ASPECTOS LEGALES DE LA SEGURIDAD Y CONFIDENCIALIDAD EN LA INFORMACIÓN CLÍNICA

Alberto Andérez González

Director de Administración y Recursos Humanos del Servicio Navarro de Salud-Osasunbidea
Asesor Jurídico del Gobierno de Navarra
Letrado de la Administración de la Seguridad Social

INTRODUCCIÓN

Cuando el profesional del Derecho se enfrenta al estudio de la problemática que suscitan los sistemas de información en el ámbito sanitario (fundamentalmente en relación con la historia clínica), no puede sustraerse a una sensación, en cierto modo contradictoria, de inquietud intelectual, por un lado, y de insatisfacción e inseguridad, por otro. La complejidad propia de este sector del ordenamiento jurídico, que es el Derecho sanitario, se acentúa al entrar en conjunción la utilización en este ámbito de las nuevas tecnologías de la información que, amén de las cuestiones de índole estrictamente técnica, presenta una problemática jurídica peculiar derivada de la aparición de un nuevo cuerpo normativo cuyo objeto es regular el tratamiento de la información con la finalidad de garantizar la protección de los derechos de la persona.

En este marco son muchas las dudas y conflictos de naturaleza jurídica que ocupan la atención de los juristas que abordan esta materia, si bien son a su vez bastantes las ocasiones en que, para desesperación de los profesionales ajenos al mundo del Derecho que viven a diario esta problemática, no existe consenso respecto de la solución que la norma establece para cada uno de aquéllos.

Sin que pretenda servir de justificación a la situación descrita, sí pueden señalarse diversos factores que contribuyen a perfilar el panorama actual:

a) La complejidad del Derecho sanitario proviene en gran medida de la implicación, en muchas de las situaciones que regula, de derechos básicos de la persona (vida, integridad física, libertad individual, intimidad personal) que plantean dificultad para su articulación normativa y suscitan al mismo tiempo importantes conflictos no solo legales, sino también éticos a los que no son ajenos las distintas soluciones propugnadas.

b) El dinamismo que caracteriza el desarrollo tecnológico en la nueva sociedad de la información, amén de su contenido eminentemente técnico, encuentra difícil acomodo en un campo, como el del Derecho, con vocación de estabilidad y permanencia, y pone por ello mismo de manifiesto el anacronismo de algunas de las previsiones legales y la necesidad de su modificación, conclusión que es per-

fectamente predicable de una norma básica en el ámbito sanitario como es la Ley General de Sanidad de 25 de abril de 1986.

c) En este contexto, la aparición (con la Ley Orgánica 5/1992 y posteriormente con la Ley Orgánica 15/1999) de un marco legal ciertamente riguroso regulador de la protección de datos de carácter personal contribuye, en ocasiones, a clarificar ciertos debates, provoca en otros supuestos dudas razonables respecto de la solución ajustada a Derecho, y genera en todo caso una sensación de vértigo ante el alto nivel de exigencia que comporta la adaptación a los requerimientos legalmente establecidos.

d) La existencia de un severo régimen sancionador, tanto penal como administrativo, con el que se cierra el sistema de garantías diseñado por el legislador, contribuye a extender igualmente un temor generalizado, y muchas veces no del todo racional, entre los profesionales del ámbito sanitario, que deja en segundo plano en ocasiones las exigencias deontológicas que de modo ineludible deben estar presentes en toda buena práctica clínica y de gestión.

Estas consideraciones se hacen patentes de manera especial en el tratamiento de los aspectos de confidencialidad y seguridad relacionados con los sistemas de información clínica, cuyo estudio en este breve trabajo se estructura en tres partes que analizan, respectivamente, el ámbito de la regulación en materia de protección de datos, las cuestiones relativas al acceso y comunicación de los datos incluidos en sistemas de información clínica, y, por último, las notas principales de la regulación contenida en el Real Decreto 994/1999.

NORMATIVA SOBRE PROTECCIÓN DE DATOS Y CONFIDENCIALIDAD

La primera cuestión que debe suscitarse al abordar la problemática afectante a los aspectos de seguridad y confidencialidad de los sistemas de información es la que plantea el ámbito de protección dispensado por el nuevo marco legal regulador del tratamiento de datos de carácter personal, cuestión ésta de alcance no solamente teórico, sino también con especial trascendencia en cuanto a las repercusiones prácticas que pueden deducirse en relación con el régimen sancionador asociado al incumplimiento de la norma.

En esta materia concreta, la dificultad deriva en gran medida de la necesidad de poner en relación el fundamento o razón última que subyace al tratamiento legal de la protección de datos de carácter personal con el sentido o interpretación que se dé a determinados conceptos que la Ley utiliza y, en ocasiones, define, aun

cuando esta labor de definición no termine de despejar todas las dudas que puedan plantearse.

El artículo 18.4 de la Constitución y la llamada "libertad informática"

El punto de partida en cuanto al tratamiento legal de los datos de carácter personal se sitúa en el art. 18.4 de la Constitución, cuando señala 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".

Esta declaración constitucional ha dado lugar a un profundo debate en torno a si el precepto citado configura un derecho fundamental distinto al propio derecho a la intimidad personal y familiar (consagrado en el apartado 1 del mismo artículo), o 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.

Aún cuando puede considerarse mayoritaria la opinión doctrinal contraria a la afirmación de un derecho fundamental nuevo o autónomo a partir de lo preceptuado en el art. 18.4 de la Constitución, lo cierto es que una conclusión en gran medida distinta puede extraerse de los escasos pero interesantes pronunciamientos recaídos en esta materia hasta el momento, especialmente aquellos dictados por el Tribunal Constitucional en su función de intérprete máximo de la Carta Magna.

A raíz de la muy comentada sentencia 254/1993, de 20 de julio, ha venido conformándose un cuerpo de doctrina conforme al cual se entiende que la previsión del art. 18.4 citado no se ciñe a un mero mandato dirigido al legislador que no otorgaría derechos al ciudadano en tanto aquél no cumpla su función de desarrollo, sino que, acudiendo al fundamento y sentido de los textos internacionales ratificados por el Estado Español, la Constitución habría incorporado una nueva garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona". Dicha sentencia, con una posición un tanto ecléctica, afirma que nos encontramos "ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos".

Moviéndose entre las dudas sobre su configuración o no como derecho autónomo, el Tribunal Constitucional señala que la garantía del derecho a la intimidad adopta actualmente un "contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona", dando así lugar a la llamada "libertad informática" como "derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)".

Sentencias posteriores del mismo Tribunal han continuado con esta doctrina, reiterando el carácter a la vez de derecho instrumental y de derecho fundamental en sí mismo que cabe afirmar de la llamada "libertad informática", que por otro lado se halla dotada de un contenido mínimo (derivado de la propia Constitución) que comporta, entre otros aspectos, las facultades de conocer la existencia, identidad y responsable de los ficheros informatizados que contengan datos de la persona o, por ejemplo, el derecho de ésta a oponerse a que dichos datos personales sean utilizados para finalidades distintas a las que justificaron su obtención. Son especialmente significativas en este punto las sentencias 143/1994, de 9 de mayo, 11/1998, de 13 de enero (seguida de otras muchas recaídas sobre el mismo supuesto de hecho), y 202/1999, de 8 de noviembre.

En este punto cabe efectuar una primera e importante reflexión; a saber, que con independencia del debate doctrinal acerca de la naturaleza del derecho reconocido en el art. 18.4 del Texto Constitucional, el mismo entraña una ampliación respecto de lo que tradicionalmente ha venido constituyendo objeto de protección a través del derecho a la intimidad personal y familiar. Obviamente, la garantía y protección frente a terceros de un ámbito íntimo o reservado de la persona cuenta con una larga tradición jurídica, y en este sentido la novedad ha venido provocada por el hecho de que las nuevas tecnologías posibiliten el flujo y utilización masiva de la información concerniente a las personas, información que, por otro lado, es necesario facilitar, cada vez con mayor frecuencia, a distintos entes públicos o privados para el ejercicio legítimo de las funciones atribuidas a éstos.

Por ello, el ámbito de la llamada "libertad informática" (también conocido como derecho a la autodeterminación informativa) no abarca únicamente a aquella información que reviste un carácter reservado (por afectar a la esfera más íntima de la persona), sino a cualquier dato o información referida a personas físicas individualizadas o susceptibles de individualización, ya que se parte de que el tratamiento y comunicación de datos personales, aunque éstos en principio y aisladamente considerados no sean sensibles, posibilita la obtención de un determinado perfil de la persona, permitiendo la intromisión en facetas reservadas de su personalidad y generando incluso el riesgo de que dicha información influya en la adop-

ción de determinadas decisiones (sea por sujetos públicos o privados) en relación con el individuo.

Basta, para comprobar la ampliación señalada, una comparación entre el objeto tradicional de protección de la intimidad (señala la Ley Orgánica 1/1982, de 5 de mayo, que "la protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia") y el ámbito de la normativa sobre protección de datos, conforme a la cual se definen los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables" (art. 3.a de la Ley Orgánica 15/1999).

El desarrollo del artículo 18.4 de la Constitución. El ámbito de las Leyes Orgánicas 5/1992 y 15/1999

La concreción del mandato contenido en el art. 18.4 de la Constitución tiene lugar por primera vez, como es sabido, con la Ley Orgánica 5/1992, de 29 de octubre, por la que se regula el tratamiento automatizado de los datos de carácter personal, cuyo ámbito de aplicación reviste algún matiz con relación al precepto constitucional que desarrolla. Así, mientras aquel precepto alude al uso de la "informática", el art. 1 de la Ley Orgánica define su objeto por la limitación del "uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal".

Desde este punto de vista, aun cuando pudiera considerarse más amplio el ámbito de la Ley Orgánica que el que deriva del Texto Constitucional, no hay inconveniente en admitir que en último extremo se trata de atender o satisfacer la misma necesidad jurídica, esto es, la protección de los derechos de la persona (especialmente el de su intimidad personal y familiar, pero también otros) ante los riesgos que para tales derechos supone el inmenso flujo de información posibilitado, merced a las nuevas tecnologías, por el tratamiento masivo de los datos de carácter personal y su constancia en ficheros organizados.

La mayor amplitud del objeto de la Ley Orgánica puede afirmarse por la previsión de otros posibles medios técnicos de tratamiento automatizado de datos distintos de la informática (lo que no deja de plantear un debate semántico), pero en todo caso el fundamento último de la regulación coincide con el fin constitucional previsto en el art. 18.4. No es ocioso señalar que el término automatizado, en su sentido gramatical, hace referencia a procesos o dispositivos automáticos, esto es, basados en mecanismos que funcionan en todo o en parte por sí solos.

No obstante, la cuestión adquiere rasgos de mayor complejidad con la derogación de la Ley Orgánica 5/1992 en virtud de la nueva Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal, uno de cuyos principales efectos, advertido desde un principio por la doctrina, consiste en la ampliación del objeto o ámbito de aplicación de la norma en relación con la normativa ahora derogada.

Es conocido que la promulgación de la Ley Orgánica 15/1999 resultaba obligada con el fin de adaptar el Derecho interno español a 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; pero no está tan claro que, al menos en este punto concreto que ahora se examina, dicha adaptación se haya llevado a cabo con la precisión que debiera. Por otro lado, las modificaciones que introduce la nueva Ley Orgánica respecto de la anterior no se limitan a aquellos aspectos necesitados de adaptación, sino que alcanza también a otros contenidos de la regulación legal que, aunque pueda considerarse que resultan razonables o comprensibles, no son objeto de justificación expresa por parte del legislador al haberse omitido, inexplicablemente, la exposición de motivos en el nuevo texto legal.

En cualquier caso, y centrándonos en el ámbito de aplicación de la norma, el aspecto más destacable es sin duda su ampliación a cualquier tipo de tratamiento de los datos personales, con independencia de su carácter automatizado o no; así resulta sin más de lo dispuesto en el art. 1 de la Ley Orgánica, que habla del tratamiento de dichos datos sin ningún otro calificativo, por contraste con la redacción, e incluso el título mismo, de la regulación derogada.

La aplicación del marco legal regulador de los datos de carácter personal al tratamiento manual o no automatizado de los mismos es, por tanto, la primera consecuencia que se desprende de la ampliación señalada, y esta misma circunstancia es la que genera importantes dudas respecto al alcance último de la nueva normativa legal en la materia, dudas motivadas en gran medida por la utilización de determinados conceptos cuya definición no termina de perfilar nítidamente el ámbito de protección de la Ley.

Algunos conceptos legales: tratamiento, fichero y cesión de datos

Ya se ha hecho referencia a la noción de “datos de carácter personal”, cuyo alcance aparece en principio como casi ilimitado; y este mismo es el caso del concepto de “tratamiento”, que curiosamente mantiene la misma definición que en la Ley Orgánica 5/1992 (en la que ya se aludía a su carácter automatizado o no), esto

es, 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". Como puede observarse, no existe apenas limitación teórica en cuanto al tipo de actividades que pueden entenderse incluidas en el concepto de tratamiento, salvo por la referencia al carácter "técnico" de los citados procedimientos y operaciones, precisión cuyo alcance no despeja en absoluto las dudas interpretativas (el adjetivo "técnico" significa gramaticalmente "perteneciente o relativo a las aplicaciones de las ciencias y las artes").

Otro concepto relevante es el de "fichero", definido en la Ley Orgánica como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", noción indudablemente más amplia que la de fichero automatizado que empleaba la regulación anterior, aun cuando la referencia a su carácter organizado exige en todo caso una mínima estructuración de la información recogida, cualquiera que sea el soporte físico en el que se contenga. En todo caso, la relativa indefinición de los términos utilizados no aclara los contornos que permiten considerar cuándo un fichero, sobre todo en el caso de los no automatizados, se ve afectado o no por las disposiciones legales en materia de protección de datos.

De todas formas, ambos conceptos, los de fichero y tratamiento, guardan una conexión que obliga a interpretarlos de manera conjunta, como lo pone de manifiesto la propia Ley Orgánica 15/1999 al definir en el art. 2 su ámbito de aplicación por referencia a "los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de" los mismos, o al definir, también de manera indistinta, la figura del responsable del fichero o tratamiento.

Las dificultades interpretativas son patentes; si se tiene en cuenta la amplitud del concepto de cesión de datos ("toda revelación de datos realizada a una persona distinta del interesado"), puede comprenderse que la aplicación o no del régimen legal que se examina, y sobre todo de las previsiones sancionadoras que el mismo contempla, va a depender, en el caso de los ficheros no automatizados, de cómo se entienda el carácter más o menos organizado de un fichero o la naturaleza técnica de los procedimientos en que se basa el tratamiento de los datos contenidos en él; y todo ello, según se ha dicho, con independencia del grado de reserva o sensibilidad de los datos que hayan sido objeto de comunicación.

Dicho de otro modo, y sin perjuicio de lo que luego se dirá respecto a la efectividad temporal del régimen legal en el caso de los ficheros no automatizados, desde la perspectiva de las consecuencias prácticas que derivan de esta cuestión, la promulgación de la Ley Orgánica 15/1999 y la extensión de su ámbito de protección a los ficheros no automatizados conlleva, en principio, una notable ampliación, al menos potencial, del número de conductas susceptibles de quedar sujetas al marco legal y sancionador establecido por aquélla, aun cuando vengan referidas a datos o informaciones que no incidan directamente en el ámbito íntimo de las personas. Esto es, la revelación de datos personales no reservados, que efectuada de manera aislada no entrañaría una infracción del derecho a la intimidad ni constituiría, por tanto, una vulneración del deber de confidencialidad, puede no obstante determinar importantes responsabilidades al amparo de la Ley Orgánica citada en la medida en que constituya un tratamiento sujeto a dicha norma legal o afecte a datos contenidos en un fichero regulado por la misma, conclusión que se agrava por la falta de una clara definición del tipo de ficheros y actividades sujetos al régimen legal del tratamiento de datos personales.

Nótese que, llegados a este punto, y aun cuando el amparo de la Ley Orgánica 15/1999 en la Directiva 95/46/CE es incuestionable además de obligado, el distanciamiento entre la norma legal (que se aplica a todo tipo de tratamiento de datos personales) y el art. 18.4 de la Constitución (que utiliza expresamente el término "informática") es más patente. En cualquier caso, y aunque la aplicación práctica de la norma en los próximos años será la que revele las pautas de interpretación de la misma, parece ineludible conectar la nueva regulación legal con el interés jurídico que trata de protegerse, y en este sentido delimitar los conceptos legales de fichero y tratamiento en función de las posibilidades de utilización o circulación masiva de los datos personales objeto de los mismos, toda vez que son estas circunstancias, según revela la doctrina y jurisprudencia elaboradas sobre esta materia, las que evidencian el riesgo para la intimidad y demás derechos de las personas que, a su vez, está en la base de la ampliación del ámbito tradicional de protección de estos derechos.

En esta línea parece que cabe interpretar la propia normativa comunitaria cuya adaptación al Derecho interno lleva a cabo la Ley Orgánica 15/1999. El artículo 3 de la Directiva citada circunscribe su ámbito de aplicación al "tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero"; esto es, su objeto queda definido en principio por el tratamiento de carácter

automatizado, y alcanza también al no automatizado en la medida en que afecta a datos incluidos en un sistema organizado de información.

Aplicación transitoria de la Ley Orgánica de Protección de Datos a los ficheros no automatizados

El propio legislador es consciente, sin duda, de la repercusión que entraña la ampliación llevada a cabo por la Ley Orgánica 15/1999, y de ello es muestra el contenido de la Disposición Adicional primera esta norma legal, que pospone la plena aplicación de la Ley a los ficheros y tratamientos no autorizados hasta octubre de 2007, con la única excepción relativa al ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados, que se entiende que pueden hacerse valer, por tanto, desde la propia entrada en vigor de aquélla.

Por otro lado, y a pesar de que pueda existir alguna opinión discrepante, parece también indudable que el ámbito de aplicación del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, queda limitado, según expresa su propio título, a los ficheros de tal carácter, sin que pueda hacerse extensivo, por tanto, a los ficheros manuales o no automatizados.

Esta conclusión se impone a la vista de lo establecido en la Disposición Transitoria tercera de la Ley Orgánica 15/1999, conforme a la cual, y en tanto no se dicten las oportunas normas reglamentarias por el Gobierno, continuarán en vigor, en cuanto no se opongan a la Ley, las normas reglamentarias existentes, y en concreto, y entre otros, el citado Real Decreto 994/1999. A pesar de que la regulación legal se extiende a los ficheros no automatizados, el sentido de la norma transitoria comentada no es el de ampliar a su vez el ámbito de aplicación del Reglamento de medidas de seguridad, efecto éste que requeriría una declaración expresa en tales términos y que, además, resultaría contradictoria con la citada Disposición Adicional primera de la Ley Orgánica en cuanto que el cumplimiento de las normas de seguridad de los datos no se encuentra entre las previsiones de la Ley que tienen eficacia inmediata respecto de los ficheros no automatizados.

A mayor abundamiento, sería inadmisible pretender aplicar el régimen sancionador dispuesto en caso de incumplimiento de la regulación legal del tratamiento de datos personales mediante una extensión de los requerimientos contenidos en el Real Decreto 994/1999 a los ficheros no automatizados, no expresamente incluidos en el ámbito del reglamento.

El resultado no deja de ser paradójico; es incuestionable la ampliación del objeto legal de la regulación del tratamiento de datos de carácter personal, y las dificultades interpretativas que ello suscita, si bien la repercusión inmediata de esta ampliación es muy relativa al limitarse, y no sin problemas de aplicación, al ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Esta consideración reduce, de momento, el estudio de las normas sobre seguridad de ficheros a los de carácter automatizado. Una matización mayor debe hacerse, no obstante, en lo que concierne a las normas sobre confidencialidad de los ficheros; entendida en sentido amplio, abarcando, por tanto, todas las previsiones contenidas en la Ley Orgánica 15/1999 que regulan el acceso y la comunicación de los datos de carácter personal, hay que entender que, conforme a la Disposición Adicional primera ya examinada, la aplicación plena de tales normas sólo puede predicarse respecto de los ficheros automatizados. Sin embargo, es también indudable que los ficheros no automatizados quedan sujetos a las normas generales que protegen el derecho al honor y a la intimidad personal y familiar del individuo, y en tal sentido es obligado afirmar un deber estricto de confidencialidad en relación con los datos personales de carácter reservado o íntimo que se contengan en tales ficheros.

EL ACCESO A LA INFORMACIÓN CLÍNICA Y LA CESIÓN DE DATOS

De acuerdo con el concepto amplio antes apuntado, el estudio de la confidencialidad de los sistemas de información permite abarcar, por un lado, las normas que contemplan las personas habilitadas para el tratamiento y acceso a los datos de carácter personal, y por otro, la regulación de la comunicación o cesión a terceros de dichos datos.

A) EL ACCESO A LA INFORMACIÓN CLÍNICA

Comenzando por el primero de los aspectos señalados, y desde la óptica de los sistemas de información clínica, cabe señalar que precisamente una de las cuestiones de mayor trascendencia, y al mismo tiempo dificultad, que suscita la historia clínica y que se agrava con su tratamiento automatizado viene constituida por la determinación de las personas que, además del propio paciente, deben considerarse autorizadas para el acceso a la misma; ello es debido a que no es éste un extremo que venga concretado normativamente.

Normativa sanitaria y legislación sobre protección de datos

La legislación sanitaria se limita a enunciar un principio general de restricción en cuanto al acceso a la historia, según se deduce de los términos que utiliza el art. 61 de la Ley General de Sanidad, conforme al cual se contempla el acceso a la misma, además de por el propio paciente, por parte de los facultativos implicados directamente en el diagnóstico y tratamiento del paciente. Esta última mención legal no es suficiente por cuanto, al referirse en exclusiva al personal facultativo implicado directamente en el diagnóstico y tratamiento del enfermo, no prevé, por tanto, que otros diversos colectivos profesionales que trabajan en el ámbito de las instituciones sanitarias pueden también acceder o manejar, bien es cierto que de modo más limitado, la historia clínica (piénsese en el personal de enfermería que debe consultarla para el ejercicio de las funciones que le son propias, o incluso en el personal administrativo que deba reflejar en ella determinados datos).

La Ley Orgánica 5/1992 no aportaba mayor solución a este problema, por cuanto se limitaba a exigir que quede constancia del órgano (en el caso de las Administraciones Públicas) o la persona (en el caso de ficheros de titularidad privada) que tiene la consideración de responsable del fichero; determinación que por sí sola no permite concretar la totalidad de personas que pueden utilizar o acceder, con fines más amplios o más restringidos, a la historia clínica informatizada, si bien contribuye a delimitar responsabilidades en caso de acceso o utilización no autorizada de aquélla.

La Ley Orgánica 15/1999 introduce alguna modificación respecto de la regulación precedente. Se mantiene la figura del responsable del fichero o tratamiento, definido como “persona física o jurídica, de naturaleza pública o privada, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”; pero junto a ella aparece el encargado del tratamiento, que 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”.

Además, y afectando de manera específica a los sistemas de información clínica, constituye una novedad destacable de la Ley Orgánica 15/1999 la previsión contenida en su artículo 7.6, que, siguiendo en gran medida el criterio de la Recomendación de 13 de febrero de 1997 del Consejo de Europa, autoriza el tratamiento, entre otros, de los datos relativos a la salud siempre que el mismo se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

Esta última norma contribuye bastante más a delimitar el perfil de las personas autorizadas para el acceso y tratamiento de los datos de salud; no obstante, tampoco está exenta de algunas dudas interpretativas en lo que afecta a determinar cuáles son esas otras personas con obligación de secreto equivalente a la de los profesionales sanitarios. En efecto, si se parte de que toda persona que por razón de su actividad laboral o profesional tenga acceso a información de carácter reservado (y la que afecta a datos de salud lo es) viene obligada por un deber de confidencialidad respecto de la misma, habrá que entender que esa obligación de secreto equivalente a la de los profesionales sanitarios debe representar un plus sobre aquel deber genérico; pero por otro lado, tampoco es pacífica, al menos en el Derecho español, la cuestión relativa a en qué actividades cabe afirmar un deber de secreto profesional en sentido propio, cuestión con importantes consecuencias legales y procesales (el vigente Código Penal, sin ir más lejos, tipifica como delitos distintos la vulneración del secreto profesional y la revelación de datos reservados conocidos por razón de la actividad laboral o profesional).

Esta previsión normativa está llevando a entender, al menos en ámbitos no sanitarios, que cuando los sistemas de información incluyan datos de esta naturaleza su tratamiento debe encomendarse a profesionales de la salud. No obstante, este criterio, tal vez válido en aquellos sectores de actividad donde el tratamiento de información sanitaria sea una excepción, no resulta satisfactorio en el ámbito sanitario, en el que parece ineludible, al menos 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.

Previsiones del Real Decreto 994/1999, de 11 de junio

En todo caso, la regulación legal respecto a las personas autorizadas para el acceso y tratamiento de datos personales debe completarse, a su vez, con lo establecido en el Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, normativa que incide más en la exigencia de una previa constancia e identificación de las personas con acceso autorizado a cada fichero, que en el establecimiento de criterios generales respecto a quiénes deban ser objeto de autorización.

En este sentido, la relación de todas y cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información, con indicación además de sus funciones y obligaciones concretas, forma parte del contenido necesario del denominado documento de seguridad, que constituye la pieza clave en la ordena-

ción de las medidas de seguridad de todos los niveles. A esta obligación se añade, además, la exigencia dirigida al establecimiento de procedimientos de identificación y autentificación para el acceso al sistema de información, así como de controles de acceso con el fin de que los usuarios puedan acceder a aquellos contactos y recursos estrictamente necesarios para el desarrollo de sus funciones.

Estas previsiones, establecidas para el nivel básico pero exigibles para todos los niveles, se incrementan en los niveles medio y alto mediante un reforzamiento de las exigencias de identificación y autentificación, hasta llegar a la implantación, en los ficheros de nivel alto, de un registro de accesos que permita guardar en relación con cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

En suma, el conjunto de normas legales y reglamentarias examinadas permiten establecer un principio restrictivo en cuanto al acceso y manejo de la información de carácter personal, en el sentido de que, aun admitiendo diversas posibles formas de organización del trabajo, el volumen de información accesible a cada persona es el estrictamente imprescindible para el correcto desempeño de sus funciones, aspecto éste que en cualquier caso puede ser revisado y fiscalizado con base en el citado documento de seguridad.

Todo ello con independencia de que, en cualquier caso, es también indudable el deber general de secreto que se impone a toda persona que por razón de su trabajo tenga acceso a información de datos relativos a la intimidad de las personas; deber cuya infracción acarrea además importantes consecuencias legales.

Contratación externa del tratamiento de datos

El tratamiento de esta materia no puede cerrarse sin hacer una referencia a la posibilidad del acceso de los datos por cuenta de terceros, actualmente prevista en el art. 12 de la Ley Orgánica 15/1999, que representa una importante novedad con respecto a la regulación anterior y que permite solventar ciertas dudas surgidas al amparo de ésta última. La afirmación contenida en dicho precepto, en el sentido de que “no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento”, constituye en realidad una habilitación para la posible contratación externa del tratamiento de datos de carácter personal, cuestión siempre debatida por los riesgos que entraña en orden a la seguridad y confidencialidad de la información.

Téngase en cuenta que la no consideración como comunicación de datos conlleva la innecesariedad del consentimiento del afectado. Por ello, a partir de esta modificación legal es patente la admisión de esta figura, si bien sometida a determinados requerimientos legales como son, básicamente, la necesaria constancia en contrato escrito (u otra forma que permita acreditar su celebración y contenido), la necesidad de pactar expresamente determinadas obligaciones del encargado del tratamiento (acatamiento de las instrucciones del responsable del tratamiento, no aplicación de los datos a fin distinto al del contrato y no comunicación de los mismos al tercero) y de estipular las medidas de seguridad aplicables, y la obligación de destrucción o devolución de los datos al responsable del tratamiento una vez cumplida la prestación contractual.

Esta regulación legal viene, en gran medida, a otorgar rango normativo a determinados criterios que la práctica había venido aplicando para la utilización de la contratación externa, ya que en todo caso la conclusión contraria a la admisión de la misma, aun a pesar del silencio de la Ley Orgánica 5/1992, no parecía una solución razonable.

B) COMUNICACIÓN DE DATOS. EL CONSENTIMIENTO DEL AFECTADO Y SUS EXCEPCIONES

El segundo gran apartado, el referido a la determinación de los supuestos en que la información clínica es accesible a terceros, obliga a considerar conjuntamente los dos ámbitos normativos implicados, a saber, la legislación sanitaria por un lado, y la regulación legal del tratamiento de datos de carácter personal. Con base en una y otra normativa, no obstante, el fundamento que legitima el acceso por parte de terceros a información de carácter personal es el mismo; a saber, el derecho del paciente a la confidencialidad de la información sanitaria relativa a su proceso, caracterizado como derecho fundamental en cuanto expresión al derecho a la intimidad personal del sujeto, no está exento de límites o excepciones, del mismo modo que sucede con cualquier otro derecho reconocido por el ordenamiento jurídico que, por definición, nunca es absoluto sino que encuentra su límite en la protección de otros derechos o intereses legítimos.

Comenzando por el segundo bloque normativo señalado, debe indicarse que las previsiones de la Ley Orgánica 15/1999 relativas a los supuestos expresamente admitidos de cesión y comunicación de datos son indudablemente aplicables, dado su carácter de regulación general, a los sistemas de información clínica.

En este sentido, el principio general que consagra la norma es el de la necesidad del previo consentimiento del interesado para que los datos de carácter perso-

nal objeto de tratamiento puedan ser comunicados a un tercero, siempre y cuando, además, dicha comunicación obedezca al cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario. Mayor interés que el principio general reviste, sin embargo, la determinación de los supuestos en que la necesidad de aquel consentimiento queda exceptuada, ya que son éstos los supuestos que plantean mayor conflictividad en su aplicación práctica y los que generan asimismo importantes dudas de interpretación.

Exepciones de carácter general

a) La primera de las excepciones viene referida a aquellos casos en que la cesión esté autorizada por una ley. Por esta vía es necesario efectuar una remisión a la regulación específica en el ámbito sanitario, a la que luego se aludirá.

b) Queda exceptuada también del consentimiento del afectado la comunicación de datos recogidos de fuentes accesibles al público, aspecto éste en el que la Ley Orgánica 15/1999 introduce, en relación con la legislación derogada, la novedad importante de definir de modo exhaustivo cuáles son las fuentes que tienen tal carácter.

c) Una excepción importante es la que contempla la ley al excluir el consentimiento "cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros". Las dificultades interpretativas de este precepto son notables, aún cuando en principio parece extender al ámbito de la comunicación de los datos la misma excepción al consentimiento del afectado que rige para el tratamiento de los mismos (esto es, la existencia de una relación negocial que exija necesariamente la cesión). Teniendo en cuenta la amplitud de los conceptos manejados por la propia regulación legal y los términos en que se expresa este precepto, no sería descartable su aplicación a supuestos tradicionalmente problemáticos y discutibles, como son los de acceso por parte de un tercero a datos personales (incluso sensibles) con base en el interés legítimo derivado de un contrato suscrito entre dicho tercero y el afectado; el ejemplo típico, en el caso de los sistemas de información clínica, viene constituido por las peticiones de acceso a datos de la salud de las personas formuladas por entidades aseguradoras con quienes el interesado tiene suscrito un determinado contrato de seguro para cuyo cumplimiento puede resultar necesario el conocimiento de aquella información.

d) La Ley Orgánica 15/1999 contempla también, como excepción al consentimiento del afectado, la comunicación de datos que deba efectuarse a favor del

Defensor del Pueblo, el Ministerio Fiscal, los Jueces y Tribunales y el Tribunal de Cuentas (incluyendo a las instituciones autonómicas con funciones análogas al primero y último de los citados), cuando se enmarque en el ejercicio de las funciones que tienen atribuidas. La previsión legal no resulta novedosa en relación con la disposición de la información clínica a favor de los órganos judiciales, conforme a un criterio y una práctica comúnmente admitidos, aunque no exentos de dudas y conflictos planteados, sobre todo, en relación con las condiciones en que debe facilitarse esa información a los Juzgados y Tribunales. Sin embargo, la nueva regulación legal sí añade una mayor claridad al incluir, junto a los órganos judiciales, a las demás instituciones que cita, respecto de las que el acceso a información de carácter personal, incluso reservada, se fundamenta en el ejercicio legítimo de las funciones que constitucional y legalmente tienen atribuidas.

La cesión entre Administraciones Públicas

Mención especial merece el tratamiento de la cesión de datos entre las Administraciones Públicas, ya que en este caso se amplían de modo considerable las posibilidades de cesión de la información de carácter personal con fundamento, asimismo, en el ejercicio de las funciones que legalmente se atribuyen a las Administraciones Públicas.

De la redacción del art. 21 de la Ley Orgánica se desprende que no es necesario el consentimiento del afectado (como se encarga de aclarar su apartado cuarto) en diversos supuestos; en primer lugar, la redacción inicial del precepto permite entender que la cesión entre Administraciones Públicas distintas está autorizada cuando se trata de ejercer las mismas competencias sobre idéntica materia (sólo así se entiende la formulación de la norma en términos negativos).

Pero además, aun no concurriendo esta circunstancia, la cesión o comunicación se permite, de acuerdo con el mismo precepto, siempre que haya sido prevista por las disposiciones de creación del fichero o por una disposición de rango superior que regule su uso, y en todo caso cuando la comunicación tenga por objeto el posterior tratamiento de los datos con fines históricos, estadísticos o científicos. En suma, la ampliación de los supuestos admitidos de comunicación de datos en el caso de las Administraciones Públicas es notable con respecto a los ficheros de titularidad privada, que quedan sujetos sin más a las normas generales señaladas.

Estas conclusiones, no obstante, deben ser revisadas a tenor de la reciente sentencia 292/2000, de 30 de noviembre, dictada por el pleno del Tribunal Constitucional en el recurso de inconstitucionalidad promovido por el Defensor del Pueblo respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, cuyo

fallo, estimatorio del recurso interpuesto, declara inconstitucionales, y por tanto nulos, determinados incisos de los preceptos impugnados. Sin perjuicio de un examen más profundo del citado pronunciamiento (que excede del objeto del presente estudio), debe resaltarse, por lo que aquí interesa, que la declaración de inconstitucionalidad afecta a la previsión legal de la posibilidad de cesión de datos entre Administraciones Públicas, para el ejercicio de competencias distintas o sobre materias diferentes, siempre que aquélla hubiera sido prevista por la norma de creación del fichero o por una disposición de superior rango que regule su uso.

Esta declaración, de consecuencias ciertamente notables (y que debiera obligar en buena lógica a una reforma de la Ley que delimite en mayor medida los supuestos admisibles de cesión de datos entre Administraciones Públicas), descansa en un motivo ("claro", según señala el Tribunal) expresado en el fundamento decimocuarto de la sentencia, que no obstante suscita importantes dudas. El vicio de inconstitucionalidad viene provocado, a juicio del Alto Tribunal, por el hecho de que la Ley haya renunciado a fijar "los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado", afirmación esta última que no deja de resultar peculiar si se tiene en cuenta que precisamente el ejercicio legítimo de las funciones encomendadas a la Administraciones Públicas habilita a éstas para el tratamiento (y por tanto la recogida) de datos sin necesidad de consentimiento del interesado, conforme al artículo 6 de la propia Ley Orgánica 15/1999, excepción que, salvo que en sí misma fuera declarada también inconstitucional, parece coherente en su fundamento con la previsión legal ahora anulada.

Excepciones propias de los sistemas de información clínica

a) La última de las excepciones que contempla la Ley Orgánica, en cuanto a la comunicación de datos sin consentimiento del interesado, viene referida a un supuesto específico o propio del ámbito sanitario como es "la cesión de datos de carácter personal relativos a la salud (que) sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica". El inciso primero de la norma prevé lo que podría considerarse un supuesto de estado de necesidad sanitaria, reflejo de la consideración que al legislador le merece la especial problemática que puede suscitarse en relación con los sistemas de información de datos sanitarios, de la que es ejemplo a su vez el tratamiento específico que recibe la transferencia internacional de datos que "sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o trata-

miento médicos o la gestión de servicios sanitarios", a la que se exime del cumplimiento de los requisitos generales exigibles para el movimiento internacional de datos.

b) Por otro lado, es obligada la remisión a la propia legislación sanitaria para completar el régimen legal de habilitación de la cesión o comunicación de datos, remisión que, como se ha visto, la Ley Orgánica ordena en dos ocasiones, una con carácter general (supuestos de cesión autorizada por una Ley) y otra específica en el supuesto de cesión necesaria para la realización de estudios epidemiológicos conforme a la legislación sobre sanidad.

En este sentido, la propia regulación legal de la historia clínica contempla diversos supuestos en los que el carácter reservado de la información contenida en aquélla cede ante determinados fines; así lo establece el art. 61 de la Ley General de Sanidad, que permite la posible utilización de la información contenida en las historias clínicas con fines científicos o para la realización de estudios epidemiológicos, así como para las actuaciones de inspección médica (excepción justificada en el ejercicio legítimo de las funciones de inspección y control atribuidas legalmente a las Administraciones sanitarias).

No obstante, cabe destacar la existencia de un proyecto de modificación en esta materia, que se plasma en un borrador de regulación legal básica en materia de información y documentación clínica, elaborado en 1999 por el Ministerio de Sanidad y Consumo, y que modificaría en este y en otros puntos la normativa vigente contenida en la Ley General de Sanidad. Por su interés merece hacer mención de las previsiones contenidas en dicho borrador en relación con el acceso y disposición de la historia clínica, materia en la que establece un grado de concreción mayor, al contemplar las siguientes situaciones:

1) Como regla general, la historia estará disponible para todos los profesionales que intervengan en el proceso asistencial. Nótese que el término utilizado (profesionales y no facultativos) es más amplio que el actual y permite solventar algunas de las dudas que han quedado apuntadas.

2) Se contempla, asimismo, el acceso en supuestos de requerimiento judicial, seguridad y salud pública, investigación y docencia debidamente autorizados, y demás situaciones previstas en la Ley.

3) También se permite la utilización de la historia clínica para el ejercicio de funciones de inspección sanitaria, actividades de evaluación y acreditación y otras

motivadas por la autoridad sanitaria que tengan por objeto mejorar la calidad de la asistencia.

4) Y por último, se prevé el acceso a la historia en defensa de los intereses generales en casos de urgencia o necesidad.

En suma, y aun con dificultades de interpretación en algunas de las excepciones previstas, la aplicación conjunta de la normativa sanitaria y de la regulación del tratamiento de datos permite concretar con relativa precisión los supuestos en que es legalmente admisible el acceso por parte de terceros a la información clínica, configurando de esta manera el contorno y los límites del deber de confidencialidad exigible en relación con los datos de carácter personal.

ASPECTOS PRINCIPALES DE LA REGULACIÓN CONTENIDA EN EL REAL DECRETO 994/1999, DE 11 DE JUNIO

El 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, constituye el desarrollo de lo dispuesto en el art. 9 de la Ley Orgánica 5/1992, precepto legal cuya redacción, con la única salvedad referida a la inclusión del encargado del tratamiento junto al responsable del fichero como sujeto obligado, se mantiene intacta en la Ley Orgánica 15/1999.

Este precepto legal, a través de los tres párrafos en que se redacta, contempla en realidad tres previsiones distintas. Por un lado, se establece un deber, definido en términos genéricos, de adoptar "las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado". Como puede observarse, este apartado no efectúa una remisión al reglamento en orden a la determinación de cuáles son esas medidas, sino que contiene una obligación, en principio jurídicamente exigible, que se concreta en función de las propias circunstancias, o, como señala el propio precepto, de acuerdo con el "estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos".

La llamada al Reglamento se efectúa propiamente en los dos restantes apartados de la norma legal comentada, con carácter general para todo tipo de datos de carácter personal, por un lado, y de modo específico para los datos especialmente protegidos, entre los que se encuentran los relativos a la salud de las personas, por otro. Dicha norma reglamentaria debe regular, según el mandato legal, las condiciones de integridad y seguridad de los datos y de los centros de tratamiento, loca-

les, equipos, sistemas y programas, así como los de los ficheros y las personas en el caso de tratamiento de datos sensibles.

Cabe destacar que el régimen sancionador dispuesto por la propia Ley Orgánica tipifica como infracción grave el incumplimiento de las condiciones que se establezcan reglamentariamente en relación con los ficheros, locales, programas o equipos que contengan datos de carácter personal, si bien el incumplimiento del deber genérico contenido en al apartado primero del precepto legal que se examina podría, probablemente, encontrar acomodo en alguna otra de las conductas susceptibles de ser sancionadas conforme a aquel régimen.

Abordada con anterioridad la cuestión relativa al ámbito de aplicación del Reglamento, el estudio debe centrarse en un breve análisis de algunos de los aspectos destacables de una regulación que, no obstante su carácter esencialmente técnico, merece también ciertas consideraciones de índole jurídica, comenzando por la primera y esencial referida a su fundamento o razón de ser, que, como expresa su propia exposición de motivos en concordancia con la norma legal objeto de desarrollo, radica en la necesidad de garantizar la confidencialidad e integridad de la información como modo de protección de los derechos al honor y a la intimidad personal y familiar y demás derechos de la persona.

Debe reseñarse, igualmente, el carácter básico o mínimo que revisten las previsiones establecidas en el Reglamento, en cuanto aplicables a todo tipo de ficheros que contengan datos de carácter personal con independencia de las medidas especiales que puedan establecerse para ficheros que, por la peculiar naturaleza de los datos contenidos en ellos, exijan una mayor protección.

Niveles de seguridad

Las disposiciones reglamentarias se articulan en torno a tres niveles de seguridad, que se establecen atendiendo a la naturaleza de los datos que son objeto de tratamiento. Las exigencias y medidas de seguridad se disponen de manera 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.

Los ficheros que contengan datos referidos a la salud y a la vida sexual de las personas se clasifican entre los de nivel alto, lo que implica, en principio, el sometimiento de los sistemas de información clínica al grado más elevado de protección dispensado por la norma reglamentaria.

El establecimiento de tres niveles de protección trasciende asimismo al ámbito de aplicación temporal del Reglamento, que dispone la implantación de las medidas de nivel básico en el plazo de seis meses desde su entrada en vigor (prevista para el día siguiente a su publicación oficial), en el de un año en el caso de las medidas de nivel medio, y en el de dos años para las de nivel alto. El primero de los plazos resulta, por lo demás, ampliado hasta el 26 de marzo de 2000 en virtud de la modificación introducida por el Real Decreto 195/2000, de 11 de febrero.

Ámbito de aplicación

El Reglamento es de aplicación, según se ha visto, a los tratamientos de datos personales de carácter automatizado, si bien la norma se encarga de precisar que sus previsiones resultan aplicables íntegramente a tales ficheros ya sean permanentes o temporales, ordenando respecto de estos últimos su borrado una vez que dejen de ser necesarios para los fines que motivaron su creación. Asimismo, las medidas establecidas para cada uno de los niveles se aplican al acceso a datos de carácter personal a través de redes de comunicaciones, según señala el art. 5 del Reglamento.

El documento de seguridad.

La regulación descansa, como elemento básico, en el documento de seguridad, en el que deben integrarse y contenerse las medidas, normas y procedimientos de seguridad establecidos por el responsable del fichero conforme a las propias exigencias del Reglamento; de ahí que éste defina un contenido mínimo del documento de seguridad, respecto del que se ordena asimismo su permanente revisión y actualización en función de las modificaciones operadas en el propio sistema de información o en las disposiciones normativas aplicables en materia de seguridad.

Las normas establecidas para el nivel básico, y aplicables por tanto a todo fichero, vienen referidas a las funciones y obligaciones del personal, a la existencia de un registro de incidencias, a la identificación y autentificación de usuarios, a los controles de acceso, a la gestión de soportes y a las copias de respaldo y seguridad. En los niveles superiores, con carácter general, se incrementan las exigencias impuestas para cada uno de tales aspectos, incorporando en algunos supuestos obligaciones añadidas, como es el caso de la figura del responsable de seguridad y la auditoría (interna o externa) en los ficheros de nivel medio (y por tanto, también en los de nivel alto), o la necesidad de cifrado de datos para la distribución de soportes de datos, o transmisión de los mismos a través de redes de comunicaciones, en el caso de los ficheros de nivel alto.

Algunas consideraciones de carácter jurídico

a) A la vista del criterio establecido para determinar la aplicación de las medidas de seguridad de uno u otro nivel, reviste un notable interés, desde un punto de vista jurídico, la delimitación del concepto de "datos de salud" a que alude el Reglamento. A falta de una definición legal del término, parece que debe considerarse incluida dentro del mismo toda información referida al estado de salud física o mental de la persona, no estando tan claro que constituyan datos de tal naturaleza (aunque puede resultar discutible) aquellas informaciones de tipo administrativo o burocrático referidas al proceso asistencial. Tampoco la jurisprudencia aclara demasiado al respecto, ya que los escasos pronunciamientos recaídos hasta el momento se han dictado sobre supuestos de hecho no dudosos, como es el caso de la sentencia 202/1999, de 8 de noviembre, ya citada, del Tribunal Constitucional, que considera de tal naturaleza la información relativa al diagnóstico médico contenida en una base de datos de absentismo laboral.

b) Por otro lado, y aun cuando afecta a aspectos de naturaleza esencialmente técnica, es llamativo, desde una perspectiva legal, el alto nivel de exigencia que deriva de la aplicación estricta del Reglamento de medidas de seguridad, que en ocasiones plantea dudas reales respecto de la posibilidad misma de cumplimiento de sus previsiones. A efectos ilustrativos cabe citar, por ejemplo, el ya comentado registro de accesos que es obligatorio para los ficheros de nivel alto, y cuya efectiva implantación parece requerir, desde un punto de vista estrictamente técnico, una capacidad de los sistemas de información muy superior a la necesaria para el propio tratamiento de los datos. La referencia al "estado de la tecnología" que se contiene en el artículo 9 de la Ley al establecer el deber de adopción de las medidas de seguridad de los datos queda, en cierto modo, puesta en entredicho con previsiones como la que se examina.

c) Como último aspecto de la regulación en materia de seguridad, cabe mencionar la remisión al régimen sancionador de la Ley Orgánica 5/1992 (referencia que hay que entender hecha en la actualidad a lo dispuesto en la Ley Orgánica 15/1999) para el caso de incumplimiento de las medidas de seguridad impuestas por el Reglamento; régimen que, como es sabido, determina la inaplicación de sanciones económicas a las infracciones cometidas por las Administraciones Públicas, sustituidas por la facultad de la Agencia de Protección de Datos de dictar resolución con las medidas de obligado cumplimiento para el cese de la conducta infractora y de proponer la iniciación de las actuaciones disciplinarias oportunas.

A MODO DE CONCLUSIÓN

El examen jurídico de la regulación relativa al tratamiento de datos de carácter personal, y específicamente en materia de seguridad y confidencialidad, parece arrojar más dudas que certezas en relación con un marco legal que, sin demasiados

riesgos, puede calificarse como exigente y riguroso. Las críticas, sin embargo, no deben dirigirse contra esta última caracterización (fruto de una determinada opción legislativa), sino contra la falta de una clara delimitación de aspectos y elementos esenciales que afectan al propio ámbito de protección dispensado por de la norma o a la aplicación de instrumentos y garantías esenciales previstos por la misma.

Las incertidumbres sobre la interpretación y aplicación que definitivamente se dé a la Ley Orgánica 15/1999 son por ello importantes, y frente a las mismas cabe reclamar más que nunca la necesidad de un criterio ponderado que conjugue los intereses que se tratan de proteger con la debida consideración de la realidad social en que la norma debe ser aplicada.

ANEXO. RELACIÓN DE NORMAS Y SENTENCIAS CITADAS

1. Ley 14/1986, de 25 de abril, General de Sanidad. BOE 29-4-1986, núm. 102.
2. Ley Orgánica 5/1992, de 29 de octubre, por la que se regula el tratamiento automatizado de los datos de carácter personal. BOE 31-10-1992, núm. 262.
3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal. BOE 14-12-1999, núm. 298.
4. 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. DOCE nº L 281/39.
5. 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. BOE 25-6-1999, núm. 151.
6. Ley Orgánica 1/1982, de 5 de mayo, reguladora de la protección civil del honor, de la intimidad personal y familiar y de la propia imagen. BOE 14-5-1982, núm. 115.
7. Sentencia del Tribunal Constitucional 254/1993, de 20 de julio. BOE 18-8-1993.
8. Sentencia del Tribunal Constitucional 143/1994, de 9 de mayo. BOE 13-6-1994.
9. Sentencia del Tribunal Constitucional 11/1998, de 13 de enero. BOE 12-2-1998.
10. Sentencia del Tribunal Constitucional 202/1999, de 8 de noviembre. BOE 16-12-1999.
11. Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. BOE 4-1-2001.