ARTÍCULO ESPECIAL

La protección de datos en la práctica privada

José M.ª Dorado[a] y Jesús Fernández-Herrera[b]

[a]*Dermatólogo, práctica privada; abogado. Servicio de Dermatología. Hospital Universitario de La Princesa. Madrid. España.*
[b]*Jefe de Sección. Servicio de Dermatología. Hospital Universitario de La Princesa. Madrid. España.*

INTRODUCCIÓN

En los últimos años la práctica de la medicina ha cambiado sustancialmente. La relación entre médico y paciente, el núcleo más humano de la profesión médica, en uno de sus aspectos más importantes, la intimidad y el deber de secreto de los médicos se desarrollan hoy en día de una manera completamente diferente a como se hacía hace poco tiempo. Los recientes cambios tecnológicos y sociales que han dado lugar a la llamada *sociedad de la información y a la infoética* se han reflejado directamente en dicha relación. La tecnificación y aplicación de las nuevas tecnologías desempeñan hoy en día un papel fundamental en la práctica de la medicina y en la organización de las instituciones sanitarias. La burocratización, los cambios de valores y la gestión de la asistencia sanitaria, entre otros factores, ha influido en un cambio de rol del paciente y del médico, llegando a modificar la relación entre ambos. Se ha pasado de una relación basada en el principio ético de beneficencia o paternalismo (hacer todo por el paciente pero sin el paciente) a otra sustentada en el principio de autonomía, cuya implicación en la práctica clínica obliga al médico a contar con el paciente en la toma de decisiones. Esto ha dado lugar a un equilibrio en la relación médico-paciente, trasladándose a éste la responsabilidad de decidir sobre la forma de abordar su propia enfermedad, para lo cual es presupuesto ineludible la información terapéutica.

Hasta hace poco dicha relación se podía mantener aislada del entorno y del acceso a terceros con facilidad, simplemente con la obligación del médico de mantener el secreto profesional guardando silencio. Hoy en día la práctica médica en muchos aspectos es ya telemedicina (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), estática o interactiva, estando a la orden del día, por ejemplo, las *webs* sanitarias.

Producto de la evolución social es el tratamiento de los datos sanitarios, consecuencia directa del desarrollo tecnológico, con evidentes ventajas para el paciente y la organización sanitaria, pero si no se emplea correctamente puede dar lugar a que el derecho a la intimidad sea agredido por las nuevas fórmulas de utilización de su información personal. La autonomía del paciente frente a la obtención de datos sobre la salud, la confidencialidad de los mismos y la seguridad en su transmisión es una cuestión esencial. La protección de datos personales en el campo sanitario genera diversos problemas éticos y jurídicos que derivan del conflicto entre dicho derecho y los derechos a la salud y a la intimidad. Las nuevas técnicas de procesamiento y almacenamiento (antes físico, ahora principalmente informático) de la información generan un peligro potencial para la intimidad de los pacientes cuyos datos son recogidos. En el presente se están produciendo numerosos problemas éticos y jurídicos derivados de dos derechos fundamentales referidos al paciente: el derecho a la salud, por un lado, y los derechos a la intimidad y a la protección de los datos personales, por el otro.

Los profesionales sanitarios que desarrollan su actividad de manera individual y los centros sanitarios privados son responsables de la gestión y la custodia de la documentación asistencial que generen, debiendo proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o deban de ser tratados en los mismos de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

No es de extrañar por tanto, que cada vez con más frecuencia vayamos encontrando advertencias relacionadas con datos personales o datos de salud como por ejemplo *«contiene documentación bajo secreto médico. Declinamos toda responsabilidad criminal por violación de los derechos constitucionales de la persona»*.

NORMATIVA[1]

En la Comunidad Europea se ha ido desarrollando una extensa normativa que regula el tratamiento de

[1] Existen multitud de normas en el ámbito internacional, la Comunidad Europea y nuestro Derecho Interno relacionadas con la materia tratada en este artículo. Debido a ello se ha pretendido, por un lado, reseñar la normativa imprescindible que se ha ido desarrollando con relación a los datos personales y, por el otro, no hacer dicha relación exhaustiva. Como para hacer mínimamente comprensible el tema se ha seguido una relación en el tiempo, y en las sucesivas normas reseñadas aparecen expresiones cuyo alcance legal en prin-

datos personales, atendiendo a los derechos de las personas, la libre circulación de la información y la protección jurídica de las bases de datos. La norma de referencia es la directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a su libre circulación.

En el ámbito europeo el derecho a la protección de datos está basado en los principios de limitación de objetivos, proporcionalidad y calidad (adecuados, pertinentes y no excesivos o necesarios para el fin que se persigue, exactos y puestos al día) de los datos que se recaben, transparencia sobre su manejo, confidencialidad y seguridad del tratamiento automatizado. La reciente Constitución Europea recoge el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, que dichos datos se traten de modo leal, para fines concretos y sobre la base de consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley, y el derecho de acceso a los datos recogidos y a obtener su rectificación.

En la actualidad no existe en nuestro Derecho Interno una norma expresa que ampare las singularidades del tratamiento automatizado y protección de los datos de salud, por lo que se debe acudir a la Constitución española, a la doctrina del Tribunal Constitucional y a otras normas genéricas sobre tratamiento automatizado de datos personales. Las disposiciones legales básicas de la aplicación en esta materia son de carácter general, la Ley Orgánica de Protección de Datos de Carácter Personal de 1999 (en adelante LOPD) y el Reglamento de Medidas de Seguridad de 1999 (en adelante RMS). En general, la aplicación de las leyes tanto en el sector público como en el privado, los principios de protección de datos en cuanto al tratamiento de los mismos, así como los derechos específicos que concede la ley a los ciudadanos son de obligado cumplimiento para cualquier ciudadano que trate datos de carácter personal, con independencia de su naturaleza pública o privada. Las diferencias que se establecen en la LOPD son básicamente procedimentales (cómo debe realizarse una determinada actuación o gestión), dependiendo que el responsable de tratamiento sea uno u otro tipo de entidad.

CONSTITUCIÓN ESPAÑOLA Y DOCTRINA DEL TRIBUNAL CONSTITUCIONAL

La protección de los datos sobre la salud dentro de nuestro ordenamiento jurídico nace en nuestra Constitución, y tiene su máximo exponente en el artículo 18.4, en el que se señala lo siguiente: *«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»*.

El derecho fundamental[2] a la intimidad personal y familiar está dirigido a proteger a la persona frente a cualquier invasión que pueda realizarse en el ámbito de su vida personal y familiar. El derecho fundamental a la protección de datos busca garantizar a la persona un poder de disposición o control sobre sus datos personales, su uso y destino, impidiendo su tráfico ilícito y lesivo para su dignidad y derecho, lo que atribuye a su titular una serie de facultades jurídicas para imponer a terceros la realización u omisión de determinados comportamientos, como la obligación de informar sobre ciertos datos o rectificarlos, su cancelación, etc. Es decir, es un derecho que se traduce en la potestad de control sobre el uso que se hace de sus datos personales, permitiendo evitar que, a través del tratamiento de nuestros datos se pueda llegar a disponer de la información sobre nosotros que afecte a nuestra intimidad y demás derechos fundamentales y libertades públicas.

El Tribunal Constitucional tiene reconocido el derecho a la protección de datos personales como un derecho o libertad fundamental dotado de entidad propia, de carácter independiente, autónomo y distinto respecto del derecho general a la intimidad personal y familiar, dirigido a hacer frente a las potenciales agresiones a la dignidad y a la libertad de las personas producidas por el uso ilegítimo del tratamiento mecanizado de datos, estableciendo que «el derecho a la protección de datos no se reduce sólo a los datos íntimos de las personas, 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, porque su objeto no es sólo la intimidad individual».

Este derecho específico lo define como el derecho que tiene toda persona a controlar sus datos personales, lo que le faculta para decidir quién posee esos datos y para qué los va a usar, pudiendo oponerse a esa posesión o uso. Para el Tribunal Constitucional los datos amparados por el derecho fundamental a la protección de datos son todos aquellos de carácter personal, no referidos exclusivamente a los datos íntimos, que identifiquen o permitan la identificación de la persona, que pueden servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirven para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

La llamada *libertad informática* o el también denominado *derecho a la autodeterminación informativa* (construcción del Tribunal Constitucional Federal alemán)

cipio es desconocido (p. ej., fichero, dato de salud, cesión de datos, responsable del fichero, etc.), más adelante se procura aclarar su significado.

[2] Derecho irrenunciable; prevalece sobre otros derechos no fundamentales.

sería la potestad del particular de disponer y controlar la información que obra sobre su persona mediante datos insertos en un programa informático, su uso, difusión y manejo y la facultad de oponerse a que determinados datos personales sean utilizados para fines distintos del fin legítimo que justificó su recogida.

El único límite del derecho fundamental a la protección de datos son los demás derechos constitucionales y bienes jurídicos de rango constitucional; por tanto, no es un derecho absoluto, y se encuentran en colisión directa con él, entre otros, el derecho a la vida y el derecho a la salud, que priman sobre aquél.

Ley 14/1986, de 25 de abril, General de Sanidad

Recoge el deber de secreto al que están sometidas todas las personas que acceden a los historiales clínicos de los pacientes y el mandato a los poderes públicos para adoptar las medidas necesarias para garantizar en dichos pacientes sus derechos a la intimidad personal y familiar. Señala el derecho a la confidencialidad de toda la información relacionada con el proceso [médico] y con la estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público. La Ley General de Sanidad (en adelante LGS) establecía en su artículo 61 que la historia clínica debería estar a disposición de los enfermos y de los facultativos que directamente estuvieran implicados en el diagnóstico y el tratamiento del enfermo, así como a efectos de inspección médica o para fines científicos, y debe 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, tuviera acceso a la misma. Aunque este artículo está derogado, su contenido es recogido en términos similares en normas posteriores, de ahí su reseña.

Recomendación n.º 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre protección de datos médicos

Esta norma busca un equilibrio entre la protección que debe ser dispensada a la intimidad de las personas, lo que constituye uno de sus ejes básicos y, en el otro extremo, la salud pública. Aconseja a los gobiernos de los Estados miembros la regulación de la recogida y procesamiento de los datos médicos para salvaguardar la seguridad y confidencialidad de los datos personales relacionados con la salud, empleándose de acuerdo con los derechos y libertades fundamentales de las personas, especialmente con el derecho a la intimidad.

En su primer artículo se especifica qué debe entenderse por dato personal, dato médico y dato genético. El artículo tercero restringe la recogida y el procesamiento de datos médicos a los profesionales sanitarios, individuos u órganos que trabajen en su representación. Estos profesionales de los Estados parte del Consejo están sometidos a estrictas normas de confidencialidad, y su vulneración genera una sanción penal. Se permite la recogida y tratamiento de datos a otros profesionales (administrador de un archivo) siempre que queden sujetos a normas de confidencialidad idénticas a las que está sometido el personal sanitario.

Convenio para la protección de los derechos humanos y de la dignidad del ser humano con respecto a las aplicaciones de la biología y de la medicina hecho en Oviedo el 4 de abril de 1997

Este convenio, a diferencia de otras declaraciones internacionales que le han precedido, es el primer instrumento internacional con carácter jurídico vinculante para los países que lo suscriben, y a través de él se busca una armonización de las legislaciones de los diversos países en estas materias. En él se establece un marco común para la protección de los derechos humanos y la dignidad humana en la aplicación de la biología y la medicina, y se reconocen varios derechos de los pacientes, entre los que destacan el derecho a la información, el consentimiento informado y la intimidad de la información relativa a la salud de las personas.

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

En esta norma se recoge la obligación de adoptar los responsables de ficheros y, en su caso, los encargados de tratamiento, las medidas de seguridad de índole técnica y organizativa conducentes a garantizar la seguridad y confidencialidad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado. El nivel de protección para los ficheros automatizados que almacenan datos relativos a la salud es el más alto de los previstos, y están especialmente protegidos, lo que constituye el grado máximo de seguridad exigible. Igualmente, se precisa la elaboración de un documento de seguridad, de obligado cumplimiento para todo el personal con acceso a los datos, y en el que se deben regular todos los aspectos relacionados con la seguridad.

Entre las medidas técnicas que conlleva el nivel alto de protección aplicable a los datos sanitarios resalta el de la obligatoriedad del cifrado de dichos datos o mecanismo similar, tanto en la distribución de los soportes informáticos que los contienen como en su transmisión a través de redes de comunicaciones, con la finalidad de garantizar que la información no sea inteligible ni manipulable por terceros. Igualmente, en relación con los datos sanitarios, es obligado un

registro de accesos, en el que se debe guardar en relación con cada acceso, la identificación del usuario, fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si fue autorizado o denegado. El periodo mínimo de conservación de los datos registrados es de 2 años.

La seguridad de las comunicaciones por las que circulan datos sobre salud de las personas constituye un imperativo ético. La salvaguarda de la protección en este campo respecto a los estándares de seguridad y control de los sistemas de información, requiere el uso de tecnología de encriptación y utilización de redes cerradas.

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento de los Datos de Carácter Personal (en adelante LORTAD) inicia la regulación de los datos personales en nuestro país, ajustándose tanto a las previsiones del Convenio Europeo para la protección de los derechos fundamentales de las personas (Convenio de 4 de noviembre de 1950) como al Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108 del Consejo de Europa, de 28 de junio de 1981).

La evolución en la regulación del derecho a la protección de datos llevará al Parlamento Europeo y al Consejo de la Unión Europea a adoptar la directiva 95/46/CE, antes citada, cuya transposición a la legislación española se realizará mediante la LOPD.

La LOPD tiene como objeto *«garantizar y proteger, en lo concerniente al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar»*. Su ámbito de aplicación son ley *«los datos de carácter personal* (sean o no íntimos) *registrados en soporte físico* (no en sentido estricto ficheros electrónicos o informáticos, sino también los recogidos en papel, microfichas o cualquier otro que pueda ser objeto de utilización) *que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados»*. Por tanto, se aplica a cualquier tratamiento, con independencia de su soporte.

Se excluyen del ámbito de aplicación de la ley los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. Respecto a los ficheros manuales (la mayoría de historias clínicas) se confiere un plazo hasta el 24 de octubre de 2007 para su automatización.

La entrada en vigor de la ley estableció importantes obligaciones a las que quedan sujetos los profesionales autónomos y las personas jurídicas que, debido a su trabajo, tratan datos personales, así como un régimen severo de sanciones en caso de su incumplimiento (artículo 45), por lo que desde un punto de vista práctico, cualquier profesional de la salud que trate datos de carácter personal está obligado a tomar una serie de medidas de seguridad que garanticen los derechos de los titulares de dichos datos. Dicha ley es la norma principal sobre la que se articula el régimen jurídico relacionado con la protección de datos de carácter personal en España.

Para aplicar y adecuarse a la LOPD, las comunidades autónomas, transferidas las competencias del Instituto Nacional de la Salud, los hospitales, centros sanitarios privados y profesionales autónomos se deben adecuar a su cumplimiento, especialmente en su vertiente informática, y deben garantizar la confidencialidad de los datos sanitarios frente a terceros. Debido a ello, la mayoría de las comunidades autónomas han ido aprobando leyes sanitarias que regulan los tratamientos de datos sanitarios.

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Esta ley desarrolla los principios de calidad, información, consentimiento y seguridad de los datos en el campo de la información y documentación clínica. Para la ley *«toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y documentación clínica debe ser orientada por la dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad»*.

En esta norma se recoge también el principio de calidad de los datos almacenados en la historia clínica (en adelante HC), definiéndose, igualmente, su contenido mínimo.

HISTORIA CLÍNICA

En España está regulada en la LGS, que incluyó el derecho del paciente frente a las administraciones públicas sanitarias a que quedara constancia por escrito de su proceso asistencial, y se estableció el principio de historia clínico-sanitaria única en el Real Decreto 63/1995 y en la proposición de Ley 622/000010, *«debiendo quedar plenamente garantizado el derecho del enfermo a su intimidad personal y familiar y el deber de guardar secreto por quien, en virtud de sus competencias tenga acceso a la HC»*.

La HC es una *«prestación sanitaria»* (apartado 11 del art. 10 de la LGS y el punto 6 del apartado 5.º del anexo I del RD 63/95) y, en otro sentido, según la LOPD, un fichero de datos personales sometido a las medidas de seguridad de nivel alto si está informatizada. La HC, sea manual o electrónica, debe recoger exclusivamente la información clínica necesaria para asegurar, bajo un criterio médico, el conocimiento veraz, exacto y actualizado del estado de salud del paciente.

La Ley 41/2002, Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica define a la HC como el *«conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial»*. La HC *«comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos...»*

Todo paciente tiene derecho a que quede constancia, por escrito o en soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales realizados por el servicio de salud, tanto en el ámbito de la atención primaria como de la atención especializada. El consentimiento será verbal por regla general y sólo se prestará por escrito en los casos de intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, cuando se trate de aplicación de procedimientos que supongan riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente, y otros como los trasplantes, la reproducción humana asistida o los ensayos clínicos. La HC debe incorporar la información que se considere transcendental para el conocimiento veraz y actualizado del estado de salud del paciente.

Tienen acceso a la HC los profesionales sanitarios del centro que realiza el diagnóstico o el tratamiento del paciente. El personal de administración y gestión de los centros sanitarios sólo pueden acceder a los datos de la HC relacionados con sus propias funciones. Se puede acceder a ella con fines epidemiológicos, de salud pública, investigación o docencia, preservándose en todos ellos los datos de identificación personal del paciente, o con fines judiciales, estando para lo que dispongan los jueces y tribunales en el proceso que dé origen a su acceso.

El paciente tiene el derecho de acceso a la documentación de la HC y a obtener una copia de los datos que figuren en ella, obligación que afecta tanto al centro sanitario público como al privado. Este derecho del paciente tiene como límites el derecho a la confidencialidad de los datos aportados por terceros y las anotaciones personales de los médicos que no constituyan propiamente juicios clínicos, que pueden oponer al derecho de acceso la reserva de sus observaciones, apreciaciones o anotaciones subjetivas.

La Ley de Autonomía del Paciente señala: *«cada centro archivará las HC de sus pacientes, cualesquiera sea el soporte, papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información»*.

La protección de la HC es esencial, y lleva implícito el deber de confidencialidad impuesto por el secreto profesional y la protección de datos regulada en la normativa. La HC genera derechos (p. ej., derecho de acceso a la información) y deberes en las instituciones, los profesionales sanitarios, personal administrativo y pacientes, que pueden entrar en conflicto. Se puede acceder a la HC con fines judiciales, de inspección, epidemiológicos, de seguridad, salud pública, investigación o docencia. El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las HC. La ley establece un plazo básico de custodia, y señala que los centros sanitarios están obligados a conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, y como mínimo 5 años desde la fecha del alta de cada proceso asistencial.

La HC se regula, además, por autonomías. Así, por ejemplo la normativa de las Comunidades Autónomas del País Vasco, Cataluña y Galicia delimitan su contenido y los documentos que deben contener.

Propiedad, conservación y custodia

En la consulta privada, la propiedad corresponde al médico, si trabaja por cuenta propia, o al centro sanitario. Con relación a la propiedad, la Ley Gallega establece que la propiedad corresponde al médico que realiza la atención sanitaria: *«la entidad o facultativo propietario es responsable de la custodia de las historias clínicas y habrá de adoptar todas las medidas precisas para garantizar la confidencialidad de los datos o de la información contenida en las mismas»*.

La conservación y custodia es responsabilidad del médico que presta sus servicios por cuenta propia. El periodo de conservación de las HC varía según la regulación de cada comunidad autónoma.

Acceso a la información contenida en la historia clínica

El paciente, según el amparo que la LGS reconoce a su derecho de información, tiene derecho a acceder al contenido de la misma si lo solicita. Este derecho no es absoluto, ya que encuentra sus límites en el derecho a la intimidad y confidencialidad de terceras personas (que afecte a la intimidad del fallecido, o bien las anotaciones subjetivas de los profesionales o si se perjudica a terceras personas).

Igualmente, tienen acceso a la misma los profesionales sanitarios, el personal de administración y terceras personas (finalidades epidemiológicas, de salud pública, investigación, docencia, seguridad, judiciales), estando sujetos al deber de secreto y de confidencialidad de los datos del paciente.

Sólo se facilitará el acceso a la HC de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. El acceso de terceros motivados por riesgos para su salud se limita a los datos pertinentes.

Informatización de la historia clínica

La informatización de la HC debe sustentarse en los preceptos de la LOPD. La HC informatizada tiene el mismo valor jurídico que en soporte papel, aunque en el caso de la informatización entra en juego el artículo 18.4 de la Constitución española, que limita 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.

El artículo 4.7 de la Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias señala como uno de los principios del ejercicio de las profesiones sanitarias, que *«existirá formalización escrita de su trabajo* (profesionales sanitarios) *reflejada en una HC que deberá ser común para cada centro y única para cada paciente atendido en él. La HC tenderá a ser soportada en medios electrónicos y a ser compartida entre profesionales, centros y niveles asistenciales»*.

DATO PERSONAL. DATO DE SALUD. DATO MÉDICO

La LOPD define el dato personal como *«toda información relativa a una persona física identificada o identificable»*. Por tanto, es un dato de carácter personal *«cualquier información* (numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo) *susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable»*, es decir, todos aquellos referidos a personas físicas, a partir de los cuales se puede obtener información sobre los hábitos, preferencias, vida privada, etc., de los individuos, como el nombre, el teléfono o la dirección del correo electrónico. El elemento fundamental para determinar que se trata de un dato personal es que la información, combinada o por sí misma, permita conocer datos de una persona concreta, bien por estar directamente identificada a través de algún dato, o porque pueda llegar a ser identificable por otro medio.

Se considera identificable (Directiva 95/46/CE) *«toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social»*.

No está claramente determinado por la legislación española (LOPD y las normas que la desarrollan) qué se considera dato de salud o dato médico, lo que se puede y no es necesario proteger. En el artículo 7 de la LOPD se consideran los datos de salud (pero no los define) como datos especialmente protegidos, al igual que los datos referentes a ideología, afiliación sindical, religión, creencias, origen racial, vida sexual, infracciones penales o administrativas. Dicha protección acarrea criterios más estrictos en el uso, tratamiento y cesión de los datos, y medidas de seguridad por adoptar en los ficheros en los que se contengan dichos datos. El dato de salud es personal cuando está íntima y directamente relacionado con un ser humano en concreto.

En la recomendación n.º 5 se califica el dato médico como un dato personal referido a la salud de las personas físicas, y se define como *«todos los datos de carácter personal relativos a la salud de la persona, comprendiendo igualmente los que tengan una manifiesta y estrecha relación con la salud, así como con las informaciones genéticas»*.

Se puede, a partir de lo anterior, estimar como dato médico cualquiera de carácter personal que esté relacionado con la salud de un individuo. El concepto de dato sanitario debe entenderse de forma amplia, abarcando todos aquellos datos que de alguna forma, directa o indirectamente, se refieran a la salud de las personas o guarden relación con ella.

FICHERO

La LOPD define el fichero como *«todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso»*. No se trata sólo de ficheros integrados en sistemas informáticos o telemáticos, sino también de ficheros manuales o información personal recogida en soportes manuales, como ficheros de fichas manuscritas o similares que pueden estar archivados en armarios, cajones o estanterías, siempre que los datos se encuentren estructurados u organizados por algún criterio que permita acceder fácilmente a los datos de determinada persona.

RESPONSABLE DEL FICHERO. ENCARGADO DE TRATAMIENTO. USUARIO

Responsable del fichero o tratamiento

Según la LOPD, responsable del fichero es la *«persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso de tratamiento»*. El responsable del fichero es quien decide la creación del mismo, para qué se va a utilizar y el uso que se le va a dar. Está obligado a dar respuesta a los ciudadanos ante el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición. Las obligaciones del titular del fichero se centran en tomar todas las medidas necesarias orientadas a impedir el abuso o mal empleo de la información, así como a hacer un tratamiento de los datos legal y leal. Si el responsable del fichero es una persona o empresa privada, será aquél sobre quien recaigan las posibles sanciones pecuniarias en caso de comisión de infracciones a la legislación sobre protección de datos personales, sin perjuicio de la responsabilidad di-

recta del autor de la infracción, si lo hubiera. Dentro del ámbito de los ficheros de titularidad pública, el responsable del fichero siempre es un órgano administrativo.

Toda persona que mantenga un archivo con datos de carácter personal está obligada, entre otros deberes, a:

1. Inscribir el fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos (en adelante AEPD).
2. Tratar de forma legal y leal los datos de carácter personal en todas las fases (recogida, utilización, cesión, etc.).
3. Facilitar el ejercicio de los derechos al afectado.
4. Mantener el deber de secreto.
5. Adoptar las medidas de seguridad que marca la Ley.

Encargado de tratamiento

La LOPD lo concreta como 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»* (p. ej., empresa con la que se establece una relación contractual para que se encargue de la destrucción de los documentos que contienen datos de carácter personal en los archivos de un médico).

USUARIO

Usuario es cualquier persona al servicio del responsable del fichero o encargado de tratamiento que tenga acceso a los datos de carácter personal como consecuencia de tener encomendadas tareas de utilización material de datos almacenados o que se almacenen en los ficheros. Está obligado al cumplimiento de las medidas de seguridad establecidas para el tratamiento de datos y sujeto al deber de secreto.

No debe confundirse la figura legal del usuario de los datos personales o tratamiento de datos recogida en la LOPD con la del usuario de una prestación sanitaria, que según la Ley de Autonomía del Paciente es *«la persona que utiliza los servicios sanitarios de educación y promoción de salud, de prevención de enfermedades y de información sanitaria»*.

PROCEDIMIENTO DE DISOCIACIÓN

Para la LOPD es *«todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable»*. Cuando los datos personales no permiten la identificación de una persona concreta pierden el carácter de personales y quedan al margen de la normativa sobre protección de datos. Igualmente, la utilización de este procedimiento, con carácter previo al acceso y tratamiento de datos, exime de la exigencia de solicitar el consentimiento del interesado para poder utilizar dichos datos en el tratamiento previsto.

TRATAMIENTO DE DATOS DE SALUD. CESIÓN. COMUNICACIÓN

Obtención y tratamiento

La LOPD recoge el marco jurídico del tratamiento de datos. La ley, en sentido general, aumenta las garantías de los titulares de datos personales, mediante el deber de información previa y la necesidad de contar, como norma general, con el consentimiento para el tratamiento de los datos personales, incluida la cesión o comunicación. En los casos en los que no es necesario el consentimiento del interesado, éste tiene derecho a oponerse a dicho tratamiento.

La LOPD define tratamiento de datos de carácter personal como *«todas las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación de datos, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias»*.

Los datos personales que hagan referencia a la salud pueden ser tratados, sin necesidad del consentimiento del afectado, si dicho tratamiento tiene por finalidad proteger un interés vital del interesado como el necesario para la prevención o 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 a una obligación equivalente de secreto. De igual forma la ley recoge que las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

El artículo 25 de dicha ley permite la creación de ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que la ley establece para la protección de las personas.

Cesión de datos de salud

La LOPD señala como cesión o comunicación de datos *«toda revelación de datos realizada a una persona dis-*

tinta del interesado (persona física titular de los datos que sean objeto del tratamiento)». Por tanto, es cesión una simple consulta que un tercero realice a estos datos, aunque sea a distancia y sin creación de un fichero o tratamiento nuevo. Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la ley.

La cesión de datos de salud requiere el consentimiento previo del interesado, excepto, cuando dicha cesión sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

MEDIDAS DE SEGURIDAD DE LOS FICHEROS QUE CONTIENEN DATOS DE SALUD

La LOPD obliga al responsable del fichero y en su caso, al encargado del tratamiento, a adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal, evitar su alteración o pérdida y tratamiento o acceso no autorizado. Dichas medidas las ha desarrollado el RMS, reglamento de seguridad que tiene por objeto el establecimiento de medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la LOPD.

El responsable del fichero es el centro sanitario, institución, consulta privada o médico que decida sobre la finalidad del mismo. Los usuarios del sistema de información o personal son los facultativos y demás personal sanitario y terceras personas que, sin ser personal sanitario, quedan sujetas a las mismas obligaciones de confidencialidad que los anteriores.

Las medidas de seguridad exigibles se clasifican en tres niveles (básico, medio y alto), establecidos atendiendo a la naturaleza de la información tratada y en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de los datos recogidos. En cuanto a los datos de salud, los ficheros que los contengan deben cumplir las medidas de seguridad del nivel alto. El hecho de que un determinado fichero sea temporal (p. ej., información que un médico guarda en su ordenador personal) no exime a su responsable de la obligación de implantar las medidas de seguridad que le corresponden atendiendo a su contenido. El RMS recoge la obligación de borrar los ficheros una vez que los datos contenidos dejen de ser necesarios para los fines que motivaron su creación.

NIVELES DE SEGURIDAD DE LOS FICHEROS

	Medidas de seguridad exigibles		
	Básico	*Medio*	*Alto*
Documento de seguridad	*	*	*
Funciones y obligaciones del personal	*	*	*
Registro de incidencias	*	*	*
Identificación y autentificación	*	*	*
Control de acceso	*	*	*
Gestión de soportes	*	*	*
Copias de respaldo y recuperación	*	*	*
Responsable de seguridad		*	*
Control de acceso físico		*	*
Auditoría periódica		*	*
Pruebas con datos reales		*	*
Distribución de soportes			*
Registro de acceso			*
Telecomunicaciones		*	

Tomada y modificada de *Guía de Protección de Datos Personales para Colegios Profesionales*. Agencia de Protección de Datos de la Comunidad de Madrid.

DOCUMENTO DE SEGURIDAD

El responsable del fichero que contenga datos de salud (especialmente protegidos, nivel máximo de seguridad) y, en su caso, el encargado del tratamiento, deberán elaborar e implantar la normativa de seguridad mediante un documento de seguridad de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información. Dicho documento puede contener la normativa de seguridad para todos los ficheros de los que es responsable la organización o bien se pueden redactar tantos documentos como ficheros se posean. El documento tiene que mantenerse en todo momento actualizado, adecuado a las disposiciones vigentes en materia de seguridad de datos de carácter personal y ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, y debe recoger, como mínimo:

1. La identificación del responsable o responsables de seguridad.
2. El personal que podrá tener entrada a los locales donde de encuentran ubicados los sistemas de información con datos de carácter personal, siendo dicho personal el único que puede acceder a tales datos.
3. El ámbito de aplicación del mismo, con especificación detallada de los recursos protegidos.
4. Las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el grado de seguridad exigido en el RMS y los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Las funciones y obligaciones del personal, que deberán estar claramente definidas y documentadas. El responsable del fichero debe adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones y las consecuencias que deriven de su incumplimiento.

6. La estructura de los ficheros con datos de carácter personal y la descripción de los sistemas de información que los tratan.

7. El procedimiento de notificación, gestión y respuesta ante las incidencias. Debe registrarse el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos producidos por dicha comunicación.

8. Los procedimientos de realización de copias de respaldo y de recuperación de datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos han sido necesarios grabar manualmente en el proceso de recuperación. Es necesaria la autorización por escrito del responsable del fichero o tratamiento para la ejecución del procedimiento de recuperación de datos. Igualmente, deben constar en el documento las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado, y debe impedirse cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda su baja en el inventario.

El responsable del fichero debe encargarse de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información, el tipo de acceso al que están autorizados y establecer procedimientos de identificación y autentificación para dicho acceso. Los usuarios deben tener acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, y el responsable del fichero debe establecer los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos o permisos distintos de los autorizados.

Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad. Deben conservarse sendas copias de respaldo y de los procedimientos de recuperación de datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan. Debe establecerse un sistema de registro de entrada y de salida de soportes informáticos que permita conocer el tipo de soporte, fecha y hora, el emisor o destinatario, el número de soportes, tipo de información que contienen, la forma de envío y la persona responsable de la recepción o de la entrega, que deberán estar debidamente autorizados. La salida de soportes informáticos que contengan datos de carácter personal fuera de los locales en los que esté ubicado el fichero sólo puede ser autorizada por el responsable del mismo, y se deben adoptar las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

La distribución de los soportes debe realizarse cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte. Cuando la transmisión de datos se realice a través de redes de telecomunicaciones de titularidad ajena a la propia empresa, se debe llevar a cabo cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

De cada acceso se debe guardar la identificación del usuario, la fecha y hora en que se realizó, el tipo de acceso y si ha sido autorizado, y es preciso conservar la información que permita identificar el registro accedido, o denegado.

El responsable del fichero debe implantar una clave personal intransferible para cada usuario del sistema y designar uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. El responsable de seguridad controla directamente los mecanismos que permiten el registro de los datos, y tiene que revisar periódicamente la información de control recogida y elaborar un informe de las revisiones realizadas y los problemas detectados una vez al mes.

Los sistemas de información e instalaciones de tratamiento de datos deben someterse, al menos cada 2 años, a una auditoría interna o externa, para verificar el cumplimiento del RMS y de las instrucciones y procedimientos vigentes en materia de seguridad de datos, y se debe plasmar en un informe de auditoría que debe dictaminar sobre la adecuación de dichas medidas y controles, identificar las deficiencias y proponer las medidas correctoras y/o complementarias necesarias. Estos informes deben ser analizados por el responsable de seguridad, que debe elevar las conclusiones al responsable del fichero para que adopte las medidas subsanadoras adecuadas. Se establece un periodo mínimo de conservación de los datos registrados de 2 años.

PRINCIPIOS QUE RIGEN EL TRATAMIENTO DE DATOS PERSONALES

Recogidos por la LOPD, son de obligado cumplimiento y la base del tratamiento de datos personales. El responsable del fichero y/o el encargado del tratamiento son los garantes de que cualquier tratamiento de datos se adapte a dichos principios; su incumplimiento es motivo de sanción.

Principio de la calidad de los datos

Los datos de carácter personal sólo pueden recogerse para su tratamiento cuando sean adecuados,

pertinentes y no excesivos (no en el sentido de cantidad, sino en el de proporcionalidad) para el cumplimiento de las finalidades del fichero, que deben estar determinadas de forma explícita y ser legítimas. Los datos no pueden ser utilizados para propósitos incompatibles con los que motivaron su recogida (para la ley nunca son incompatibles los fines históricos, estadísticos o científicos).

Los datos personales han de ser exactos y mantenerse al día; en caso contrario, tienen que ser cancelados, rectificados o completados. Deben ser cancelados cuando hayan dejado de ser pertinentes o necesarios. No pueden conservarse de forma que permitan la identificación del interesado durante un periodo superior al necesario para la finalidad por la que fueron solicitados o registrados. Hay que almacenarlos de forma que permitan el ejercicio al derecho de acceso, salvo que sean legalmente cancelados.

Principio de información de recogida de datos

El paciente ha de ser advertido de manera expresa, precisa e inequívoca de que los datos médicos que a él le afectan van a ser recogidos en un fichero, así como de la finalidad y el destino o destinatarios de los mismos. La información debe facilitársele, antes de prestar su consentimiento, por cualquier medio (palabra, escrito, formulario, documento, etc.) y se le debe indicar, además:

1. La identidad y el responsable del fichero.
2. Si es obligatoria o no su respuesta a las distintas preguntas planteadas.
3. Las consecuencias de la obtención de los datos o de su negativa a suministrarlos.
4. La posibilidad de que pueda ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

Principio de consentimiento[3]

La LOPD exige la prestación de consentimiento previo e inequívoco del afectado para el tratamiento de sus datos, aunque establece una serie de excepciones, que no eximen de la obligación de informar, ni permite el tratamiento de cualquier dato, sino aquellos que cumplan el principio de calidad.

Principio de datos especialmente protegidos o «sensibles»[4]

La LOPD prevé la necesidad de proteger especialmente los datos que, por la información a que se refieren, pueden generar con mayor facilidad lesiones en otros derechos fundamentales, además del propio derecho a la protección de datos. Estos datos son los relativos a ideología, afiliación sindical, religión o creencias, origen racial, salud y vida sexual, y los relacionados con la comisión de infracciones penales o administrativas. Dicha protección se concreta en las siguientes características:

1. Como norma general se exige el consentimiento expreso y por escrito del afectado para la recogida y uso de estos datos.
2. Se precisa el establecimiento de medidas de seguridad de nivel alto para los ficheros que los contienen.
3. Las infracciones concernientes a estos datos son consideradas más graves.

Principio de seguridad de los datos

1. El responsable del fichero debe tomar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales integrados en los ficheros con el fin de evitar que éstos puedan perderse, alterarse, usarse o ser accesibles por personas no autorizadas.
2. Las medidas de seguridad que adoptar deben recogerse en el *documento de seguridad* y darse a conocer a todos los usuarios del sistema de información, quienes están obligados a cumplirlo. Dicho documento debe reflejar el grado de seguridad que debe cumplir el fichero.

Deber de secreto

Se exige al responsable del fichero, al encargado del tratamiento si lo hubiera y a todos los que intervengan en cualquier fase del tratamiento, obligación que se mantiene incluso finalizada la relación que permitió el acceso al fichero. Este deber de secreto es un deber genérico que alcanza a cualquier persona que intervenga en el proceso de datos y que no debe confundirse con el secreto profesional. Se ha producido una ampliación de los sujetos tradicionales con obligación de confidencialidad en el campo de los datos sobre la salud, dado que ahora recae en cualquier persona física o jurídica que tenga acceso a la información, por lo que afecta al médico, sanitarios, personal de la administración, responsable y/o encargado del tratamiento de datos, al proveedor del servicio de telecomunicaciones que comparte la información y a cualquier usuario que acceda a ellos.

El secreto profesional del médico puede entrar en pugna con el derecho a la tutela judicial efectiva de otro ciudadano, y plantearse un conflicto entre éste y el derecho a la intimidad y a la protección de datos personales.

[3] La LOPD excepciona los datos recogidos en el seno de la atención asistencial por un profesional sanitario; en estos casos el tratamiento de los datos especialmente protegidos puede realizarse amparado en un consentimiento tácito e implícito en la propia relación asistencial.

[4] Ídem que la anterior.

DERECHOS DE LAS PERSONAS EN RELACIÓN CON LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Derecho de consulta al Registro General de Protección de Datos

Faculta a cualquier persona a recabar información sobre la existencia de ficheros de datos de carácter personal inscritos en los registros, la finalidad de éstos y la identidad del responsable del fichero. El ejercicio de este derecho es público y gratuito.

Derecho de acceso

Derecho a conocer los datos que sobre su persona figuren en un fichero determinado sometidos a tratamiento, cuál ha sido su origen y qué cesiones se han realizado o se prevé realizar en el futuro. El ejercicio de esta facultad es gratuito, pero sólo se puede realizar una vez cada 12 meses, salvo que se acredite un interés legítimo *(causa justificada)*.

Derecho de oposición

Oposición de la persona, una vez informada, al tratamiento de sus datos cuando existan motivos fundados y legítimos relativos a una situación personal concreta.

Derecho de rectificación y cancelación

Suponen la facultad del interesado a instar al responsable del fichero a rectificar o cancelar los datos cuyo tratamiento no se ajuste a la ley, en particular, los datos inexactos o incompletos, inadecuados o excesivos o si no existiera derecho a registrarlos. La cancelación da lugar al bloqueo de los datos, pero no necesariamente al borrado físico de la información, dado que a veces los datos deben conservarse hasta que prescriban (p. ej., para disposición judicial).

Derecho de impugnación de valoraciones

Permite al interesado impugnar aquellas decisiones que tengan efectos jurídicos y cuya base sea únicamente un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Derecho a indemnización

Si a consecuencia del incumplimiento de la Ley una persona sufre daño o lesión en sus bienes o derechos, tiene derecho a solicitar una indemnización económica, instada ante la jurisdicción ordinaria cuando la lesión provenga de entidades privadas.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y AGENCIAS DE LAS COMUNIDADES AUTÓNOMAS

Creada por la derogada LORTAD y regulada en la LOPD, es la instancia a la que pueden acudir los afectados para ser tutelados en el ejercicio de sus derechos, y se configura como el órgano de control del cumplimiento de la LOPD. Es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que ejerce sus funciones con entera independencia de las Administraciones públicas. Por tanto, es un organismo independiente que, entre otras funciones, vela por el cumplimiento y aplicación de la legislación sobre protección de datos.

Esta agencia lleva a cabo acciones normativas, dicta las instrucciones (disposiciones de carácter general con objeto de aclarar y apoyar la interpretación de la ley) precisas para adecuar el tratamiento de los datos a los principios contenidos en la ley. La AEPD ha optado por una interpretación amplia de los preceptos y conceptos recogidos en la LOPD, siempre que dicha interpretación implique el favorecimiento de la defensa de la intimidad y privacidad de las personas.

Entre sus funciones figura la potestad inspectora (de oficio y a instancia de parte) y sancionadora en los términos previstos en la ley. Atiende peticiones y reclamaciones de los ciudadanos y les informa sobre sus derechos. Ordena el cese de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se ajusten a las disposiciones de la ley, ejerce el control y adopta las autorizaciones que procedan en relación con los movimientos internacionales de datos, etc.

Como un órgano integrado en ella se encuentra el Registro General de Protección de Datos, en el que deben inscribirse, entre otros, los ficheros de titularidad de las Administraciones Públicas y los de titularidad privada, y al que compete velar por la publicidad de la existencia de los ficheros para hacer posible el ejercicio de los derechos de información, acceso, rectificación, oposición y cancelación amparados por la ley.

La distinción entre ficheros públicos y privados es importante, ya que el régimen jurídico previsto en la LOPD para ellos varía. Es de aplicación a los ficheros públicos un conjunto de excepciones a la regulación general, como la relativa al consentimiento para el tratamiento de datos personales y para la cesión de éstos o los límites al derecho de cancelación. El procedimiento para la creación de ficheros y el de infracciones y sanciones de la ley es distinto. Los ficheros públicos se crean a través de una disposición de carácter general que tiene que ser publicada en un diario oficial, mientras que los ficheros privados se crean a través de una notificación de la AEPD. Las infracciones en el caso de los ficheros privados llevan aparejadas un régimen de sanciones económicas ele-

vado, mientras que las infracciones en el ámbito de los ficheros públicos dan lugar, principalmente, a una resolución que declara la infracción administrativa, la comunicación al defensor del pueblo y al superior jerárquico de la persona que ha cometido la infracción y la propuesta de apertura del procedimiento disciplinario.

Existen agencias de protección de datos de carácter autonómico (p. ej., en las comunidades de Madrid y Cataluña) con funciones de control, vigilancia, inspección, labores de colaboración, consultoría y resolución de consultas, publicaciones, etc. Así, por ejemplo, la Agencia de Protección de Datos de la Comunidad de Madrid tiene un servicio de asesoramiento para facilitar el cumplimiento de las obligaciones derivadas de la legislación de protección de datos que incluye la resolución de consultas sobre casos concretos e, igualmente, ha realizado distintos programas de formación, comisiones de seguimientos, grupos de trabajo, etc., y dispone de una revista digital de suscripción gratuita.

Las competencias de estas agencias autonómicas están restringidas a los ficheros de datos personales creados o gestionados por las comunidades autónomas o por la Administración local de su ámbito territorial. Pueden crear sus propios registros de protección de datos para ficheros de su competencia, aunque todos los ficheros y tratamientos de titularidad pública tienen que figurar inscritos en el Registro General de Protección de Datos. Las agencias de protección de datos de las comunidades autónomas sólo pueden ejercer sus competencias de control sobre los ficheros creados o gestionados para el ejercicio de potestades de derecho público y de competencias administrativas, es decir, para el ejercicio de funciones públicas, y es necesario que la entidad de derecho público desarrolle competencias reconocidas a la comunidad en su Estatuto de autonomía y que hayan sido debidamente transferidas. El control de los ficheros privados corresponde a la AEPD, al igual que los ficheros de la propia Administración General del Estado que se mantengan en el territorio de una comunidad autónoma. Los ficheros utilizados en funciones privadas deben inscribirse exclusivamente en el Registro General de Protección de Datos de la AEPD.

CÓDIGO PENAL DE 1995. SANCIONES DE LA AEPD

El Código Penal castiga con penas de prisión de 1 a 4 años y multa de 12 a 24 meses *«al que sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado»*. Se imponen iguales penas a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. Además, se considera como agravante, si la revelación afecta a datos de carácter personal que se refieran a la salud de las personas.

Igualmente, con relación a los datos personales, un médico con consulta privada o que desempeña sus funciones en un centro privado o concertado puede incurrir en delito de vulneración de secreto profesional tipificado en el Código Penal.

Por último y en relación con las infracciones calificadas en la LOPD como leves, graves y muy graves, ya han sido impuestas en España por la AEPD sanciones de más de 400.000 euros, y se puede llegar, si la infracción se comete en el ámbito privado, a más de 600.000 euros.

ADDENDUM

Temas como datos genéticos (datos especialmente vulnerables y con medidas adicionales de seguridad), investigación clínica, biotecnología, clonación, técnicas de reproducción humana asistida, ensayos clínicos, firma electrónica, receta médica, TAIR (Terminal Autónomo de Identificación del Paciente en las Recetas), firma electrónica, transferencia internacional de datos personales, códigos tipo, etc., se han dejado al margen en este artículo, circunscrito a la consulta privada, principalmente por problemas de extensión del mismo.

Declaración de conflicto de intereses

Declaramos no tener ningún conflicto de intereses.

BIBLIOGRAFÍA RECOMENDADA

Agencia de Protección de Datos de la Comunidad de Madrid: Guía de protección de datos personales para Colegios Profesionales. Civitas Ediciones, S.L. 2004.

Davara Rodríguez MA. El abogado y la protección de datos. Ilustre Colegio de Abogados de Madrid. 2004.

De Lorenzo R, Díaz Pérez JL, Díaz Díaz RM, et al. Información, consentimiento y documentación clínica en Dermatología. Ricardo de Lorenzo y Montero, Editores Médicos, S.A. 2005.

De Miguel Sánchez N. Secreto médico, confidencialidad e información sanitaria. Marcial Pons, ediciones jurídicas y sociales, S.A. 2002.

De Miguel Sánchez N. Tratamiento de datos personales en el ámbito sanitario: intimidad *versus* interés público. Editorial Tirant lo Blanch. 2004.

Hernández Martínez-Campello C, Suárez García E. Preguntas y respuestas sobre la Ley 41/2002, que regula diversos aspectos de la relación médico-paciente. Fundación del Ilustre Colegio Oficial de Médicos de Madrid. 2004.

Ilustre Colegio Oficial de Médicos de Madrid. La responsabilidad civil y penal del médico. Ilustre Colegio Oficial de Médicos de Madrid. 1999.

Jañez Ramos FM, Puente Serrano N, Zapatero Gómez-Pallete J, et al. La Protección de Datos Personales en el Ambito Sanitario. Editorial Aranzadi, S.A. 2002.

Sánchez-Caro J, Abellán F. Telemedicina y protección de datos sanitarios (Aspectos legales y éticos). Editorial Comares, S.L. 2002.

Sánchez-Caro J, Abellán F. Datos de salud y datos genéticos, su protección en la Unión Europea y en España. Editorial Comares, S.L. 2004.

Zamarriego Crespo J, Pérez Corral F. Nuevos paradigmas de la profesión médica para el próximo milenio. Ilustre Colegio Oficial de Médicos (ICONEM), 1999.

NORMATIVA

Ley 2/1974, de 13 de febrero, de Colegios Profesionales.

Constitución Española de 27 de diciembre de 1978.

Ley 1/1982, de 5 de mayo, de Protección del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

Ley 14/1986, de 25 de abril, General de Sanidad.

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.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Convenio para la protección de los derechos humanos y de la dignidad del ser humano con respecto a las aplicaciones de la Biología y de la Medicina hecho en Oviedo el 4 de abril de 1997.

Decreto 110/1997, de 11 de septiembre, sobre autorización de centros, servicios y establecimientos sanitarios.

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.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid.

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.

Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias.