completa independencia de las Administraciones públicas en el ejercicio de sus funciones [217]. Estas últimas se llevan a cabo por medio del *Director de la Agencia* [218], que es quien la dirige y ostenta su representación, y a quien corresponde dictar las resoluciones e instrucciones que se requieran [219].

Las funciones de la Agencia son básicamente las de velar por el cumplimiento de la legislación sobre protección de datos y con-

[217] V. Art. 35.1 de la LOPD, donde además se dice que la Agencia se regirá por lo dispuesto en la citada ley y en su Estatuto (aprobado por el Real Decreto 428/1993, de 26 de marzo).

Asimismo, dentro de la Comunidad de Madrid existe la Agencia de Protección de la Comunidad de Madrid, cuyo funcionamiento se establece en el Capítulo IV, de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid (B.O.C.M., núm. 175, de 2001).

[218] V. Art. 2.3 del Estatuto de la Agencia de Protección de Datos, en el que se manifiesta que «*… los actos del Director se consideran actos de la Agencia*». Asimismo, el art. 38 de la LOPD prescribe que el Director está asesorado por un Consejo Consultivo.

[219] V. Art. 12 del Estatuto.

trolar su aplicación, dictar instrucciones para la adecuación los tratamientos a la ley, atender las peticiones y reclamaciones de las personas que pudieran resultar afectadas por un tratamiento de datos, requerir la adopción de medidas a los responsables y encargados de los tratamientos, ejercer la potestad sancionadora y velar por la publicidad de la existencia de los ficheros de datos de carácter personal [220].

Dentro de la Agencia de Protección de Datos, y como un órgano integrado de la misma, se halla el *Registro General de Protección de Datos*, donde deben inscribirse, entre otros, los ficheros de que sean titulares las Administraciones públicas y los ficheros de titularidad privada [221].

Este Registro es el órgano al que corresponde velar por la publicidad de la existencia de los ficheros, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación que confiere la ley a los interesados [222].

[220] V. Art. 37 de la LOPD.

[221] V. Art. 39.2 de la LOPD, donde se indica que deben inscribirse también en el Registro General de Protección de Datos, las autorizaciones a que se refiere la Ley, los códigos tipo a que se refiere el art. 32 de la misma y los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

[222] V. Art. 23 del Estatuto de la Agencia de Protección de Datos.

IV.4.6.2. *Intervención de la Agencia en el campo sanitario*

IV.4.6.2.1. *Caso de cesión de datos de pacientes a favor de una clínica dental*

Dentro del ámbito sanitario se han producido algunas actuaciones inspectoras por parte de la Agencia de Protección de Datos, como la originada a raíz de una denuncia de una posible cesión ilegal de datos pertenecientes a una clínica dental por parte de un médico que trasladó su residencia fuera del territorio nacional [223]. La denunciante presentó escrito de reclamación en la Agencia tras recibir publicidad de la clínica dental, con la que no había mantenido contacto alguno.

En la inspección realizada en la citada clínica no se encontraron datos informatizados de la denunciante y, según manifestaron los responsables de la misma, los datos les fueron facilitados por el médico en libretas manuscritas con el nombre, apellidos, dirección y teléfono de los pacientes, habiéndose destruido las mismas tras realizar el mailing a las personas allí incluidas.

El Director de la Agencia decidió archivar las actuaciones dado que, a la vista de los hechos denunciados, y teniendo en consideración que los datos relativos a la denunciante no estaban automa-

[223] Caso recogido en el apartado 2.5.1, de la *Memoria de la Agencia de Protección de Datos del año 1999.*

tizados y se destruyeron al hacer el envío publicitario, tales hechos se encontraban fuera del ámbito de aplicación de la ley [224].

IV.4.6.2.2. *Caso de la documentación sanitaria abandonada*

Otra de las denuncias se refería a unas fichas de cartulina y un libro-registro de atenciones de urgencias, conteniendo datos, diagnósticos y prescripción de medicamentos de pacientes identificados, correspondientes a una Gerencia de Atención Primaria determinada, que miembros de la Guardia Civil de una Comandancia de La Coruña se encontraron en una pista forestal. Las fichas de cartulina se referían a un período comprendido entre 1.973 y 1.986, y el libro registro a 1.988, todo ello manuscrito y algunas de las fichas escritas a máquina.

El Director de la Agencia resolvió archivar las actuaciones, por no ser de aplicación la ley de protección de datos dado que los

[224] Debe tenerse en cuenta que al tiempo de practicarse la labor inspectora en este caso, se encontraba vigente la Ley Orgánica 5/1992, de 29 de octubre (LORTAD), cuya aplicación recaía, a tenor de lo establecido por el art. 2.1 de la citada ley, sobre los datos de carácter personal que figuraran en ficheros automatizados. Ahora bien, la Ley Orgánica 15/1999, de 13 de diciembre (LOPD), que sustituyó a la anterior, modificó el citado precepto señalando (art. 2.1) que su ámbito de aplicación está constituido por los datos de carácter personal registrados en soporte físico (no necesariamente en ficheros automatizados) que los haga susceptibles de tratamiento (y a toda modalidad de uso posterior de los mismos por los sectores público y privado).

contenidos en los documentos encontrados por la Guardia Civil no habían sido informatizados [225].

IV.4.6.2.3. *Caso de información deficiente por parte de un Centro de transfusión de sangre*

El Director de la Agencia de Protección de Datos resolvió un expediente contra un Centro de transfusión de sangre autonómico, declarando que había cometido una infracción grave, debido a que al reclamante, para donar sangre, si bien se le había avisado sobre los casos de exclusión total, exclusión temporal y otras recomendaciones para los donantes, no se le llegó a informar en absoluto sobre la automatización de sus datos, sobre el responsable del fichero, ni sobre la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación [226].

[225] Caso igualmente recogido en el apartado 2.5.1, de la *Memoria de la Agencia de Protección de Datos del año 1999*, al que resulta también aplicable el comentario de la nota anterior, toda vez que la ley de protección de datos vigente al tiempo de las actuaciones era la LORTAD del año 1992, y no la LOPD del año 1999.

[226] También incluido en el apartado 2.5.1, de la *Memoria de la Agencia de Protección de Datos del año 1999*. Se declaró que el Centro había cometido infracción del art. 5 de la LORTAD, tipificada como grave en el artículo 43.3 c) *in fine* de dicha norma.

IV.4.6.2.4. *Caso de los ficheros del ordenador personal de los profesionales de la medicina* [227]

Los hechos tienen su origen en el año 1.996 con ocasión de una denuncia presentada ante la Agencia de Protección de Datos por el administrador de un consultorio médico en base a una supuesta utilización, sin consentimiento de los afectados y por parte de un médico ginecólogo que había prestado allí sus servicios profesionales, de datos personales pertenecientes al centro.

La Agencia de Protección de Datos, a través de su Inspección, requirió al facultativo que enviara una copia de todos los datos personales existentes en su archivo automatizado relativos a tres de sus pacientes.

El médico se negó a entregar los datos citados amparándose en su deber de secreto profesional, lo que motivó que la agencia le sancionara con una multa de diez millones de pesetas por obstaculizar la labor inspectora.

La sanción fue recurrida judicialmente por el facultativo, oponiéndose al recurso la Abogacía del Estado por considerar que,

[227] Este caso se incluye en el apartado 5.3.5 de la *Memoria de la Agencia de Protección de Datos del año 2000*, y además fue ampliamente comentado por CARLOS HERNÁNDEZ, letrado asesor del Ilustre Colegio Oficial de Médicos de Madrid, en su artículo *El secreto médico y la Agencia de Protección de Datos*, publicado en el *Diario Médico* de fecha 8 de septiembre de 2000 (Sección Normativa. pág. 9).

frente a la Agencia de Protección de Datos, no podía invocarse el secreto profesional, pues la información obtenida se utiliza por dicha institución de forma confidencial a efectos simplemente de determinar responsabilidades por hechos denunciados o conocidos que pudieran estar infringiendo la legislación sobre protección de datos. Además, se argumentada por la Abogacía que el derecho a la intimidad de los que reciben el servicio médico, derecho invocado para negar la entrega de los datos a la inspección, es precisamente el derecho fundamental cuya protección tiene encomendada la Agencia de Protección de Datos.

Establecido el debate en los términos referidos, el Tribunal Superior de Justicia de Madrid [228] admitió el recurso del facultativo sobre la base de que el contenido del ordenador personal de un profesional de la medicina, en el que se incluyen las historias clínicas de sus pacientes, debía considerarse fuera del ámbito de aplicación de la ley de protección de datos [229] y, por consiguiente, de la labor inspectora de la Agencia de Protección de Datos. Asimismo, afirmaba el Tribunal que las eventuales violaciones del deber de confidencialidad del médico tenían sus propios cauces jurídicos de reacción, distintos y al margen de los establecidos en la ley de protección de datos, por lo que los ficheros del facultativo, en cuanto se limitaban a recoger historias clínicas de sus pa-

[228] Sentencia de 12 de julio de 2000, de la Sección Octava de la Sala de lo Contencioso-Administrativo, del Tribunal Superior de Justicia de Madrid.

[229] Se trataba entonces de la LORTAD de 1992.

cientes, permanecían al margen de dicha ley y, en consecuencia, nunca podían dar lugar a infracciones tipificadas en la misma [230].

Algunos autores opinan que no hay razón para considerar que los razonamientos de la Sentencia comentada, aunque referida a un supuesto en el que era de aplicación la LORTAD de 1992, tengan que verse afectados por la promulgación de la LOPD de 1999 [231], si bien la Agencia de Protección de Datos, a la luz de la nueva norma, aboga porque las previsiones constitucionales sobre el secreto profesional se compatibilicen con las relativas a la protección de datos personales, derivadas igualmente de la Carta Magna, de tal forma que se permita, también en este caso del ordenador personal, la comprobación del cumplimiento de los principios de protección de datos y de los derechos reconocidos en la propia ley [232].

[230] Añadía el Tribunal en la citada Sentencia que no existió obstrucción a la labor inspectora de la agencia, sino una discrepancia absolutamente razonable en orden al alcance de su actuación en relación con los datos de los pacientes, que el médico tenía registrados en un ordenador personal de su exclusivo uso, y cuya confidencialidad quedaba garantizada por el secreto profesional.

[231] En este sentido, ver CARLOS HERNÁNDEZ en su citado artículo *El secreto médico y la Agencia de Protección de Datos*.

[232] Ver la referencia anterior a la Memoria de 2000 de la Agencia.

En cualquier caso, debe decirse que los preceptos de la LORTAD y de la LOPD en esta materia no son exactamente iguales, ya que la primera, en su art. 2.2, b), decía que el régimen de protección de datos de carácter personal establecido por la ley no era de aplicación *«A los ficheros mantenidos por personas físicas con fines exclusivamente personales»*; sin embargo en la LOPD de 1999 esta excepción ha quedado matizada de la siguiente forma (art. 2.2 a): *«A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas»*. Así pues, en el precepto derogado se aludía

IV.4.6.2.5. *Caso de la difusión de datos de Sentencias condenatorias por negligencia médica*

La Agencia de Protección de Datos ha tenido ocasión también de pronunciarse sobre esta controvertida cuestión [233].

La consulta planteada a la Agencia fue concretamente si era posible difundir a través de internet datos relativos a sentencias firmes condenatorias por delitos relacionados con negligencia médica, sin recabar con carácter previo el consentimiento de los interesados [234].

Para la Agencia dicha pretensión no es admisible legalmente teniendo en cuenta que la ley de protección de datos consagra el principio del consentimiento del afectado para el tratamiento de sus datos, salvo en determinadas excepciones entre las que no se encontraba el supuesto referido. Y, además, porque la citada ley prevé, de forma expresa, que los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo

---

al criterio excluyente de «fines personales», y en la norma vigente al de «actividades personales o domésticas», donde quizás resulte más difícil incluir la actividad médica profesional.

233 Apartado 3.2.6 de la *Memoria* del año 2000.

234 Los consultantes apelaban al supuesto carácter de datos extraídos de «fuentes accesibles al público», que atribuían a las sentencias judiciales. Sin embargo, para la Agencia los citados datos no podían tener dicha consideración legal al entender que sólo son «fuentes de acceso al público» las enumeradas de forma taxativa en el art. 3, j), de la LOPD, donde no se incluyen las Sentencias judiciales.

pueden ser incluidos en ficheros de las Administraciones Públicas competentes y, exclusivamente, cuando así lo establezca una norma con rango suficiente [235], con lo que queda vedado el tratamiento de los mismos a cualquier entidad de derecho privado.

Para la Agencia su conclusión en esta materia tampoco contradice el principio de publicidad de las actuaciones judiciales [236], dado que la citada publicidad tiene por objeto asegurar el pleno desenvolvimiento del derecho de las partes a obtener la tutela efectiva de los jueces y Tribunales en el ejercicio de sus derechos, sin que en ningún caso pueda producírseles indefensión [237]; mientras que la previsión sobre la materia contenida en la ley de protección de datos se fundamenta en la salvaguarda de los derechos de los ciudadanos frente a la realización de actividades que puedan producir una merma de su derecho al honor, la intimidad y la propia imagen [238].

[235] V. Arts. 6.1 y 7.5 de la LOPD.

[236] Arts. 205.6, 232 y 266 de la Ley Orgánica del Poder Judicial.

[237] Art. 24.1 de la Constitución Española.

[238] Art. 18 del mismo texto.

Como se recuerda en el mismo apartado aludido de la citada *Memoria de la Agencia del año 2000*, sobre la colisión entre la publicidad de las sentencias y el derecho a la intimidad de las personas se ha pronunciado el Consejo General del Poder Judicial, disponiendo en el Acuerdo de 18 de junio de 1997, por el que se modifica el Reglamento número 5/1995, de 7 de junio, regulador de los aspectos accesorios de las actuaciones judiciales (apartado 3 del nuevo artículo 5 bis del Reglamento), que *«en el tratamiento y difusión de las resoluciones judiciales se procurará la supresión de los datos de identificación para asegurar en todo momento la protección del honor e intimidad personal y familiar»*.

Por lo que se refiere a la difusión de los citados datos a través de internet, la Agencia considera que, dado que el contenido de los listados podría resultar conocido por cualquier usuario de la red, dicha actuación constituiría una cesión de datos de carácter personal contraria a la ley y contemplada como infracción muy grave [239].

Finalmente, en la consulta formulada a la Agencia se preguntaba también sobre la posibilidad de establecer listas o repertorios de sentencias dictadas en que existan condenas por negligencia médica, publicándose los datos con referencia exclusiva al nombre e iniciales de los apellidos de los afectados.

Sobre esta cuestión la Agencia dictaminó manifestando que, con carácter general y en lo referente a repertorios, su publicación es posible siempre y cuando de la misma no pueda derivarse el conocimiento de la persona que haya resultado condenada por la

[239] La Agencia se apoya en los artículos 11.1 y 44 de la LOPD. El primero que establece 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 cedente y del cesionario con el previo consentimiento del interesado»*. Y el segundo, que establece los distintos tipos de las infracciones en materia de protección de datos, tipifica como infracción grave (letra c, apartado 3) *«proceder a la recogida de datos personales sin recabar el consentimiento expreso de las personas afectadas, en los casos en que ésta sea exigible»;* y como infracción muy grave (letra b, apartado 4) *«la comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas»*. La consecuencia es que, conforme se prevé en el art. 45 de la LOPD, tanto el tratamiento como la publicación en internet de los citados datos podrían ser constitutivos de infracciones sancionables con multas de 10 a 50 y de 50 a 100 millones de pesetas.

sentencia. En otro caso, no es posible la difusión de las sentencias sin antes recabar el consentimiento de los afectados [240].

Recuerda no obstante también la Agencia que las disposiciones de la LOPD no son de aplicación siempre que los datos hayan sido previamente sometidos a un proceso de disociación suficiente, de tal forma que por la aplicación de dicho procedimiento resulte imposible identificar un determinado dato con su sujeto concreto [241].

Lógicamente, respecto a las sentencias sobre casos de negligencia médica no puede obviarse la facilidad de identificar al facultativo afectado, aún en el caso de prescindir de su nombre, pues las referencias a su especialidad médica, centro sanitario o área donde trabaja pueden ser más que suficientes para que se sepa o se averigüe sin gran complicación de quien se trata [242].

[240] Contemplado en el mismo apartado antes citado de la *Memoria del año 2000*.

[241] V. Art. 3 f) de la LOPD donde se define el «procedimiento de disociación» como *«Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable»*.

[242] Por este motivo, en su dictamen sobre el caso planteado la Agencia afirma lo siguiente: *«… teniendo en cuenta las especiales circunstancias concurrentes en el presente caso, en que los facultativos pueden ser identificados no sólo por su nombre y apellidos, sino también por el puesto que desempeñan en un determinado centro sanitario o, incluso, en áreas reducidas, por ser el único especialista en una determinada rama de la medicina, la mera sustitución de los apellidos por sus iniciales puede no resultar suficiente para que la disociación pueda considerarse conforme a lo prevenido en la LOPD, dado que si dicha supresión no va acompañada de la referente al puesto desempeñado y, en su caso, a la del área geográfica en la que el facultativo desempeña su profe-*

La conclusión de la Agencia es que la finalidad que debe perseguir la elaboración de un repertorio jurisprudencial es la de permitir al usuario acceder al conocimiento del modo en que los Tribunales han interpretado lo establecido en el ordenamiento jurídico, sin que sea dable que dicha finalidad pueda ser contemplada en un sentido más amplio, con la consiguiente cercenación de los derechos fundamentales de las personas que intervengan en el litigio, como sucedería si se conocieran los datos personales referidos a dichas personas, que en modo alguno aportan información adicional sobre el contenido jurídico de la sentencia [243].

IV.4.7. **El Terminal Autónomo de Identificación del Paciente en las Recetas (TAIR)** [244]

El TAIR consiste en un sistema de información implantado en los Centros de Salud de Atención Primaria del INSALUD, en los que se fija un terminal de registro y almacenamiento de datos, un lector de banda magnética para el tratamiento de la información

---

sión, no será posible considerar que aquél no resulta identificable, debiendo, en ese caso, someterse el fichero a las previsiones de la Ley, que exigen el consentimiento del afectado».

[243] Parte final del apartado 3.2.6 de la *Memoria de la Agencia de Protección de Datos del año 2000*.

[244] V. Memorias de la Agencia de los años 1998 (aptdo. 4.2.5) y 1999 (aptado. IV.2).

Asimismo, ver JAVIER SÁNCHEZ-CARO, en su artículo *Ley de Protección de Datos e Innovaciones Tecnológicas Farmacéuticas. Revista de Administración Sanitaria*. Vol. V, julio-septiembre 2001, núm. 19 (págs.135 a 156).

contenida en la Tarjeta Sanitaria Identificativa (TSI), cuyos datos son almacenados y posteriormente transmitidos o descargados en un ordenador personal del Centro de Salud, y una impresora para la emisión de etiquetas autoadhesivas e irremovibles [245]. La información debe figurar en modo carácter y código de barras, para facilitar su lectura y grabación automatizada.

El objetivo fundamental del proyecto TAIR es el de proporcionar a los médicos de atención primaria del INSALUD un dispositivo de lectura, registro e impresión de los datos contenidos en la citada tarjeta sanitaria (TSI) con el fin de asegurar la correcta identificación de los pacientes; mejorar los sistemas de información para la gestión de los servicios sanitarios; ayudar al médico a cumplimentar los documentos derivados de la asistencia sanitaria mediante la emisión de etiquetas; realizar el seguimiento de las recetas; y colaborar, por último, en el control y lucha contra el fraude en la prestación farmacéutica, a través del conocimiento de los perfiles de prescripción de cada paciente y de la correcta identificación de los diferentes tipos de usuarios.

[245] El mecanismo de utilización es el siguiente: al inicio de cada sesión de consultas, el médico introduce su identificación en el TAIR. A continuación, por cada acto médico derivado de la atención al paciente, el médico, mediante el TAIR, recoge los datos de identificación del paciente y los datos de la actividad asistencial (que no pueden ser consultados o actualizados por él mismo mediante la utilización de dicho dispositivo) y emite las correspondientes etiquetas que incluyen tres tipos de datos: identificación del médico, identificación del paciente y datos de la actividad asistencial.

A partir del TAIR se generan dos flujos de información:

• Uno interno, relativo a la actividad asistencial y recetas médicas, sin que se recoja en ellas el medicamento prescrito (este último es incluido en la receta de forma manual por el médico) [246].

• Y otro externo, relativo a la información generada por la receta médica, cuya grabación se realiza por los colegios farmacéuticos que la remiten finalmente al INSALUD [247].

Pues bien, a raíz de diversas denuncias presentadas ante la Agencia de Protección de Datos por posibles vulneraciones de la ley, se iniciaron en el año 1.998 actuaciones de investigación finalizadas en el año 1999 [248], en virtud de las cuales se analizó el

[246] En los Centros de Salud se realiza una explotación de estos datos para la gestión asistencial y administrativa de los mismos (pacientes atendidos por consulta, pacientes derivados a especialidades, recetas entregadas a pacientes, parte de incapacidad temporal, solicitud de pruebas diagnósticas, etc.), no saliendo la información del entorno de dichos Centros y existiendo diversos niveles de acceso a la misma en función del trabajo realizado por cada persona.

[247] En concreto el proceso es el siguiente: las oficinas de farmacia dispensadoras de los medicamentos recogen las recetas agregando físicamente el cupón precinto que corresponde al medicamento y que contiene otro código de barras, así como los datos relativos a la propia farmacia. Posteriormente, las recetas son enviadas a los respectivos colegios farmacéuticos, donde, generalmente a través de terceras empresas contratadas al efecto, se graban en un CD ROM, que se envía mensualmente al Colegio General de Colegios Farmacéuticos quien, a su vez, los entrega en las dependencias del INSALUD.

[248] Por Resolución del Director de la Agencia de Protección de Datos, de fecha 24 de abril de 1999, se acordó el archivo de las actuaciones en relación con el tratamiento de datos de las recetas.

circuito externo de los datos del TAIR, siendo las cuestiones legales planteadas las siguientes:

• *La norma habilitante para la creación o modificación del fichero automatizado*. Teniendo en cuenta que la novedad del TAIR, en lo que se refiere al tratamiento de nuevos datos de usuarios del Sistema Nacional de Salud y, en particular, de personas con derecho a la prestación farmacéutica, se limita a la información relativa al código de identificación personal (CIP) contenido en la Tarjeta Sanitaria Identificativa (TSI), puede concluirse que resulta suficiente la habilitación normativa preexistente para la creación de ficheros automatizados del Ministerio de Sanidad y de sus Organismos Autónomos [249].

• *El consentimiento de los afectados*. Opera la excepción legal a la obtención del consentimiento prevista en la ley respecto de los casos en que los datos se recogen para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias [250].

[249] La norma habilitante es la Orden Ministerial de 21 de julio de 1994, modificada por la Orden Ministerial de 19 de enero de 1999, para mejorar el sistema de información mediante su vinculación con el proyecto TAIR y, posteriormente, por la Orden Ministerial de 15 de abril de 1999.

[250] Art. 6 de la LOPD.

Y también art. 85.2, de la Ley 25/1990, de 20 de diciembre, del Medicamento, que establece que *«las recetas y órdenes hospitalarias de dispensación deberán contener los datos básicos de identificación del prescriptor, paciente y medicamentos»*. En consecuencia, el hecho de que tales datos se asocien a los contenidos en la TSI no significa otra cosa que la Administración sanitaria actúa dentro del marco de sus competencias, por lo que cabe prescindir del consentimiento del afectado.

• *El derecho de información en la recogida de datos.* Resulta también aplicable la excepción contenida en la ley al citado derecho, que indica que no será necesaria la información si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban [251]. Aquí, la naturaleza de los datos personales solicitados (los incluidos en la TSI) y las circunstancias en que se recaban (acto médico de atención al paciente), permiten deducir la existencia de un fichero automatizado de titularidad de la Administración sanitaria, así como su finalidad, los destinatarios de la información y el carácter obligatorio de su respuesta, dada la obligatoriedad de justificar documentalmente el derecho a la prestación farmacéutica. Todo ello al margen de la información que debe suministrarse a los afectados en el momento de la solicitud de la TIS.

• *Tratamiento automatizado de los datos personales relativos a la salud de las personas.* La ley permite que las instituciones y los centros sanitarios públicos y privados y los profesionales, puedan proceder al tratamiento automatizado de los datos personales relativos a la salud de las personas que a ellos acudan o hayan de ser tratados por los mismos, de acuerdo con la normativa sanitaria correspondiente [252].

[251] Art. 5.3 de la LOPD. En este caso, ha de tenerse en cuenta que los datos personales de los usuarios que se incorporan como novedad a la receta a través del TAIR se refieren exclusivamente al código de identificación personal (CIP) incluido en la Tarjeta Sanitaria Identificativa (TSI).

[252] Art. 8 de la LOPD.

• *La participación de empresas privadas en el tratamiento de datos*. La posibilidad de realizar el tratamiento de datos personales por cuenta de terceros está admitida en la ley, tal y como hemos visto anteriormente en este trabajo [253].

IV.4.8. **El proyecto DIGITALIS** [254]

Desde 1.973, la necesidad de facturar las recetas médicas dio origen a un fichero de control y gestión de las mismas. Su objetivo era el de gestionar la prestación farmacéutica mediante el conocimiento de la facturación de las recetas, además de facilitar la facturación a las oficinas de farmacia. El fichero actual de gestión de la prestación farmacéutica tiene como finalidad declarada la gestión y control de la prescripción y dispensación de medicamentos con cargo a la Seguridad Social, así como su utilización como herramienta en la confección de estadísticas.

Pues bien, las ventajas de explotar la totalidad de los datos que se recogen en la receta, de modo que se cumpla la doble finalidad, por un lado, de la comprobación contable sobre la veracidad de las facturas y, por otro, conocer con exactitud el consumo de medica-

[253] Art. 12 de la LOPD. Las empresas que intervienen en el proceso se obligan a salvaguardar la identidad y el secreto de los datos tratados, así como a cumplir la normativa correspondiente en materia sanitaria y de protección de datos.

[254] Este apartado aprovecha el artículo de JAVIER SÁNCHEZ-CARO, denominado *Ley de protección de datos e innovaciones tecnológicas farmacéuticas*, publicado en la *Revista de Administración Sanitaria*; ob. cit. (julio-septiembre 2001).

mentos (y facilitar la detección de fraudes), relacionándolo con las características de los distintos agentes que lo determinan, dio origen a la aplicación informática DIGITALIS [255].

A tenor de los trabajos del INSALUD y de las observaciones de la Agencia de Protección de Datos, los principales problemas legales planteados por el proyecto DIGITALIS son los siguientes:

• *Información a los afectados*. Al igual que se manifestó al hablar del derecho de información respecto del TAIR, en el caso de DIGITALIS es aplicable la misma excepción a la obligación de informar prevista para los supuestos en que dicha información puede deducirse claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban [256]. En este caso, puede considerarse que se cumplen las exigencias de la Ley al respecto, al complementarse la información suministrada a los pacientes al solicitar la Tarjeta Sanitaria Identificativa

[255] El fichero se nutre de los datos recabados mediante el dispositivo TAIR y otros capaces de emitir etiquetas con código de barras, así como de la información contenida en los sellos estampados en las recetas que contienen los datos de los médicos, en los diversos centros de salud, relativos al acto médico de confección de recetas. Estos datos se completan con la grabación de las recetas médicas y con la incorporación al fichero de datos procedentes de otro fichero: «usuarios del sistema sanitario y sistema de información de población protegida del Instituto Nacional de la Salud» (Fuente: INSALUD. Subdirección General de Atención Primaria-Área de Gestión de Farmacia).

[256] Art. 5.3 LOPD.

(TSI) [257], con la que ofrece la propia receta [258]. No obstante, resultaría más adecuado que la cláusula informativa incluida en la solicitud de la citada tarjeta sanitaria (TSI) contuviera una referencia genérica a las finalidades de la misma en el ámbito del Sistema Nacional de Salud.

• *El consentimiento de los afectados*. El problema más importante en materia de consentimiento que planeta el DIGITALIS consiste en que determinadas aplicaciones de este sistema permiten obtener un perfil farmacoterapéutico del paciente. En tal sentido, ha de existir una justificación expresa e importante que ponga de relieve que dichos datos son adecuados, pertinentes y no excesi-

[257] La cláusula informativa en el documento de solicitud de tarjeta sanitaria dice lo siguiente: *«Los datos de este formulario van a ser incorporados al fichero «sistema de información de población protegida». Los datos recogidos son los mínimos obligatorios para la identificación del usuario, del facultativo elegido y la expedición de la tarjeta. Para ejercer el derecho de acceso, rectificación y/o cancelación se informa que el órgano de la Administración responsable del fichero es la Presidencia Ejecutiva del INSALUD, y el ejercicio del derecho de acceso se efectuará ante la Subdirección General de Atención Primaria. Las posibles cesiones previstas son a otros organismos sanitarios y oficiales de estadísticas. Al firmante del presente documento le asiste el derecho a no declarar sobre su ideología, religión o creencias»*.

[258] El texto incluido en los modelos de receta es el siguiente: *«En cumplimiento del artículo 5 de la Ley 5/1992, se informa que los datos de la receta van a ser incorporados al fichero 'gestión de la prestación farmacéutica' para la gestión y control de la misma, cuyo órgano responsable es el INSALUD. La posibilidad de ejercitar los derechos de acceso, rectificación y cancelación podrá realizarse a través de la Gerencia de Atención Primaria del INSALUD»*.

vos en relación al ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido [259].

• *Medidas de seguridad*. Es evidente que las medidas de seguridad establecidas en las normas son exigibles para la puesta en funcionamiento del DIGITALIS [260].

IV.4.9. **Los delitos informáticos relacionados con la información sanitaria**

La última salvaguarda del derecho a la intimidad la encontramos en el Código Penal, donde para las agresiones más relevantes se consagra el delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos [261].

[259] V. Art. 4 de la LOPD, en relación con las Leyes General de Sanidad y del Medicamento, así como las normas reglamentarias que las desarrollan. Además, ha de tenerse en cuenta la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, respecto de la prevención y protección de la salud pública en materia de información epidemiológica, detección e información de efectos adversos que pudieran haber sido causados por los medicamentos y de valoración y control de la prescripción para la garantía de un uso racional del medicamento.

[260] En concreto las establecidas en el Real Decreto 994/1999, de 11 de junio.

[261] Art. 197 del Código Penal, donde se prevén penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

El delito mencionado contempla, además, como agravante, el hecho de que la revelación afecte a datos de carácter personal que se refieran, entre otros aspectos, a la salud de las personas [262].

Tampoco es ajeno al ámbito sanitario el delito de falsedad documental [263], referido a las conductas de alteración, simulación, suposición de personas que no han intervenido y falta de verdad en documentos, entendiendo por este último todo soporte material que exprese o incorpore datos [264].

El sabotaje informático dirigido a destruir o alterar datos de las historias clínicas tiene igualmente su previsión punitiva, como forma agravada del delito de daños, en el Código Penal [265].

La conducta típica de este delito consiste en la destrucción o en la producción generalizada de daños en sistemas, datos, programas o documentos informáticos o telemáticos.

262 Apartado 5 del citado art. 197 del Código Penal.

263 V. JAVIER SÁNCHEZ-CARO y FERNANDO ABELLÁN. *Imprudencia y negligencia en la profesión médica*. Fundación Salud 2000. Granada 2001 (págs. 60 y 61).

264 Arts. 390 y ss., del Código Penal.

265 Art. 264.2 del Código Penal, que castiga con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses *«... al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos»*.

Como afirma MARCHENA GÓMEZ, el daño a que se refiere esta figura delictiva puede ser un daño no tangible, un daño carente de realidad física. El daño sufrido por los sistemas o programas informáticos normalmente será un destrozo funcional, un menoscabo en la correcta operatividad del sistema, incorrección que, como sostiene el citado autor, puede al propio tiempo proyectar sus efectos sobre otros bienes jurídicos cuya incolumidad dependa del preciso y adecuado funcionamiento del ordenador [266].

[266] MANUEL MARCHENA GÓMEZ. *El sabotaje informático: entre los delitos de daños y desórdenes públicos*. Revista *Actualidad Informática Aranzadi*, dirigida por MIGUEL ÁNGEL DAVARA, núm. 40, julio 2001. Afirma el citado autor que el resultado de este delito encierra una capacidad pluriofensiva tan variada como variadas sean las posibles utilidades que reporta el tratamiento informático. En este sentido, considera que en aquellas ocasiones en que la originación de un perjuicio económico sea el propósito que filtre la acción del sujeto activo, se estará en presencia de un *delito de daños* del art. 264.2 del Código Penal. Por el contrario, en aquellos otros casos en que se busque de forma deliberada la interrupción o destrozo de las comunicaciones, resultará obligada la aplicación del art. 560.1 del mismo Código, referido a una de las modalidades del *delito de desórdenes públicos* (*«Los que causaren daños que interrumpan, obstaculicen o destruyan líneas o instalaciones de telecomunicaciones o la correspondencia postal, serán castigados con la pena de prisión de uno a cinco años»*).

V
CONCLUSIONES

• El concepto tradicional de telemedicina ha evolucionado en los últimos tiempos en el sentido de dejar de asociarse exclusivamente a la utilización de las telecomunicaciones para prestar asistencia sanitaria en zonas remotas deficientemente atendidas, y convertirse en sinónimo de mejora de la calidad de la atención médica propia de los tiempos modernos, de la denominada Sociedad de la Información.

• Al mismo tiempo, la multiplicidad de factores (éticos, sociales, tecnológicos, etc.) que confluyen en el campo de las nuevas tecnologías, y que para algunos autores conforman una disciplina propia (lo que se ha dado en llamar infoética), hacen que al tratar de telemedicina en sentido genérico, se estén contemplando diferentes realidades: por un lado, una nueva forma de entender y ejercer la medicina, por otro lado, el manejo electrónico de datos sobre la salud de las personas y, finalmente, la problemática que desde un punto de vista tecnológico origina la práctica de la medicina por medios técnicos (estándares técnicos, certificación de técnicas adecuadas, protocolos de utilización).

• Las aplicaciones básicas de la telemedicina se proyectan en una triple vertiente: los procesos asistenciales (teleasistencia, televigilancia, teleconsulta), gestión de pacientes y administración (citas, pruebas, etc.) y servicios de información y formación tanto a ciudadanos como a profesionales sanitarios (a través de internet).

• Por lo que se refiere a las webs sanitarias, actualmente es cuestionable la aceptabilidad en el plano ético de la evacuación a través de las mismas (sin que exista una relación previa médico-paciente) de consultas directas efectuadas por los pacientes, siendo exigible en estos casos al responsable de la web el respeto a una serie de principios, tales como la transparencia del proveedor (su identificación y también la de los patrocinadores económicos y autoridad científica) y el respeto a la confidencialidad de la información.

• El uso de la telemedicina se justifica sólo por el mejor interés del paciente (nunca por la comodidad del médico), del que debe obtenerse el consentimiento informado. Además, el médico debe asegurarse de que existen medidas de seguridad adecuadas para garantizar la confidencialidad de la información, y abstenerse de practicar telemedicina cuando no esté seguro de la eficacia y calidad del equipo técnico.

• La mayor parte de los autores y organizaciones internacionales (Asociación Médica Mundial, Comité Permanente de Médicos Europeos) son partidarios de que, siempre que sea posible, se salvaguarde el principio de inmediación médico-paciente, es de-

cir, el contacto directo, físico y personal entre ambos. La denominada medicina basada en la evidencia (es decir, en pruebas, en protocolos clínicos) no debe obviar los aspectos positivos que se desprenden de la relación médico-paciente tradicional.

• En el ámbito europeo el derecho a la protección de datos está basado en los principios de limitación de objetivos, proporcionalidad y calidad de los datos que se recaben, transparencia sobre el manejo de los mismos, y confidencialidad y seguridad de su tratamiento automatizado.

• El Tribunal Constitucional de España tiene reconocido el derecho a la autodeterminación informativa, como un derecho o libertad fundamental de carácter autónomo respecto del derecho general a la intimidad personal y familiar (y distinto de este último) dirigido a hacer frente a las potenciales agresiones a la dignidad y a la libertad de las personas provenientes del uso ilegítimo del tratamiento mecanizado de datos.

• A la hora de hablar del derecho a la protección de datos, el concepto de datos sanitarios debe entenderse de forma amplia, abarcando todos aquellos datos que de alguna forma, directa o indirectamente, se refieran a la salud de las personas. Dentro de los datos de la salud son especialmente vulnerables los datos genéticos cuya obtención limita el Convenio de Oviedo sobre los Derechos Humanos y la Biomedicina, a supuestos que tengan que ver con la protección de la salud de las personas o con la investigación médica.

• Para el Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías, a la hora de analizar la introducción de innovaciones tecnológicas en el campo sanitario deben tenerse en cuenta los principios de la dignidad humana, de autonomía, de justicia, de anticipación de beneficios y de solidaridad.

• La confidencialidad de los datos sobre la salud conlleva la obligación de obtener el consentimiento informado del paciente y el necesario establecimiento de limitaciones al acceso a sus datos. El respeto al secreto médico es un elemento central para la confianza en el sistema de salud.

• La seguridad de las comunicaciones por las que circulan los datos sobre la salud de las personas constituye un imperativo ético. La salvaguarda de la seguridad en este campo requiere el uso de tecnología de encriptación, utilización de redes cerradas, respeto a los estándares de seguridad, y control de los sistemas de información.

• En nuestro derecho interno no existe una norma expresa referida a la protección de los datos sanitarios. Las disposiciones legales básicas de aplicación en la materia son de carácter general: la Ley Orgánica de protección de datos de carácter personal y el Reglamento de medidas de seguridad (ambas de 1.999).

• Tanto en el ámbito de la Unión Europea, como dentro de nuestras fronteras, existe un sentir generalizado sobre la insuficiencia de la legislación general sobre protección de datos para abordar todos los aspectos del tratamiento de los datos sobre la salud

de las personas. Son numerosas las opiniones favorables a iniciativas legislativas que contemplen de forma específica la problemática de la protección de datos personales en el sector sanitario.

• Es posible la obtención y tratamiento automatizado de los datos sobre la salud, sin necesidad de recabar el consentimiento del afectado, cuando dicho proceso sea 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 se realice por un profesional sanitario sujeto a secreto profesional o por otra persona sujeta asimismo a una obligación de secreto equivalente.

• En cuanto a la cesión de los datos sanitarios a terceros, ésta es posible siempre que tenga por objeto el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, y se obtenga el consentimiento del interesado, salvo en caso de urgencia médica o necesidad de utilizar la información para estudios epidemiológicos, en que puede prescindirse de dicho requisito.

• Respecto de los datos sanitarios es posible ejercitar por los afectados el abanico de derechos que la ley sobre protección de datos recoge con carácter general, es decir, los derechos de acceso, de rectificación, de cancelación y de oposición. No obstante, deben tenerse en cuenta determinadas limitaciones por razón de la naturaleza singular de dichos datos.

• Los datos sanitarios son considerados legalmente como da-

tos especialmente protegidos, lo que se traduce en que los mismos deben ser objeto de medidas técnicas de seguridad de nivel elevado, entre las que se encuentran la necesidad de encriptación de los soportes en que se almacenen y de las comunicaciones, y el establecimiento de controles rigurosos de acceso a la información.

• Las recomendaciones en el ámbito europeo con relación a las medidas de seguridad de los datos sanitarios, abogan porque los sistemas de procesamiento permitan la separación de los siguientes datos: los de identificación del paciente, los administrativos, los médicos, los sociales y los genéticos.

• En el campo de las técnicas de reproducción asistida se exigen medidas de seguridad adicionales como la consistente en que la información sobre la identidad de los donantes de gametos y el resto de datos vinculados a la donación esté separada entre sí y relacionada bajo un número clave interno y secreto.

• La Agencia de Protección de Datos es el organismo independiente que vela por el cumplimiento de la legislación sobre protección de datos, habiéndose pronunciado en diferentes supuestos que afectan a los datos sanitarios, entre los que destaca el caso de la difusión de datos de Sentencias condenatorias por negligencia médica.

• Los proyectos TAIR y DIGITALIS promovidos por el INSALUD, son dos supuestos de tratamiento automatizado de datos sanitarios que se encuentran operativos y en funcionamiento en España.

• Para las transgresiones más graves del derecho a la intimidad de los datos sanitarios, el Código Penal contempla figuras específicas: el delito de descubrimiento y revelación de secretos, la falsedad documental y el sabotaje informático.

VI
ANEXO

I. NORMAS Y DECLARACIONES INTERNACIONALES

A. Unión Europea

- Tratado de la Unión Europea.
- Tratado de Ámsterdam de 1997.
- Carta de los Derechos Fundamentales de la Unión Europea, proclamada por el Parlamento Europeo, el Consejo y la Comisión, y hecha en Niza el 7 de diciembre de 2000 (Diario Oficial de las Comunidades Europeas, de 18 de diciembre de 2000).
- Directiva 2000/31/CE, de 8 de junio, de 2000, del Parlamento y del Consejo relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior.
- Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Directiva 97/66 del Parlamento y del Consejo de Europa, de 15 de diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- Directiva 97/7/EC, sobre protección de los consumidores con respecto a contratos a distancia.
- Directiva 95/46/CEE, del Parlamento Europeo y del Consejo de Eu-

ropa, 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.
- Directiva del Consejo 93/42/EEC, normativa europea sobre aparatos médicos.
- Directiva del Consejo 85/374/EEC, normativa europea sobre productos defectuosos.
- Propuesta de Resolución del Parlamento Europeo sobre las repercusiones sociales, jurídicas, éticas y económicas de la genética humana, de 24 de julio de 2001, elaborada por la Comisión temporal sobre Genética Humana y Otras Nuevas Tecnologías de la Medicina Moderna.
- Propuesta (4) de Reglamento del Parlamento Europeo y del Consejo de Europa sobre la protección de personas físicas en lo que respecta al tratamiento de datos personales por las Instituciones y Organismos de la Comunidad Europea y sobre la libre circulación de estos datos (14 de julio de 1999).

B. **Consejo de Europa**

- Recomendación R (97) 5, del Comité de Ministros del Consejo de Europa a los Estados Miembros, de 13 de febrero, relativa a la protección de datos sanitarios.
- Recomendación R (91) 15, del Comité de Ministros del Consejo de Europa, en materia de estudios epidemiológicos en el ámbito de la salud mental.
- Recomendación 81/679/CEE, de la Comisión, de 29 de julio de 1981, relativa al Convenio del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
- Recomendación R (81) 1, referida a la reglamentación aplicable a los bancos de datos médicos automatizados.

- Resoluciones del Consejo de Europa de 1973 y 1974, relativas a la protección de las personas respecto a los bancos de datos electrónicos en el sector privado y la Resolución, y a la protección de las personas respecto a los bancos electrónicos en el sector público, respectivamente.
- Resolución 509, de 1968, de la Asamblea del Consejo de Europa, sobre los derechos humanos y los nuevos logros científicos y técnicos.
- Convenio 108, de 28 de enero de 1981, del Consejo de Europa, relativo a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal hecho en Estrasburgo y ratificado por España el 27 de enero de 1984.

C. **Otros**

- Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales realizado en Roma el 14 de noviembre de 1950.
- Principios Éticos de la Telemedicina. Comité Permanente de Médicos Europeos, CP 97/33, Markku Aarimaa, 28 de noviembre de 1996.
- Declaración Universal de los Derechos Humanos adoptada y proclamada por la 183.ª Asamblea General de la ONU, el 10 de diciembre de 1948.
- Pacto Internacional de Derechos Civiles y Políticos hecho en Nueva York, el 19 de diciembre de 1966.
- Recomendación de la ONU relativa al tratamiento automatizado de datos personales, de 14 de diciembre de 1990.
- Recomendaciones de la Organización para la Cooperación y Desarrollo de Europa (OCDE), de las que destacan la relativa a la circulación internacional de datos personales para la protección de la intimidad (septiembre 80); y la relativa a la seguridad de los sistemas de información (noviembre 92).

II. LEGISLACIÓN NACIONAL

- Constitución Española, 6 de diciembre de 1978.
- Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 5/1992, de 29 de octubre, sobre la regulación del tratamiento automatizado de datos de carácter personal (LORTAD).
- Ley Orgánica 3/1986, de 14 de abril, sobre Medidas Especiales en materia de salud pública.
- Ley Orgánica del Poder Judicial.
- Ley 25/1990, de 20 de diciembre, del Medicamento.
- Ley 35/1988, de 22 de noviembre sobre Técnicas de Reproducción Asistida.
- Ley 14/1986, de 25 de abril, General de Sanidad.
- Real Decreto-Ley 14/1999, de 17 de septiembre de firma electrónica.
- Real Decreto 2070/1999, de 30 de diciembre, por el que se regulan las actividades de obtención y utilización clínica de órganos humanos y la coordinación territorial en materia de donación y trasplante de órganos y tejidos.
- 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.
- Real Decreto 412/1996, de 1 de marzo por el que se establecen los protocolos obligatorios de estudio de los donantes y usuarios relacionados con las técnicas de reproducción humana asistida, y se regula la creación y la organización del Registro Nacional de Donantes de Gametos y Preembriones con fines de reproducción humana.
- Real Decreto 413/1996, de 1 de marzo por el que se establecen los requisitos técnicos y funcionales precisos para la autorización y ho-

mologación de los centros y servicios sanitarios relacionados con las técnicas de reproducción humana asistida.

- Real Decreto 1.332/1994, de 20 de junio por el que se desarrollan algunos aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de Datos Personales.
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.
- Orden Ministerial del Ministerio de Fomento, de 21 de febrero de 2000.
- Orden Ministerial de 15 de abril de 1999, para mejorar el sistema de información mediante su vinculación con el proyecto TAIR.
- 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.
- Proposición de Ley del Senado 124/000002 sobre Derechos de información concernientes a la salud y a la autonomía del paciente, y la documentación clínica.

III. LEGISLACIÓN AUTONÓMICA

- Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.
- Ley gallega, de 8 de mayo de 2001, reguladora del consentimiento informado y de la historia clínica de los pacientes.
- Ley 21/2000, de Cataluña, sobre derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica.
- Decreto 45/1998, del País Vasco, sobre documentación clínica.
- Orden, de 14 de septiembre de 2001, de la Consellería de Sanidad por la que se normalizan los documentos básicos de la historia clínica hospitalaria de la Comunidad Valenciana y se regula su conservación.

IV. JURISPRUDENCIA

- Sentencia del Tribunal de Justicia de las Comunidades Europeas, de octubre de 2001 (asunto C-377/98).
- Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. Esta sentencia resolvió el Recurso de Inconstitucionalidad interpuesto por el Defensor del Pueblo contra algunos incisos de los artículos 21.1 y 24.2, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Sentencia del Tribunal Constitucional 115/2000, de 10 de mayo.
- Sentencia del Tribunal Constitucional 202/99, de 8 de noviembre de 1.999.
- Sentencia del Tribunal Constitucional 144/1999, de 22 de julio.
- Sentencia del Tribunal Constitucional 134/1999, de 15 de julio.
- Sentencia del Tribunal Constitucional 143/1994.
- Sentencia del Tribunal Constitucional 254/1993, de 20 de julio.
- Sentencia del Tribunal Constitucional 197/1991, de 17 de octubre.
- Sentencia del Tribunal Constitucional 231/1988, de 2 de diciembre.
- Sentencia del Tribunal Constitucional 89/1987, de 3 de junio.
- Sentencia del Tribunal Constitucional 110/1984, de 26 de noviembre.
- Sentencia del Tribunal Constitucional 73/1982, de 2 de diciembre.

V. OTROS

- Código de Ética y Deontología Médica de 1999, de la Organización Médica Colegial.

VII
BIBLIOGRAFÍA

ÁLVAREZ-CIENFUEGOS SUÁREZ, José María. «La aplicación de la firma electrónica y la protección de datos relativa a la salud», Revista *Actualidad Informática Aranzadi*, abril 2001.

ÁMERIGO, J. A. y SUÁREZ GARCÍA, Eugenio. *Telemedicina-La salud en el siglo XXI*. Estudio Editorial, 2001.

ANDÉREZ GONZÁLEZ, Alberto. Informe Seis. «La Seguridad y confidencialidad de la información clínica», capítulo «Aspectos legales de la seguridad y confidencialidad de la información clínica». Sociedad Española de Información de la Salud. Pamplona, 2000.

ATIENZA MERINO, G. «La Telemedicina en la práctica médica», *Revista Galega de Actualidade Sanitaria* (vol. 1), año 2001.

CALDERÓN, G. y TOMKINS, G. *Reproducción Asistida del siglo XXI*, capítulo El laboratorio de fecundación in vitro. Condiciones de calidad actuales, año 2000. Colección Cuadernos de Medicina Reproductiva, editado por ANTONIO PELLICER y CARLOS SIMÓN. Ed. Panamericana, noviembre 2000.

COLLADO GARCÍA-LAJARA, Enrique. *Protección de datos de carácter personal* (legislación, comentarios, concordancias y jurisprudencia), Ed. Comares-Granada 2000.

DAVARA RODRÍGUEZ, Miguel Ángel. *Manual de Derecho Infor-*

mático, Ed. Aranzadi, (3.ª edición), septiembre 2001.

DEL POZO GUERRERO, Franciso y GÓMEZ AGUILERA, Enrique, J. «Telemedicina: una visión del pasado y del futuro», Revista *Todo Hospital* (Monográfico Telemedicina), julio-agosto 2001.

FERRER-ROCA, O. *Telemedicina'* Ed. Panamericana, mayo 2001.

FERRER-ROCA, O, J. A., ABREU REYES, R., ABREU GONZÁLEZ, M., SUÁREZ DELGADO, E., SOLA-RECHE.-CATAI (Centro de Alta Tecnología en Análisis de la Imagen), Tenerife. «Capacitación médica en la sociedad de la información.—Preparando la legislación para una revolución asistencial», *Revista Clín. Esp*. 2001.

GARCÍA MÁS, Francisco Javier. «La firma electrónica: Directiva y Real Decreto-Ley 14/1999, de 17 de septiembre», Revista *Actualidad Civil Aranzadi*, mayo de 2000.

HERNÁNDEZ, Carlos. «El secreto médico y la Agencia de Protección de Datos», artículo publicado en el *Diario Médico*, de fecha 8 de septiembre de 2000.

HERRANZ RODRÍGUEZ, Gonzalo. *Aspectos Éticos de la Telemedicina*, VII Congreso Nacional de Derecho Sanitario, Madrid, octubre de 2000. Ed. Fund. Mapfre Medicina, 2001.

HOUSE, ARTHUR M. Ciclo Primavera de la Salud, dedicado a la Telemedicina y organizado en Madrid por la Universidad Complutense, *Diario 16*, de 8 de junio de 2.000.

JIMÉNEZ RIUS, Pilar. «Antecedentes legislativos de la nueva Ley Orgánica de Protección de Datos Personales». Revista *Actualidad Administrativa* (La Ley) núm. 26.

LUCAS MURILLO DE LA CUEVA, Pablo. *La publicidad de los archivos judiciales y la confidencialidad de los datos sanitarios*, VII Congreso Nacional de Derecho Sanitario, Madrid, octubre de 2000. Ed. Fund. Mapfre Medicina, 2001.

MARCHENA GÓMEZ, Manuel. «El sabotaje informático: entre los delitos de daños y desórdenes públicos». Revista *Actualidad Informática Aranzadi*, julio 2001.

MARTÍNEZ SÁNCHEZ, Mar. *La Ley Orgánica 15/1999, de 13 de diciembre y la inscripción de ficheros (archivos del profesional sanitario)*, VII Congreso Nacional de Derecho Sanitario, Madrid, en octubre de 2000. Ed. Fund. Mapfre Medicina, 2001.

— «Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal», Revista *Actualidad Informática Aranzadi*, abril de 2000.

MARTÍN-CASALLO LÓPEZ, Juan José. *Derechos de acceso, rectificación y cancelación de los datos sanitarios en la LOPD*, VII Congreso Nacional de Derecho Sanitario, octubre de 2000. Ed. Fund. Mapfre Medicina, 2001.

MONTEAGUDO PEÑA, José Luis. «Telemedicina». Revista *Informática y Salud*, núm 29 (enero/febrero 2.001).

— «Modelos de implantación de telemedicina. Impulsores y barreras» Incluido en la Revista *Todo Salud*, julio-agosto 2001.

MURILLO DE LA CUEVA, Pablo Lucas. *La publicidad de los archivos judiciales y la confidencialidad de los datos sanitarios*, VII Congreso Nacional de Derecho Sanitario, Madrid, octubre de 2000. Ed. Fund, Mapfre Medicina, 2001.

PALAU, Enrique. «Telemedicina: un intento de aproximación desde lo sanitario». Revista *Administración Sanitaria*, Vol V, núm 19, julio-septiembre 2001.

PARERAS, LLUIS. G. *Aseguramiento y Medicina Virtual. Los nuevos desafíos*. (Actas del simposio celebrado en Madrid, el 17 de octubre de 2000). Ed. Fundación Sanitas y otros. Madrid, 2001.

POMPIDOU, Alain. Prólogo de la obra *'Telemedicina'* de OLGA FERRER-ROCA, Ed. Panamericana, mayo 2001.

RUBÍ NAVARRETE, Jesús. «Los códigos tipo: la alternativa de la autorregulación», Revista *Actualidad Informática Aranzadi*, abril de 2000.

SÁNCHEZ-CARO, Javier y SÁNCHEZ-CARO, Jesús. *El Médico y la Intimidad*, Editorial Diaz de Santos. Madrid, julio de 2001.

— «Ley de Protección de Datos e innovaciones tecnológica farmacéuticas», Revista *Administración Sanitaria*, julio-septiembre 2001.

SÁNCHEZ-CARO, Javier y ABELLÁN, Fernando. *La Historia Clínica*. Fundación Salud 2000, mayo 2000.

— *Imprudencia y negligencia en la profesión médica.* Fundación Salud 2000, Granada 2001.

STANBERRY, Benedict. Artículo: *Law, Ethics and Risk in Telemedicine*, VII Curso Catai, abril 2000.

TANGALOS, Eric G. *Telemedicina. La salud en el siglo XXI.* Estudio Editorial, 2001.

VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal.* Ed. Civitas, Primera Edición, 2001.

WALLACE, Simón. *La tecnología de la información: impacto en la política y gestión sanitaria del siglo XXI*. (Actas del simposio celebrado en Madrid, el 7 de octubre de 1999). Ed. JOAN JOSEP ARTELLS I HERRERO, JULIÁN RUÍZ FERRÁN y AURORA BERRA DE UNAMUNO. Madrid, 2000.

WILSON, Petra. (VII Curso Catai), *Infoethics-The European Perspective*, marzo 2000.

— *An overview of legal issues in European Telemedicine*. Octubre, 1998.

VIII

ÍNDICE DE AUTORES

NOTA RECORDATORIA DEL SERVICIO GRATUITO DE CONSULTAS JURÍDICAS

SERONO, a través de la FUNDACIÓN SALUD 2000 tiene concertado con DERECHO SANITARIO ASESORES un servicio jurídico de evacuación de consultas, de carácter gratuito para todos lo médicos, dirigido a responder a todas aquellas cuestiones que se susciten sobre responsabilidad civil y penal en el ámbito de la reproducción asistida, de la neurología, de la endocrinología pediátrica y de la inmunología.

Las consultas deben enviarse a DERECHO SANITARIO ASESORES, siempre por escrito, y con indicación del nombre y apellidos del consultante, su dirección, especialidad, teléfono, fax y, en su caso, correo electrónico.

Una vez recibidas en DERECHO SANITARIO ASESORES, un grupo de profesionales del derecho especializados en la materia, las contestarán por escrito y enviarán al médico consultante con la mayor celeridad posible y por el medio en que se hayan recibido, salvo que el interesado solicite su remisión por otro conducto distinto.

Todas las consultas quedan amparadas por el secreto profesional de la abogacía.

ENVIAR LAS CONSULTAS A:

«DERECHO SANITARIO ASESORES»
C/. O'Donnell, 43, 1.º A
28009 MADRID
Teléfono: 91-576.75.80. Fax: 91-577.28.33
Correo Electrónico: dchosanitario@wanadoo.es