

“La protección de datos sanitarios en el sector farmacéutico”

- 1.- Introducción. Objeto del trabajo.....4
- 2.- Aproximación al derecho a la protección de datos: un acercamiento a su régimen jurídico.5
 - 2.1.- La *libertad informática* como límite a la creciente utilización de tratamientos automatizados con datos de carácter personal.....7
 - 2.2.- Breve resumen de las disposiciones relativa a la *libertad informática* anteriores a la Ley Orgánica 15/99, de Protección de Datos de Carácter Personal (LOPD).....9
 - 2.3.- La Ley Orgánica 15/99, de Protección de Datos de Carácter Personal.....16
- 3.- La especialidad de los datos sanitarios.....18
 - 3.1.- Aproximación al concepto de “dato sanitario”.....18
 - 3.2.- Los datos “especialmente sensibles” en la LOPD.....20
 - 3.2.1.- El consentimiento.....22
 - 3.2.2.- Excepciones recogidas en la LOPD a la hora de otorgar el consentimiento.....25
- 4.- La especialidad en el sector farmacéutico.....28

La protección de datos sanitarios en el sector farmacéutico

- 4.1.- La especialidad en los colegios oficiales de farmacéuticos.....30
 - 4.1.1.- Ficheros privados y públicos.....30
 - 4.1.2.- Los datos de facturación de los colegios oficiales de farmacéuticos.....32
 - 4.1.3.- El carácter de “fuente accesible al público” de algunos ficheros.....35
 - 4.1.4.- Otros aspectos.....39
- 4.2.- La especialidad en la Oficina de Farmacia.....41
 - 4.2.1.- La receta electrónica: el caso de Castilla La Mancha.....42
 - 4.2.2.- La cesión de datos para la elaboración de fórmulas magistrales. El caso de Castilla La Mancha.....45
 - 4.2.3.- La aplicación del Real Decreto 994/1999, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.....48
 - 4.2.4.- Otros aspectos.....64
- 5.- Bibliografía.....70

ABREVIATURAS

| | |
|-------------|--|
| C.E..... | CONSTUCIÓN ESPAÑOLA |
| LOPD | LEY ORGÁNICA DE PROTECCIÓN DE DATOS |
| LORTAD..... | LEY ORGÁNICA DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL |
| RMS. | 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 |
| STC | SENTENCIA DEL TRIBUNAL CONSTITUCIONAL |
| STS..... | SENTENCIA DEL TRIBUNAL SUPREMO |

1.- Introducción. Objeto del trabajo.

Resulta innegable que la aparición de las “TIC” como herramienta potenciadora de la actividad empresarial, trae consigo una variedad de problemas jurídicos de diversa índole. Entre éstos, los más relevantes se presentan como aquellos que hacen referencia a derechos constitucionalmente reconocidos, y más concretamente, los relativos a la privacidad de los usuarios o interesados. En efecto: con frecuencia encontramos en la prensa diaria noticias sobre la aparición de historiales clínicos en la calle, o cesiones de datos considerados como especialmente sensibles sin el previo consentimiento expreso¹. Resulta lamentable, pero esto es mucho más habitual de lo que en un primer momento pudiera parecer².

En particular, la problemática respecto a los datos sanitarios es clara. La Agencia Española de Protección de Datos (AEPD), consciente de la importancia, ha venido interpretando la legislación de forma muy proteccionista de cara al interesado, hasta el punto de considerar dato “especialmente sensible” a informaciones relativas en nóminas de los empleados de una empresa (ya que existen informaciones relativas a las retenciones del impuesto sobre la renta), por poner un ejemplo.

La revolución tecnológica de esta “Sociedad del Conocimiento” abarca todos los sectores, incluyendo, como no podía ser de otra forma, al sanitario. Pero es precisamente en este sector donde la privacidad se puede vulnerar de una forma mas contundente, por el grado de sensibilidad de los datos objeto de tratamiento. El objeto del presente trabajo monográfico es estudiar la situación de los datos sanitarios en el sector farmacéutico. Habrá que recurrir no solo a la legislación básica, sino también a ciertas disposiciones autonómicas para estudiar casos concretos, ya que se pretende un acercamiento a un ámbito geográfico muy concreto: Castilla La Mancha.

¹ Para referirse al problema DEL PESO NAVARRO utiliza una frase bastante gráfica: “Tu dato es mi conocimiento”. Quiere ello decir que los titulares de la información sobre nuestra persona somos nosotros mismos, y se nos deberán respetar nuestras garantías. “*Ley de Protección de Datos: la nueva LORTAD*”. Ed. Experiencia, Madrid, 1999.

² Como señalan los autores, “...la tecnología informática permite (gracias a sus posibilidades prácticamente ilimitadas de captar, almacenar, relacionar y transmitir todo tipo de datos) reunir de forma personalizada, a partir de informaciones dispersas —e incluso anónimas—, múltiples facetas de la vida de hombres y mujeres totalmente ajenos al hecho de que sus hábitos vitales están en manos de terceros dispuestos a utilizarlos y aun a costa de depararles perjuicios importantes...” FERNÁNDEZ DOMÍNGUEZ, J., RODRÍGUEZ ESCANCIANO, S. “*Utilización y control de datos laborales automatizados*”, Agencia de Protección de Datos. 2001.

2.- Aproximación al derecho a la protección de datos: un acercamiento a su régimen jurídico.

Se suele afirmar que el derecho a la protección de datos es un “novísimo derecho fundamental”³. Lo cierto es que esto no es exactamente así⁴. A pesar de que los problemas derivados entre la Sociedad de la Información y la privacidad han propiciado la existencia de numerosos estudios sobre el tema, podríamos situar en la década de los setenta los primeros trabajos verdaderamente importantes.

Todos ellos tienen en común varios denominadores:

-Una preocupación constante relativa a los avances tecnológicos y la creciente automatización de las bases de datos que contienen datos de carácter personal.

-El constante peligro que supone la introducción de las redes de telecomunicaciones para la informática empresarial.

Antes de profundizar, será preciso establecer y fijar los conceptos oportunos. Para referirnos al Derecho a la Protección de Datos se suelen citar varias acepciones, entre las que destacan las siguientes:

-Derecho a la Intimidad Informativa. La elaboración de esta acepción la podemos situar en un momento anterior al Derecho a la Autodeterminación Informativa. Va encaminada a proteger la intimidad de las personas frente a la captación de sus datos de carácter personal, informatizados o no. Ello es lógico, ya que estamos aún en una fase embrionaria de formación del derecho.⁵

³ Rafael de Mendizábal Allende.

⁴ De hecho algún autor ha realizado estudios sobre distintas generaciones de Leyes de Protección de Datos existentes, ordenándolas cronológicamente.

⁵ Fueron varios autores ingleses los que mencionaron este derecho en la década de los setenta, entre ellos Richard F. Hixon y Alan F. Westin.

La protección de datos sanitarios en el sector farmacéutico

-Derecho a la Autodeterminación Informativa⁶. Se menciona, por citar solo los ejemplos mas representativos, en la stc 254/93 del Tribunal Constitucional o más recientemente, 290/2000.⁷ Aunque es preciso recurrir a la trascendental stc del Tribunal Federal Alemán, de 15 de Diciembre de 1983, donde encontramos la primera aproximación a su significado.⁸ Se podría definir como todo derecho que tienen los interesados a decidir por sí mismos cuándo y dentro de qué límites procede revelar secretos referentes a su propia vida o existencia.

-Habeas Data. Quizás en un aspecto más concreto, como es el ámbito del reconocimiento de los derechos del interesado (acceso, modificación, cancelación y oposición), se menciona este término como la principal garantía legal que asiste a quien suministre una información de carácter personal. Se trata del derecho que asiste a toda persona, identificada o identificable a solicitar la exhibición de los registros, públicos o privados, en los cuales estén incluidos sus datos personales, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación, por ejemplo afiliación a partido político, creencia religiosa.

-Libertad Informática. Por citar el ejemplo más destacable, sería necesario recurrir de nuevo a la stc. 254/93. La misma concluye que la libertad informática forma parte del contenido esencial de los derechos fundamentales del artículo 18.1 CE. Y es que, esta libertad es también “garantía de otros derechos, especialmente el honor y la intimidad”.⁹ La definición es muy cercana al anteriormente mencionado “Derecho a la Autodeterminación Informativa”: “La «libertad informática», reconocida por el art. 18.4 de la Constitución, ya no es la libertad de negar información sobre los propios hechos

⁶ Para la mayoría de la doctrina, especialmente para GRIMALT SERVERA, la autodeterminación informativa es el bien jurídico protegido de la LOPD.

⁷ Sin embargo, es PEREZ LUÑO, el verdadero artífice de la introducción en España de la expresión «derecho a la autodeterminación informativa».

⁸ «la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de datos concernientes a la persona. (...) El derecho fundamental garantiza, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y la utilización de sus datos personales». STC. del Tribunal Federal Alemán, de 15 de Diciembre de 1983.

⁹ STC. 254/93.

privados o datos personales, sino la libertad de controlar el uso de esos mismos datos insertos en un programa informático: lo que se conoce con el nombre de *habeas data*”¹⁰.

En este apartado se pretende hacer un acercamiento de la evolución que se ha sufrido en el derecho a la protección de datos, culminando con un breve resumen de la Ley Orgánica 15/99, de Protección de Datos de Carácter Personal (LOPD), completándola con las interpretaciones jurisprudenciales más importantes de la misma.

2.1.- La libertad informática como límite a la creciente utilización de tratamientos automatizados con datos de carácter personal.

Fijado este concepto, es necesario hacer una apreciación al respecto. La *libertad informática* pertenece a la esfera del individuo, tratándose de un derecho personalísimo que asiste al interesado para decidir cuándo y en que momento el mismo puede decidir sobre la inclusión de sus datos en ficheros. Y nuestra Carta Magna parece prever que existe un peligro para la intimidad personal si la informática se complementa con datos que afectan a la intimidad del individuo. No parece casualidad que el art. 18.4 comience diciendo que la “ley limitará la informática...”. Es la única vez que la Constitución menciona a la informática, y no lo hace para potenciar su uso precisamente. Mas bien lo contrario.¹¹

¹⁰ Stc. 254/93.

¹¹ Este detalle ha sido puesto de manifiesto por varios autores, entre ellos el actual director de la Agencia de Protección de Datos de la Comunidad de Madrid, D. Antonio Troncoso Reinada. Sin duda, es de suma importancia que en el año de creación de la constitución se tuviera en cuenta lo que la doctrina llama “la informática”. Un acierto sin duda, por el ánimo de previsión que tuvieron nuestros constituyentes. En la actualidad, en el ámbito de la Constitución Europea, tras debatir varias propuestas planteadas en el Grupo Carta se decide incluir en la Parte I del texto constitucional de forma expresa e independiente del resto de los derechos de la Carta el derecho a la protección de datos. En dicho texto encontramos las siguientes menciones expresas al derecho a la protección de datos:

“Artículo I-51: Protección de datos personales

1. Toda persona tiene derecho a la protección de los datos personales que la conciernan.
2. Las normas sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, organismos y agencias de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos se establecerán mediante una ley europea. El respeto de dichas normas estará sometido al control de una autoridad independiente.”

Por su parte, en el art. II-68 encontramos la siguiente referencia:

La protección de datos sanitarios en el sector farmacéutico

No estamos frente a un derecho de los reconocidos en el apartado primero del art. 18 (honor, intimidad, propia imagen). Mas bien ante un derecho autónomo, aunque muy ligado a éstos. Este carácter bifronte del mismo encuentra su máxima expresión en la mencionada stc 254/93 de nuestro Tribunal Constitucional¹²

La Libertad Informática se perfila como una protección y garantía constitucional que asiste a todo ciudadano. Si uno de los valores máximos de nuestra Constitución es la protección del Derecho al Honor, Intimidad y Propia Imagen, ello puede vulnerarse desde muy diversos ángulos, incluyendo y especialmente, desde las grandes bases de datos automatizadas, en definitiva, potenciándose con las herramientas que la anteriormente mencionada “informática” y en la actualidad, “Sociedad de la Información”, pone a disposición de los sectores público y privado.

“Artículo II-68.

Protección de datos de carácter personal:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.”

Nótese cómo este último apartado 2 recoge el “Principio de Calidad” de los datos (art. 4 LOPD) y los derechos de los interesados (acceso, rectificación, cancelación y oposición).

En cualquier caso, como señala Ernesto Quílez, “...a estas alturas ya no sorprende la referencia a este derecho en un texto constitucional pues contamos con notables y diferentes precedentes normativos y como tal ha sido suficientemente asentado por la jurisprudencia y doctrina, sin embargo, es de advertir que su mención expresa en el proyecto de Constitución Europea no se contemplaba en los primeros borradores y su posterior introducción primero como art. 36 bis- no ha sido ajena a la controversia dentro el Grupo de trabajo. Por supuesto, nadie pretendía prescindir del Derecho a la protección de datos pero sí que se ha discutido oportunidad de recoger de manera expresa e independientemente dentro del articulado de la futura Constitución Europea”. *La regulación de la protección de datos en el proyecto de Constitución Europe*. Datospersonales.org.

¹² Dispone la Sentencia que “nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos 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, lo que la Constitución llama «la informática»”

2.2.- Breve resumen de las disposiciones relativas a la *Libertad Informática* anteriores a la Ley Orgánica 15/99, de Protección de Datos de Carácter Personal (LOPD).

La formación de este derecho no ha sido precisamente un camino sencillo.

Han sido muchos los estudios y disposiciones que han surgido a partir de la década de los sesenta. Su número e importancia parece que va en consonancia con el avance de las Tecnologías de la Información y Comunicación. En cierta forma, parece como si un avance de las mismas no pudiera producirse sin poner en peligro la privacidad de los usuarios. Muchos autores y muchas instituciones han estudiado esta relación¹³. Se citan a continuación los ejemplos más representativos:

-La Asamblea del Consejo de Europa. Esta Institución creó varias comisiones y redactó distintas resoluciones a partir de la segunda mitad de la década de los sesenta. Por citar un ejemplo, en el año 1967, se creó una comisión consultiva para estudiar el impacto de las nuevas tecnologías en el ámbito de los Derechos Humanos. Un año después, esa comisión redactó una Resolución, donde se revela la necesidad de establecer mecanismos de protección tanto sobre la vida privada de las personas como sobre otros derechos fundamentales que podrían afectarse con la aparición de las nuevas tecnologías.¹⁴ Lo más destacable de los trabajos de esta comisión es que no se alude a la "Protección de Datos" como tal, pero sí se pone de manifiesto lo peligroso de las nuevas

¹³ Para DEL PESO NAVARRO, los documentos claves de todos los que se mencionan son los siguientes:

-El Convenio del Consejo de Europa, de 28 de Enero de 1981.

-El Acuerdo de Schenguen, de 14 de Junio de 1985.

-La Propuesta de Directiva del Consejo de la Comunidad Económica Europea de 24 de Septiembre de 1990, relativa a la protección de las personas en lo referente al tratamiento de datos personales (modificada el 15 de Octubre de 1992), hoy Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995. "Ley de Protección de Datos: la nueva LORTAD", ed. Díaz de Santos, Madrid, 1999.

¹⁴ Otro ejemplo es la Resolución del Comité de Ministros de 26 de Septiembre de 1973, relativa a "La protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado", la Resolución de 20 de Septiembre de 1974 relativa a "la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público" y la Resolución del Comité de Ministros de 1976 por la que se crea una comisión de expertos encargada de desarrollar los trabajos preparatorios de lo que será un futuro Convenio sobre la materia.

tecnologías cuando se combinan con informaciones que pertenecen a la esfera privada del individuo.

-La Organización para la Cooperación y el Desarrollo Económicos (OCDE). En esta institución se realizaron trabajos muy en sintonía con el Consejo de Europa.¹⁵ Lo más destacable de los estudios producidos en el seno de esta Institución son las similitudes a la hora de definir conceptos. Así, a la hora de definir “dato de carácter personal”, se hace mención a “cualquier información relacionada con un individuo identificado o identificable”. Estas definiciones se “transplantarían” casi directamente un año después, en el trascendental Convenio 108 del Consejo de Europa. De hecho, esta definición está recogida en la actualmente vigente LOPD¹⁶

-Consejo de Europa. Sin lugar a dudas, el Convenio 108 del Consejo supuso la “oficialización” del Derecho a la Protección de Datos. Su influencia es tal, que probablemente no se entendería las actuales leyes de protección de datos europeas si no recurrimos al mismo, ya que en todas, en mayor o menor medida, ha extendido su manto de influencia. Hacer un resumen del mismo supone en gran parte hacer un resumen de nuestra LOPD. Existen similitudes conceptuales y, sobre todo, en los principios generales.¹⁷ Lo cierto es que en una época anterior a la LOPD, incluso a la

¹⁵ El estudio mas representativo, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, de 23 de Septiembre de 1980.

¹⁶ Art. 3 apartado A.

¹⁷ Por citar varios ejemplos:

- Se prohíbe el tratamiento automatizado de informaciones referentes al origen racial, opiniones políticas, creencias religiosas u otras, salud sexual y condenas penitenciarias (artículo 6).
- Se hace hincapié en la seguridad de los registros de los datos (artículo 7). Podemos considerarlo el antecedente del RMS.
- La exigencia de veracidad y correcta utilización de los datos (artículo 5). Mención del “Principio de Calidad de los Datos”. Hoy este principio se encuentra recogido en el art. 4 de la LOPD.
- El reconocimiento del derecho por parte de los interesados a conocer la existencia de datos que les conciernen, la posibilidad de cancelarlos o corregirlos (Artículo 8). Se trata de un reconocimiento del *Habeas Data*. Está recogido en los actuales arts. 15, 16 y 17.

LORTAD, se planteó la aplicabilidad de los conceptos de este convenio en nuestro ordenamiento jurídico. La STC 254/93 zanjó la cuestión en los siguientes términos: “es lo cierto que los textos internacionales ratificados por España pueden desplegar ciertos efectos en relación con los derechos fundamentales, en cuanto pueden servir para configurar el sentido y alcance de los derechos recogidos en la Constitución, como hemos mantenido, en virtud del art. 10.2 C.E., desde nuestra stc 38/1981”. A través de la ratificación por parte de España del Convenio Schengen, se obligaba al legislador a respetar las directrices dadas en el Convenio 108¹⁸.

-Acuerdo Schengen. Con el mismo se pretende la eliminación de los controles trasfronterizos en los países firmantes del mismo. El Acuerdo de Schengen fue establecido el 14 de Junio de 1985 entre el Benelux, la República Federal Alemana y Francia. Al mismo se adhirió posteriormente España, Portugal y Grecia. España lo hizo el 25 de Junio de 1991 y se ratificó el 23 de Julio de 1993. El verdadero valor del Acuerdo de Schengen fue el impulso que dio para la entrada en vigor en España de la LORTAD. Si el art. 18.4 es una previsión legal constitucional (“la ley limitará la informática...”), el Acuerdo de Schengen supone que los países firmantes han de adoptar las disposiciones necesarias que garanticen un nivel de protección de los datos de carácter personal que sea al menos, igual al resultante de los principios del Convenio

-
- La facultad de recurrir ante cualquier trasgresión de los derechos antes mencionados (Artículo 8). En la actualidad, este artículo ha influido claramente en los dos procedimientos a los que puede recurrir cualquier ciudadano ante una vulneración de sus derechos: el principio de tutela de derechos y el procedimiento sancionador, hoy recogidos en nuestra LOPD.
 - Los límites que el Convenio establece al ejercicio del derecho a la libertad informática son (artículo 9.1):
 - La seguridad del Estado.
 - La protección de los demás derechos fundamentales.
 - El artículo 3 del Convenio establece que su acción de protección comprende a "los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores públicos y privados". Ello está recogido en el art. 2 de nuestra LOPD.

¹⁸ La ratificación por España finalmente se produjo el 27 de Enero de 1984. Pero ello no suministraba la cobertura precisa para proteger nuestros datos personales ante el uso de la informática. Aunque el Convenio se ha incorporado ya a nuestro ordenamiento jurídico conforme al artículo 96.1 de la Constitución, hay que decir, aún así, que no estamos ante un derecho inmediatamente aplicable. La razón es que los principios recogidos en el art. 4.1 han de ser satisfechos por el legislador nacional. Su virtualidad consiste precisamente en obligar al Estado ante los demás firmantes del Convenio a proceder a su desarrollo. Este fue el verdadero valor de Schengen: el adelantar la aparición de la LORTAD.

La protección de datos sanitarios en el sector farmacéutico

del Consejo de Europa de 28 de Enero de 1981¹⁹. Esto supone un “apremio” para que el legislador tome, definitivamente, cartas en el asunto. En suma, adoptar el Convenio de Schengen significaba que España debía respetar los principios del Convenio 108, y la mejor forma de hacerlo era legislando.

-Asamblea General de las Naciones Unidas. También esta institución ha realizado diversos estudios. Es destacable el documento “Principios rectores para la reglamentación de los ficheros automatizados de datos personales”. Fueron adoptados por la Asamblea General de las Naciones Unidas en su resolución 45/95 del 14 de diciembre de 1990. Lo mas destacable de los mismos son, precisamente, los principios a los que se hace referencia.²⁰

-Tribunal Federal Alemán. Sentencia de 15 de Diciembre de 1983. Se trata de la plasmación jurisprudencial del Derecho a la Libertad Informática²¹. La Ley declaró inconstitucionales algunos artículos de la Ley del Censo de la República Federal Alemana. El movimiento “los verdes” interpuso el recurso, obteniendo una resolución

¹⁹ ...y respetando la Recomendación R(87)15 de 17 de septiembre de 1987 del Comité de Ministros del Consejo de Europa, dirigida a regular la utilización de datos de carácter personal en el sector de la policía (art. 117 del Convenio).

²⁰ Los mas destacables son los siguientes:

Principio de la licitud y lealtad: Las informaciones relativas a las personas no se deberían recoger ni elaborar con procedimientos desleales o ilícitos, ni utilizarse con fines contrarios a los propósitos y principios de la Carta de las Naciones Unidas.

Principio de exactitud: Las personas encargadas de la creación de un fichero o de su funcionamiento deberán tener la obligación de verificar la exactitud y pertinencia de los datos registrados y cerciorarse de que siguen siendo lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen, periódicamente o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando.

Otros principios importantes son el *principio de finalidad* o el *principio de acceso a la persona interesada*. Casi todos se corresponden con los principios que impulsan nuestra LOPD, y, por extensión, las normas anteriores.

²¹ Podríamos considerar a Alemania como el país impulsor de la disciplina. De hecho, la protección de los datos de carácter personal comienza en Europa en el año 1970 en el Land de Hesse de la República Federal Alemana (Datenschutz de 7 octubre de 1970) que posteriormente sería modificada en 1978 y 1986.

cautelar del alto tribunal, suspendiéndose la Ley del Censo, para posteriormente tomar una decisión definitiva sobre el fondo del asunto.²²

De la misma es necesario destacar el “antes y después” que supuso en la doctrina. Podríamos decir que ahora existe un concepto “positivo” del derecho a la intimidad, cuando antes se consideraba nada más que su esfera “negativa”. La STC establece que se deben arbitrar algunas medidas directas de cara al individuo para que el mismo controle el flujo de datos personales existentes. Hasta ahora la *libertad informática* se postulaba como un “freno” al estado. A partir de ahora se sabe que es necesaria una actitud activa por parte del mismo, ya que la privacidad se puede vulnerar igualmente.

Del mismo modo la STC establece que el individuo puede verse privado en sus derechos, más concretamente a la hora de decidir por “autodeterminación”, si el mismo conoce o sabe que los poderes públicos conocen determinadas facetas de su personalidad. Estamos en la esfera de la “autodeterminación del individuo”. La propia STC la define como “el derecho a tomar las decisiones que el mismo crea convenientes”. Estas decisiones pudieran no tomarse en libertad, esto es, por “autodeterminación”, si el estado recaba datos referentes a la esfera privada del individuo.²³

Por último, es necesario destacar que el Derecho a la Libertad Informática tiene límites, como cualquier otro derecho. La propia STC establece que sólo bajo un mandato o previsión constitucional y ante la existencia de un interés general, se podrán recabar ciertas informaciones.

-Ley Orgánica 5/92, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD).

Se trata de la plasmación legal del art. 18.4. Estamos ante el “mandato constitucional” previsto. Es la primera norma de derecho interno sobre la protección de

²² La STC se pronuncia en los siguientes términos, al afirmar que los avances tecnológicos han propiciado “una imagen total y pormenorizada de la persona respectiva -un perfil de la personalidad-, incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en *“hombre de cristal”*”.

²³ La Ley del Censo Alemana, recurrida, establecía que el estado recabaría informaciones referentes al “último puesto que ocupó en una empresa” o “fuente de los medios principales de subsistencia”. Ello, entre más de 80 informaciones distintas.

datos personales. El Convenio del Consejo de Europa, ratificado a través de Schengen, no cumplía con esta previsión.

La propia exposición de motivos de la norma comienza recordando este mandato.²⁴ Sin embargo, lo más importante de la misma –de la que la propia LOPD, incomprensiblemente, carece– es la distinción que realiza entre intimidad y privacidad. Este segundo concepto, que transpone la noción angloamericana de *privacy*– derecho a disponer de cualquier aspecto de la personalidad, incluida la información o datos sobre la persona y de su actividad en cualquier esfera – desde luego tiene una esfera mas amplia que la propia intimidad.²⁵ La privacidad es el concepto que protege principalmente la Ley. Para la intimidad, los tres primeros apartados del art. 18 de la Constitución, parecen “ser suficientes”²⁶.

La norma se divide en dos partes principales. Una general, alimentada por los preceptos delimitadores del ámbito de aplicación de la Ley, los principios reguladores generales y, sobre todo, las garantías de la persona. Otra especial donde se concretan estos extremos, y donde se dividen a los ficheros en aquellos de titularidad pública o privada. Esta distinción continúa en la LOPD, al menos en gran medida.

En términos generales, la LORTAD recogía en su totalidad las previsiones del Convenio 108 del Consejo de Europa, inspirándose en otras leyes europeas. Sin embargo, la aparición de la Directiva 95/46/CE hizo que la norma tuviera que

²⁴ “...La Constitución española, en su artículo 18,4, emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. La aún reciente aprobación de nuestra Constitución y, por tanto, su moderno carácter, le permitió expresamente la articulación de garantías contra la posible utilización torticera de ese fenómeno de la contemporaneidad que es la informática”.

²⁵ “...en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.”

²⁶ Nótese que esto no es exactamente así. Sobre todo, es necesario mencionar las leyes que desarrollan a los 3 apartados del art. 18 de la Constitución. Por citar un ejemplo, la Ley 1/82 de protección civil del derecho al honor a la intimidad personal y familiar y a la propia imagen. Norma que vino a suplir provisionalmente durante diez años la ausencia de un desarrollo del artículo 18.4 de la Constitución.

adaptarse²⁷. Por citar un ejemplo, la Ley no acogía en absoluto previsión alguna respecto a los datos contenidos en soporte físico, aspecto que chocaba frontalmente con la Directiva.

-Directiva 95/46/CE, del Parlamento Europeo y del Consejo. Ya dentro de la Unión Europea, la entrada en vigor de este texto supuso que todos los países miembros tuvieran legislaciones más homogéneas. Si hasta el año 95 habría que recurrir al Convenio 108 para encontrar un texto unificador y más o menos vinculante en materia de protección de datos en el contexto internacional, ésta Directiva supuso que todos los países miembros se vieran obligados a adaptar a sus legislaciones lo previsto en la misma.

Fueron varios los motivos que propiciaron su aparición. En plena inicio de la “Sociedad del Conocimiento”, en la década de los 90 se tuvo conciencia, no obstante, de la peligrosidad que suponía las informaciones con datos de carácter personal en soporte físico. Se pensó que no había razón alguna para dejar fuera del ámbito de aplicación de la ley a la ingente cantidad de ficheros e informaciones en soporte papel existente ya que la intimidad se podía vulnerar independientemente del soporte en el que los mismos estuvieran recogidos.²⁸

En la Directiva se siguen mencionando muchos de los principios del Convenio 108, si bien ahora existen matizaciones para los mismos. En términos generales, y además de contemplar a los ficheros en soporte físico, se hace mención a las “medidas de seguridad” que los ficheros deberán cumplir,²⁹ deberes de información para el Responsable del Fichero a la hora de recabar sus datos, necesidad de consentimiento

²⁷ Para VIZCAÍNO CALDERÓN, “La Ley de 1992 fue, en general, una buena Ley dictada en una situación de notable indiferencia social sobre las amenazas que las tecnologías de la información suponían para la privacidad de los ciudadanos”. “*Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*”, Civitas, 2001. Pág. 25.

²⁸ ORTÍ VALLEJO aludía a que “los ficheros manuales presentan más amenazas para la vida privada y las libertades, pues cuando se componen de centenares de miles o incluso de millones de fichas, su puesta al día no es posible, con lo cual se mantendrían inexactitudes en los datos personales. Los ficheros automatizados frente a los manuales tienen la ventaja de poder ser destruidos fácilmente y ser susceptibles de medidas de seguridad más eficaces para hacerlos confidenciales...se puede concluir de lo expuesto, que existen razones de peso para atraer a la órbita de la LORTAD los ficheros manuales”. “*Derecho a la Intimidad e Informática*”, Comares, 1994.

²⁹ Aludiéndose al “Principio de Seguridad de los Datos”, recogido hoy en nuestro RMS.

“reforzado” a la hora de recabar cierto tipo de datos –los especialmente protegidos-, además de la alusión al principio del “consentimiento inequívoco” del interesado o la alusión a los Derechos de acceso, cancelación y rectificación –mecanismo vertebrador para el verdadero ejercicio del “habeas data”-. La LORTAD debería ser reformada para adaptarse a esta Directiva.

2.3.- La Ley Orgánica 15/99, de Protección de Datos de Carácter Personal.

La modificación de la LORTAD con objeto de adecuarlo a la Directiva tuvo lugar con la creación de la Ley Orgánica de Protección de Datos³⁰, ley actualmente en vigor y que ha supuesto una verdadera actualización en esta materia, aunque respetando, como se verá a continuación, los principios esenciales contenidos en los anteriores textos.

No es objeto de este trabajo hacer una profundización en la norma, sin embargo, si se estima imprescindible destacar sus caracteres generales más importantes:

-Ámbito de aplicación mucho más amplio³¹. La única diferenciación entre los ficheros manuales y automatizados es el plazo de adaptación para adecuarse a lo que se ordena en la ley.³² Si la misión de la LORTAD era dar cumplimiento al mandato constitucional del art. 18.4, la de la LOPD es proteger los derechos contenidos en la Sección 1ª del Capítulo II del Título Primero de nuestra Carta Magna en lo que concierne al tratamiento de los datos personales y especialmente para garantizar el honor y la intimidad personal y familiar de las personas físicas, nada menos³³.

³⁰ Es necesario señalar que la LOPD no es, en sí misma y en su conjunto, una norma con rango de Ley Orgánica. No todos los preceptos de la Ley tienen este carácter, por lo que algunos se califican de Ley Ordinaria, de acuerdo con la doctrina del Tribunal Constitucional, que es proclive a reservar el carácter de Orgánica en relación a aquellos preceptos que afrontan directamente la regulación de los derechos y libertades de los artículos 15 a 30 de la C.E.

³¹ Para VIZCAINO CALDERÓN, “una de las particularidades de la normativa estriba, probablemente, en que su ámbito subjetivo y objetivo es tan sumamente amplio que su total cumplimiento resulte, quizás, una utopía”, *“Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal”*, ed. Civitas, Madrid, 2001.

³² 12 y 3 años, respectivamente, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados en el caso de los ficheros manuales.

³³ Todos los autores consultados (ver bibliografía) coinciden en el vasto ámbito de aplicación de la norma. Valga como ejemplo el siguiente: a principios del año 2004, el director de la AEPD mencionó la necesidad de adecuarse a la norma para los ficheros automatizados de los teléfonos móviles que

La protección de datos sanitarios en el sector farmacéutico

-Se aclaran y matizan algunos conceptos. Por citar un ejemplo, ahora se especifica qué se entiende por “consentimiento del interesado”.³⁴ Ello no sucedía en la LORTAD. No obstante en la norma se habla de distintos tipos de consentimiento. Hubiera sido necesario que en la definición de consentimiento se explicara qué se entiende por “consentimiento expreso”³⁵. Otro ejemplo es la aclaración y enumeración de las “fuentes accesibles al público”.

-Ampliación de los responsables. Las presuntas vulneraciones de la norma ya no alcanzan sólo a los Responsables de los Ficheros. Con la creación de la figura del “Encargado de Tratamiento”, el abanico de responsables se amplía. La LOPD exige una serie de formalidades para que un tercero acceda a datos. Cuando ello sea necesario para la prestación de un servicio, “no se considerará cesión de datos”, pero la prestación habrá de estar regulado por escrito, o de alguna forma que acredite su cumplimiento.

-Creación del derecho de oposición. Si bien la LORTAD permitía al interesado negarse a facilitar una determinada información si ello no se estimaba imprescindible para la consecución de un determinado fin, ahora el mismo tiene este derecho no solo en el momento de suministrar y consentir el tratamiento, también en cualquier momento posterior a este. Ello se regulará por vía reglamentaria.³⁶

-Creación de la Agencia de Protección de Datos, ahora Agencia Española de Protección de Datos. Si en la exposición de motivos de LORTAD se decía que la misma se creaba para asegurar la máxima eficacia en la aplicación de sus disposiciones, considerándola un ente público, ahora, la LOPD dedica los arts. 35 a 42 a la misma. La AEPD tiene personalidad jurídica propia, plena capacidad de obrar, actúa con plena

contuvieran el nombre y el número de teléfono, así como otras informaciones, siempre en el caso en que los mencionados dispositivos se utilizaran en el ámbito profesional, esto es, fuera de las actividades domésticas (ficheros, estos últimos, excluidos por la aplicación del art. 2 LOPD). Otro ejemplo es la supresión de la palabra “automatizado” en las definiciones contenidas en la norma.

³⁴ Art. 3 apartado “h”: Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

³⁵ Se profundizará en ello a la hora de centrarse en los datos sanitarios, ya que los mismos están sometidos aun régimen reforzado a la hora de otorgar el consentimiento.

³⁶ La Instrucción 1/98 de la AEPD regula los derechos de acceso, cancelación y rectificación.

independencia de las administraciones públicas y se rige por lo especificado en la norma y en su propio estatuto.

-Se modifica el régimen del Movimiento Internacional de Datos. Se suavizan los requisitos para proceder con ello.³⁷

Algún autor señala también otras novedades de la LOPD³⁸:

-Mejoras en la tipificación de las conductas infractoras.

-Reforzamiento de la figura del consentimiento del interesado.

-Delimitación de la figura del encargado de tratamiento.

-Reforzamiento del principio de finalidad.

-Mayor clarificación y garantías adicionales en la información al ciudadano al tiempo de la recogida de sus datos.

3.- La especialidad de los datos sanitarios.

3.1.- Aproximación al concepto de “dato sanitario”.

Si uno de los aspectos mas criticados de la LOPD es el referente a la definición de algunos términos que encontramos en la norma, al referirnos al concepto de “dato sanitario” nuestras sospechan se confirman. Sencillamente, encontramos referencias a la

³⁷ Al respecto, la Instrucción 1/2000 de la Agencia de Protección de Datos, de 1 de Diciembre, dictada por el Director de la Agencia relativa a las normas por las que se rigen los movimientos internacionales de datos, es bastante clarificadora.

³⁸ FERNANDEZ LOPEZ, J., “La nueva Ley de Protección de Datos. Su porqué y sus novedades principales”. Actualidad Informática Aranzadi, Enero 2000.

expresión en sendos arts. 7 y 8, pero carecemos de definición.³⁹ Encontramos, no obstante, algunas directrices dadas en nuestra C.E.⁴⁰

Como primera aproximación, la Recomendación de 13 de Febrero de 1997, del Comité de Ministros del Consejo sobre Protección de Datos Médicos, da una definición general de "dato médico" definiéndolo como todo dato personal relativo a la salud de un individuo⁴¹.

Sí encontramos en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, definiciones mucho mas concretas. Así, "datos médicos" se refiere a todos los datos personales relativos a la salud de un individuo. Se refiere también a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos. Por extensión, "datos genéticos" se refiere a todos los datos, cualquiera que sea su clase, relativos a las características hereditarias de un individuo o al patrón hereditario de tales características dentro de un grupo de individuos emparentados. Como no podía ser de otra forma, y en consonancia con la LORTAD o LOPD, "dato de carácter personal" abarca cualquier información relativa a un individuo identificado o identificable. Un individuo no se considerará "identificable" si la identificación requiere una cantidad de tiempo y de medios no razonables. En los casos en que el individuo no sea identificable, los datos son denominados anónimos.⁴²

³⁹ Lo que si parece claro es que los datos sanitarios son datos de carácter personal y por lo tanto el tratamiento de los mismos queda bajo el ámbito de protección de la LOPD.

⁴⁰ Acertadamente, SERRANO PEREZ parte, a la hora de analizar la LOPD, del análisis de los arts. 14 y 16 de la C.E. El mencionado art. 14 prohíbe toda discriminación por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra circunstancia personal o social. El 16 garantiza la libertad ideológica, religiosa y de culto, especificando que nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cualquier análisis de los datos sanitarios debe tener en cuenta lo establecido en estos dos artículos. "El derecho fundamental a la protección de datos. Derecho español y comparado", ed. Civitas, Madrid, 2003.

⁴¹ El apartado 3 del Capítulo 5 establece que "Los datos relativos a la salud de las personas son aquellos datos que permiten conocer, respecto de una persona identificada, las dolencias o enfermedades que ha padecido, padece o incluso padecerá o tendrá tendencia a padecer en un futuro. Se trata de datos cuya relevancia social y cuyo potencial vulnerador de la intimidad personal nadie se atreve a poner en duda".

⁴² Es obvio que la "razonabilidad" para hacer anónimos o no unos datos dependerán de muchos y de muy variados factores. Se está pensando en la disociación de la información sensible, aspecto que recoge nuestra LOPD y que promueve la AEPD. Si tenemos unas informaciones relativas a un individuo pero no podemos ponerles nombres y apellidos, es claro que no existirá peligro para la intimidad del individuo, al no poder identificarse. En todo caso, ello dependerá de las claves o conexiones existentes entre las

La protección de datos sanitarios en el sector farmacéutico

Entre otros autores, SÁNCHEZ CARAZO⁴³, establece que dentro de los datos sanitarios estarán en todo caso informaciones relativas a “...los antecedentes médicos, los diagnósticos, los procedimientos realizados, el tratamiento, el pronóstico relativo a la salud física o psíquica”.

Para SERRANO PÉREZ⁴⁴, un dato sanitario, en la medida en que identifica a una persona que soporta un tratamiento médico, queda afectada por ese adjetivo, produciéndose una petrificación y sometiéndose por ello a las reglas específicas existentes para los datos sanitarios.

Por su parte, la AEPD siempre ha apostado por un criterio amplio del concepto, hasta el punto de considerar a cualquier tipo de conexión relativa a la salud del individuo como “dato sanitario”, y por ello, “dato especialmente protegido”. Así, en casi todas las memorias de la Agencia encontramos estudios de casos concretos que finalmente siempre se resuelven tendiendo a la esfera mas proteccionista respecto del interesado. En el ámbito que nos ocupa, la Agencia ha considerado “dato de salud” a las informaciones contenidas en las recetas expedidas por el Sistema Nacional de Salud (donde existen informaciones relativas a la identificación del paciente y del fármaco suministrado). También ha considerado datos referentes a minusvalías en las nóminas como dato relativo a la salud. Estos dos ejemplos son muy esclarecedores⁴⁵.

distintas bases de datos disociadas. El concepto de “razonabilidad” puede ser criticable por la dificultad y subjetividad del mismo. De hecho, a la hora de hablar de un procedimiento de disociación en el art. 3 apartado F, se define el mismo como “todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable”. Es decir, se trata de no dejar duda alguna al respecto.

⁴³ SÁNCHEZ CARAZO, C: *La intimidad y el secreto médico*; Ed. Díaz de Santos, Madrid, 2000.

⁴⁴ La autora llega a la siguiente conclusión: si se pretende proteger la intimidad de las personas y rodearlas de las máximas garantías, no cabe otra opción que proceder a esa afectación. “*El derecho fundamental a la protección de datos. Derecho español y comparado*”, ed. Civitas, Madrid, 2003.

⁴⁵ Sin embargo, existen muchos otros, ya que la AEPD no es ajena a la importancia del tema tratado. Por citar otros ejemplos:

-La AEPD concluyó que los datos psicológicos deben ser considerados a efectos de la LOPD, como datos relativos a la salud de las personas. No es importante, a estos efectos, que los mismos se encuentre incluidos en historiales clínicos o en formularios o encuestas.

-Del mismo modo, ha estimado que los datos genéticos son datos de salud.

-Se planteó y resolvió el problema acerca del carácter de los datos referidos a la salud y formación de empleados en las empresas. Si el trabajador no consiente expresamente acerca de estos

Podemos concluir este apartado confirmando y siguiendo el criterio de la AEPD. Consideraremos “dato sanitario” a cualquier información que, directa o indirectamente, haga referencia a la salud de las personas. Sí parece deseable una legislación específica sobre protección de datos sanitarios dada su especialidad, que aclare éste y otros conceptos.

3.2.- Los datos “especialmente sensibles” en la LOPD.

Si ya se ha esbozado la casi nula referencia a los datos sanitarios –al menos, en cuanto a su definición y limitación- que existen en nuestra LOPD, si resulta necesario adentrarnos en lo que establece la norma para los mismos.

Especifica el art. 7.3 de la LOPD que “los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente”. Sin embargo, encontramos una excepción en el mismo art. 7, esta vez en el apartado 6: “cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.”

Por su parte, el art. 8 especifica que “...sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad”.

datos, el empresario sólo podrá ser informado de las conclusiones que se deriven de los reconocimientos en relación con la aptitud del trabajador, pero en ningún caso estará habilitado para el tratamiento informático de los datos relativos a la salud.

Por último, en el art. 34 de la mentada norma, al referirse a los movimientos internacionales de datos, encontramos en el apartado “c” una excepción a la norma general. Dicha norma no se aplicará “...cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.”

Hay que destacar que apenas existen diferencias entre lo dispuesto en la LORTAD y lo dispuesto en la LOPD, salvo detalles no demasiado importantes. Por ejemplo, en el art. 8 de la LORTAD se hace referencia a una relación muy pormenorizada de leyes sanitarias existentes. En la actual LOPD se ha optado, acertadamente, por incluir una “cláusula abierta”.⁴⁶

3.2.1.- El consentimiento

Una de las características principales que diferencia a este tipo de datos lo encontramos en el momento en el que el interesado presta su consentimiento para el tratamiento de los mismos. A diferencia de la LORTAD, en la LOPD sí encontramos una definición para el consentimiento. Se trata de “toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”.⁴⁷

Llama la atención la expresión “inequívoca”.⁴⁸ La mayoría de la doctrina ha interpretado este calificativo como sinónimo de indubitado, exigiéndose que el interesado, valorada la información que se le ha facilitado sobre aspectos sustanciales

⁴⁶ Establece el art. 8 de la LORTAD que “Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento automatizado 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 los artículos 8, 10, 23 y 61 de la Ley 14/1986, de 25 de abril, General de Sanidad; 85.5, 96 y 98 de la Ley 25/1990, de 20 de diciembre, del Medicamento; 2, 3 y 4 de la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública, y demás Leyes sanitarias”.

⁴⁷ Art. 3, apartado “h” de la LOPD.

⁴⁸ La definición de “consentimiento” es prácticamente idéntica a la establecida en la Directiva 95/46/CE. Sin embargo, el calificativo de “inequívoco” es un añadido del legislador español.

del fichero y sobre sus derechos sobre los datos incorporados a él, manifieste, sin ningún género de dudas, su voluntad favorable al tratamiento.

Respecto al calificativo de “informada”, parece haber menos dudas. Desde luego, se está refiriendo a toda información que el interesado ha de recibir del Responsable del Fichero, muy bien señalada en el art 5 LOPD.

El consentimiento ha de ser en todo caso específico. Supone que se concrete sobre un objeto u objetos determinados, no siendo suficiente que la manifestación tenga un carácter genérico o indeterminado

Como punto de partida, debemos recurrir al Código Civil. El art. 1262 nos dice que el consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato. Por su parte, el art. 1265 del mismo Código, establece que será nulo el consentimiento prestado por error, violencia, intimidación o dolo. Podemos concluir que la validez del consentimiento vendrá marcada por la información previa sobre el objeto del mismo y la libertad de decisión de que debe gozar el sujeto que lo presta. Será necesario, ante todo y de una forma previa, que el interesado tenga la suficiente información acerca del tratamiento de datos de carácter personal que sobre su persona vaya a realizarse. Se considerará que la información dada al interesado no es suficiente si el mismo no ha recibido la información que viene señalada en el art. 5 LOPD.⁴⁹

⁴⁹ Establece dicho art.:

“Artículo 5. Derecho de información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se

La protección de datos sanitarios en el sector farmacéutico

Además, es obvio que el consentimiento ha de producirse y manifestarse sin coacción alguna. La voluntad de prestar dicho consentimiento ha de ser totalmente libre. En definitiva, cuando se cumplan todos los requisitos explicitados en el art. 3 apartado “h” de la LOPD, entenderemos que ese consentimiento, o esa voluntad de consentir, cumplen todas las exigencias.

Problema distinto es la forma elegida en la cual ese consentimiento se plasme.⁵⁰ No parece haber problemas para admitir el consentimiento tácito⁵¹ (pero en todo caso inequívoco, informado y sin coacción alguna –libre-) como regla general, siempre y

utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una Ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

⁵⁰Entre la jurisprudencia mas autorizada, se destaca:

“Como sostiene la doctrina más autorizada, las declaraciones de voluntad constitutivas de una negocio jurídico pueden ser expresas o tácitas; la declaración de voluntad es tácita cuando el sujeto no manifiesta de un modo directo su voluntad generalmente mediante el lenguaje verbal o escrito- sino que realiza una determinada conducta que , por presuponer necesariamente tal voluntad, es valorada por el Ordenamiento jurídico como declaración; se dice entonces que la voluntad se declara por medio de hechos concluyentes”. STS 22 de Febrero de 1990.

“Fuera de aquellos casos en que la Ley exige una declaración expresa, el consentimiento en los negocios jurídicos puede ser prestado en forma tácita; pero en todo caso la declaración de voluntad emitida indirectamente ha de resultar terminante, clara e inequívoca, sin que sea lícito deducirla de expresiones o actitudes de dudosa significación sino por el contrario reveladoras del designio de crear, modificar o extinguir algún derecho”. STS 8 de Febrero de 1964.

⁵¹ Salvo que exista una ley que disponga otra cosa (art. 6.1 LOPD).

cuando no estemos ante datos “especialmente protegidos”. Ello es así por el cuidado que ha tenido el legislador a la hora de diferenciar los distintos requerimientos del consentimiento. En efecto, si se precisara un consentimiento “reforzado” para todo tipo de datos, no encontraríamos las exigencias de “expreso” y “expreso y por escrito” que se requieren para los datos mas intrusivos.

Para estos últimos (a los que la ley los denomina “datos especialmente protegidos”) se requiere consentimiento expreso y/o por escrito en algunos casos.⁵²

Se ha planteado en reiteradas ocasiones a la AEPD lo que se debe entender por “consentimiento expreso”. Lo cierto es que la razón de la distinción entre “consentimiento expreso” y “consentimiento expreso y por escrito” no es muy clara. Y es que difícilmente se puede llegar a prestar un consentimiento expreso que no sea por escrito. El problema podría plantearse a la hora de probar por parte del Responsable del Fichero que el interesado manifestó dicho consentimiento cuando sus datos fueron recabados. Es doctrina reiterada de la AEPD y de nuestra jurisprudencia mas autorizada el señalar que es el Responsable del Fichero el que debe probar en todo caso que cumplió los extremos de la LOPD. Para el supuesto de tratarse de datos “especialmente protegidos”, la recomendación es que no se admitan distinciones. La mejor forma de probar que se obtuvo el consentimiento expreso es que el interesado lo manifieste por escrito. Aunque en puridad, cuando el interesado comunica informaciones de carácter personal a un profesional sanitario, es lógico pensar que en ese momento, y siempre que el profesional haya informado convenientemente –recordemos lo explicitado en el art. 5 LOPD-, el mismo está consintiendo expresamente al tratamiento de los datos referentes

⁵² Establecen los apartados 2 y 3 del art. 7 lo siguiente:

“7.2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

7.3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.”

a su persona. Otra cosa es que sea difícil de probar dicho consentimiento si no existe ningún documento que lo acredite. Pero no por ello se estaría infringiendo la LOPD.⁵³

Lo cierto es que si el legislador hubiera querido que los datos de salud se tuvieran que manifestar de forma escrita, lo hubiera encuadrado en el segundo grupo de datos “especialmente protegidos”. Al no ser así, debemos concluir que es posible manifestar el consentimiento de forma verbal para este tipo de datos. A pesar de lo dispuesto en el párrafo anterior a la hora de afrontar el momento de probar dicho consentimiento. Cuando el legislador excepcionalmente exige otra forma de manifestar el mismo lo señala expresamente.

3.2.2.- Excepciones recogidas en la LOPD a la hora de otorgar el consentimiento.

No siempre es necesario ese consentimiento expreso. La propia LOPD, en su art. 6.2 recoge ciertas excepciones que es preciso tener en cuenta.

En primer lugar, el consentimiento no es necesario “cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias”. Prevalece por tanto el interés de la administración, mas en concreto, sus necesidades de información.⁵⁴

Además, el consentimiento tampoco será necesario “cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento”. Lo cierto es que aunque sea una excepción, en la práctica es la regla general. Cualquier supuesto en el cual el interesado precise revelar datos de su salud se encuadrará dentro de una relación “negocial, laboral o administrativa”. La relación existente entre un médico y su paciente puede ser considerada como un “arrendamiento de servicios” o un “arrendamiento de

⁵³ A este razonamiento hay que añadir lo señalado en la C.E., concretamente en el art. 16.2: “Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.” De hecho, la LOPD establece en el mentado art. 7 que “cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo”

⁵⁴ Ello no significa que la administración pueda obtener todo tipo de datos de carácter personal sobre los individuos. Además, en todo caso la misma debe cumplir todos los requerimientos establecidos a la hora de otorgar el consentimiento del interesado, en especial lo relativo al art. 5 LOPD (deber de información).

obra”. En todo caso estamos ante una relación negocial. El problema es hasta qué punto se revelarán datos “no necesarios” para el cumplimiento de dicha relación. La indeterminación del precepto aquí es patente. En cualquier caso, es difícilmente imaginable una relación negocial en la que no se precise el tratamiento de datos de carácter personal.

El consentimiento seguirá sin ser necesario “cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley”. El mismo art. 7.6 establece igualmente que los datos referidos a la salud de las personas podrán ser tratados “cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto”. Aquí se plantea un choque de intereses para el paciente o interesado. Es lógico que debe prevalecer su vida antes que su intimidad en una situación de emergencia.⁵⁵

Respecto al supuesto del art. 7.6, hay que señalar, como expone VIZCAINO CALDERON que no se entiende muy bien qué tienen que ver los datos relativos a la afiliación sindical con la prevención de servicios sanitarios⁵⁶.

Por último, el consentimiento no se requiere si los datos han sido obtenidos de “fuentes accesibles al público”. No obstante, en todo caso el tratamiento ha de ser necesario “para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado”. Como se ve, el mero hecho de

⁵⁵ El Tribunal Constitucional ha señalado en reiteradas ocasiones que el “derecho a la vida” es superior al resto. En la STC de 11 de Abril de 1985 encontramos el siguiente párrafo:

“el derecho a la vida, reconocido y garantizado en su doble significación física y moral por el artículo 15 de la Constitución Española es la proyección de un valor superior del ordenamiento jurídico constitucional – la vida humana – y constituye el derecho fundamental esencial y troncal en cuanto es el supuesto ontológico sin el que los restantes derechos no tendrían existencia posible”.

⁵⁶ El mismo autor considera incluso la existencia de un error en la LOPD. También señala que no está clara la integración del origen racial que aparece en apartado 3 en el contexto de la prevención o diagnóstico del art. 7.6. “*Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*”, ed. Civitas, Madrid, 2001.

que los datos estén en una de estas fuentes no exime al Responsable del Fichero para cumplir con este precepto.

En la actualidad, la Oficina de Farmacia es considerada establecimiento sanitario y los profesionales farmacéuticos tienen la misma consideración. Al respecto, ley 16/97⁵⁷, de 25 de abril, de Regulación de Servicios de las Oficinas de Farmacia y 14/86⁵⁸, de 25 de abril, General de Sanidad, Ley de Bases de Sanidad Nacional, Ley 25/1990, de 20 de diciembre, del Medicamento y la Resolución del Comité de Ministros de 21 de Marzo de 2001, donde se afirma tajantemente que las “asociaciones farmacéuticas son profesionales sanitarios”.⁵⁹ Por si quedaba alguna duda, la Resolución de la AEPD con número de expediente E/0255/1998 de Abril de 1988 zanjaba el asunto en los siguientes términos:

“En lo que se refiere a las actuaciones que, en virtud del Concierto, deben realizar los Colegios Oficiales de Farmacéuticos en el profesorado de facturación de las recetas y de la grabación de los datos necesarios para el correcto control de la prestación farmacéutica, deben tenerse en cuenta las previsiones del art 97 de la Ley del Medicamento.

De dicho precepto, que regula la colaboración farmacias-Sistema Nacional de Salud, cabe destacar lo siguiente: la calificación de las Oficinas de Farmacia como establecimientos sanitarios, el deber de colaboración que se les impone para garantizar el uso racional de los medicamentos y la posibilidad de ser objeto de concertación en cuestiones distintas a las obligaciones legales, que se les imponen”.

Es claro que estamos ante profesionales sanitarios y establecimientos sanitarios, siendo aplicable el catálogo de excepciones anteriormente mencionado. Distinto sería

⁵⁷ En el art. 1 se recoge lo siguiente: “las oficinas de farmacia son establecimientos sanitarios privados de interés público o sujetos a la planificación sanitaria que establezcan las Comunidades Autónomas”

⁵⁸ Al respecto, el art. 103.2 establece que Las oficinas de farmacia abiertas al público se consideran establecimientos sanitarios a los efectos previstos en el Título IV de esta Ley.

⁵⁹ Al respecto, ver arts. 7.2, 7.3 y 7.6 de la LOPD. Así, si se le realiza un estudio farmacológico a un paciente y recabamos datos de salud, no tenemos que recabar el consentimiento expreso del mismo al estar dentro del radio de acción de esta excepción.

que existieran profesionales que no fueran farmacéuticos –esto es, profesionales sanitarios- que trataran y recabaran información que hiciera referencia a la salud de las personas (administrativos, auxiliares, personas en general carentes de la titulación requerida). Para estos profesionales no sanitarios resulta muy necesario la firma de cláusulas de confidencialidad donde exista un deber expreso y plasmado del secreto al cual deben someter los datos de carácter personal accedidos.⁶⁰

4.- La especialidad en el sector farmacéutico.

El tema central de este estudio es el régimen de los datos especialmente protegidos en el sector farmacéutico. Hasta ahora se ha esbozado muy brevemente el régimen de los datos sanitarios, y se ha hecho referencias al profesional farmacéutico en varias ocasiones, pero apenas se ha profundizado en ello. Es momento ahora para hacerlo. Pero para hacer un estudio lo suficientemente global, antes es necesario hacer una mención al régimen legal de los Colegios Profesionales.

El punto de partida lo encontramos, una vez más, en nuestra Constitución Española. El art. 36 establece que “...La ley regulará las peculiaridades propias del régimen jurídico de los Colegios Profesionales y el ejercicio de las profesiones tituladas. La estructura interna y el funcionamiento de los Colegios deberán ser democráticos.” Hoy es admitido en nuestra jurisprudencia mas autorizada el carácter de “administración corporativa” de los Colegios.⁶¹

⁶⁰ De hecho, el art. 10 LOPD impone un deber genérico de secreto al Responsable del Fichero:

”El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.”

⁶¹Se pronuncia en los siguientes términos la STC 10/1996: “La Constitución ha venido a admitir expresamente la legitimidad de la genéricamente llamada Administración corporativa, es decir, de las «corporaciones no territoriales», «corporaciones sectoriales de base privada» o «entes públicos asociativos», entendiéndose por tales, en términos generales, a diversas agrupaciones sociales, creadas por voluntad de la ley en función de diversos intereses sociales, fundamentalmente profesionales, dotadas frecuentemente de personalidad jurídico-pública, y acompañadas, también frecuentemente, del deber de afiliarse a las mismas. Así lo hace, ante todo, en su art. 36 respecto de los «Colegios Profesionales», como una de las manifestaciones más características de esta Administración corporativa. “

Es doctrina reiterada y asentada el carácter bifronte de los colegios profesionales, en el sentido en que los mismos realizan actividades de carácter público y privado. En el ámbito del derecho público, sus acciones son verdaderos actos administrativos, sometidos, como no podía ser de otra forma, al régimen jurídico administrativo y revisables ante la jurisdicción contencioso-administrativa⁶². Ello influye en la consideración de los ficheros de carácter personal de los que sean responsables.⁶³

Por otro lado, es necesario precisar que el modelo de servicio que ofrece el Sistema Nacional de Salud Español habilita el intercambio de información entre diferentes Administraciones (central, autonómica y local). Se ha expuesto en reiteradas ocasiones que cada vez mas, el usuario del sistema quiere recibir servicios de calidad, sin importarle qué administración se los proporciona.⁶⁴ Ello viene acentuado por la creciente movilidad de los ciudadanos.

4.1.- La especialidad en los colegios oficiales de farmacéuticos.

Se pretende en este punto analizar algunos aspectos muy concretos que versan sobre el tratamiento de los datos de carácter personal que realizan los colegios profesionales de farmacéuticos, como verdaderos garantes y “Responsables de Ficheros” no solo de colegiados, sino también de información relativa a recetas, facturación, etc. Hay que señalar que en todos los casos estas instituciones son depositarias de información sensible o “especialmente protegida”. Conviven en los mismos, como en todos los colegios, la doble vertiente de personalidad privada y pública respecto de muchos de sus ficheros, y además, y a diferencia de otros colegios

⁶² La STS de 26 de Noviembre de 1998 se pronuncia en los siguientes términos:

“Los Colegios Profesionales desarrollan, a la par, una serie de actividades propias de un ámbito de derecho público, de servicio público e interés general, y otras de orden privado restringidas a su relación interna con los integrantes de las corporaciones y que carecen de toda eficacia externa o pública.”

“En los temas que versen, entre otros, sobre defensa de la corporación, constitución de sus órganos, régimen electoral, decisiones sobre colegiación y disciplina, por su evidente matiz de derecho público, están sujetos al control jurisdiccional del orden contencioso administrativo.”

⁶³ El Tribunal Constitucional en reiteradas ocasiones ha puesto de manifiesto este carácter bifronte.

⁶⁴ Entre otros, MUÑOZ MONTALBO, lo estudia en el artículo “*La Protección de Datos Personales en el Sistema Nacional de Salud*”, en www.alaroavant.com

profesionales, la existencia de informaciones que hacen referencia a la salud de las personas.

Los Colegios Profesionales se crean por Ley de las comunidades Autónomas. Por su parte, los Consejos Generales lo hacen por Ley de las Cortes Generales.⁶⁵ Los poderes públicos atribuyen a estas entidades el cumplimiento de funciones públicas a la hora de regular, promover y limitar el acceso a unas determinadas profesiones. Pero también los colegios son meras asociaciones de particulares con objetivos privados o corporativos.

4.1.1.- Ficheros privados y públicos.

Si los Colegios Profesionales tienen ese carácter bifronte, los mismos tendrán ficheros de dos naturalezas distintas. Así, los ficheros deben ser considerados de naturaleza pública cuando éstos sean creados para el ejercicio de potestades públicas, es decir, cuando sirvan para el desarrollo de una actividad administrativa, sometida al derecho administrativo. Además, como ya se esbozaba al principio, los colegios ejercerán también funciones privadas, por ejemplo, de mera ordenación de sus bienes, contratación de personal, contabilidad, etc. Los ficheros generados de estas funciones privadas tendrán la consideración de ficheros privados.⁶⁶

⁶⁵Encontramos en la Ley de Colegios Profesionales 2/1974 de 13 de febrero (art. 1): “Los Colegios Profesionales son Corporaciones de Derecho Público amparadas por la Ley y reconocidas por el Estado, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines”.

⁶⁶Se tiende a confundir la consideración de “fichero público” con el concepto de “fichero de acceso público”, en referencia a las “fuentes accesibles al público” reguladas y definidas en el art. 3 de la LOPD. Sin embargo, son aspectos totalmente distintos. “Fuente Accesible al Público” hace referencia a aquellos “ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.”. Un fichero de carácter público implica que ha sido elaborado por un órgano administrativo en el ejercicio de sus competencias de derecho público, pero no por ello tiene porqué ser un fichero “cuya consulta pueda ser realizada por cualquier persona...”.

Otra cosa es que, en determinados ficheros, por ejemplo el fichero colegiados, confluyan al mismo tiempo la consideración de “Fuente Accesible al Público” y “Fichero Público”. Pero en otros ficheros, por ejemplo en el caso de los Colegios Oficiales de Farmacéuticos, el fichero “Facturación de Recetas”, no existe esa consideración de “Fuente Accesible al Público”.

La protección de datos sanitarios en el sector farmacéutico

Es básico por tanto esta diferencia. Siguiendo el criterio de la AEPD, los ficheros públicos más usuales en un Colegio Oficial de Farmacéuticos son los siguientes:

-Fichero “colegiados”. Ello es así porque una de las facultades públicas o administrativas de los colegios es la ordenación y el control del acceso a la profesión.

-Fichero “deontología profesional”. Ello es así porque una de las facultades públicas o administrativas de los colegios es, en todo caso, y al hilo de lo anterior, la regulación de la profesión. Pero también, en este caso, la colaboración con la justicia, por la que en muchas ocasiones, datos relativos a la deontología profesional se hacen necesarios.

-Fichero “peritos”. Ello es así porque, al igual que el fichero anterior, una de las potestades públicas de los colegios será en todo caso la colaboración con la justicia.

-Fichero “Recetas” y/o “Facturación de Recetas”. Se estudia en el apartado siguiente.

En otra tipología de Colegios Profesionales podemos encontrar ficheros públicos tales como “Justicia gratuita”, muy propio en Colegios de Abogados. No es objeto del presente trabajo.

Como tampoco lo es hacer la distinción entre “ficheros manuales” y “ficheros automatizados”. Si bien es cierto que los segundos están sometidos a un plazo de carencia que culmina el 24 de Octubre del año 2007, ello no es así para los ficheros preexistentes, especialmente si estos últimos recogen mas información que los propios ficheros automatizados y realizan otras funciones, y por ello otros tratamientos. En todo caso, hay que señalar que todos los ficheros, independientemente de su condición manual o automatizada, habrán de respetar los derechos de acceso, cancelación y rectificación por parte de los afectados.

4.1.2.- Los datos de facturación de los Colegios Oficiales de Farmacéuticos.

La protección de datos sanitarios en el sector farmacéutico

Estamos ante un caso especial que requiere su estudio. La AEPD se ha pronunciado ante diversas cuestiones realizadas por varios Colegios Oficiales de Farmacéuticos. La cuestión a dirimir es si los Colegios y/o el Consejo General han de ser considerados Responsables de los Ficheros, y a la vez, ver la naturaleza de los mismos.⁶⁷ La respuesta es afirmativa, siendo los mismos responsables de los ficheros relacionados con los datos de facturación, proveniente todos ellos de las Oficinas de Farmacia. El tratamiento se encuentra en todo caso amparado en lo dispuesto en el art. 5 de la Ley de Colegios Profesionales.⁶⁸ Las razones para esta consideración son las siguientes:

⁶⁷ Respondiendo a la segunda pregunta, el estudio al que se hace referencia concluye de una forma tajante: el fichero “facturación de recetas” tendrá en todo caso la condición de fichero de titularidad pública, no siendo posible la notificación del mismo como fichero de titularidad privada, debiendo adoptarse la correspondiente disposición de carácter general por el órgano de gobierno del correspondiente Colegio Oficial de Farmacéuticos o por el Consejo General, tal y como establece el art. 20 de la LOPD.

⁶⁸ El extenso art. 5 de la Ley 3/74, de Colegios Profesionales, se pronuncia en los siguientes términos:

“Corresponde a los Colegios Profesionales el ejercicio de las siguientes funciones, en su ámbito territorial:

- a. Servir de vía de participación orgánica en las tareas de interés general. de acuerdo con las leyes.
- b. Ejercer cuantas funciones les sean encomendadas por la Administración y colaborar con ésta mediante la realización de estudios, emisión de informes, elaboración de estadísticas y otras actividades relacionadas con sus fines que puedan serles solicitadas o acuerden formular por propia iniciativa.
- c. Ostentar la representación que establezcan las leyes para el cumplimiento de sus fines.
- d. Participar en los Consejos u Organismos consultivos de la Administración en la materia de competencia de cada una de las profesiones.
- e. Estar representados en los Patronatos Universitarios.
- f. Participar en la elaboración de los planes de estudio e informar las normas de organización de los Centros docentes correspondientes a las profesiones respectivas y mantener permanente contacto con los mismos y preparar la información necesaria para facilitar el acceso a la vida profesional de los nuevos profesionales.
- g. Ostentar en su ámbito la representación y defensa de la profesión ante la Administración, Instituciones, Tribunales, Entidades y particulares, con legitimación para ser parte en cuantos litigios afecten a los intereses profesionales y ejercitar el derecho de petición, conforme a la Ley, sin perjuicio de lo dispuesto en el apartado 3 del artículo 1 de esta Ley.
- h. Facilitar a los Tribunales, conforme a las leyes, la relación de colegiados que pudieran ser requeridos para intervenir como peritos en los asuntos judiciales, o designarlos por si mismos, según proceda.
- i. Ordenar en el ámbito de su competencia la actividad profesional de los colegiados, velando por la ética y dignidad profesional y por el respeto debido a los derechos de los particulares y ejercer la facultad disciplinaria en el orden profesional y colegial.

La protección de datos sanitarios en el sector farmacéutico

-Los Colegios Oficiales de Farmacéuticos tienen un determinado poder de decisión sobre el fichero “facturación”. Ello es imprescindible para ser considerados “Responsables de Ficheros”, ya que, por definición, el mismo es aquella “Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”. Si fueran meros vínculos de transmisión entre las Oficinas de Farmacia y la Administración Sanitaria, podríamos buscarle un encuadre mas correcto dentro de la figura del “encargado de tratamiento”.⁶⁹

j. Organizar actividades y servicios comunes de interés para los colegiados, de carácter profesional, formativo, cultural, asistencial y de previsión y otros análogos, proveyendo al sostenimiento económico mediante los medios necesarios.

k. Procurar la armonía y colaboración entre los colegiados, impidiendo la competencia desleal entre los mismos.

l. Adoptar las medidas conducentes a evitar el intrusismo profesional.

m. Intervenir, en vía de conciliación o arbitraje, en las cuestiones que, por motivos profesionales, se susciten entre los colegiados.

n. Resolver por laudo, a instancia de las partes interesadas, las discrepancias que puedan surgir sobre el cumplimiento de las obligaciones dimanantes de los trabajos realizados por los colegiados en el ejercicio de la profesión.

ñ. Establecer baremos de honorarios, que tendrán carácter meramente orientativo.

o. Informar en los procedimientos judiciales o administrativos en que se discutan honorarios profesionales.

p. Encargarse del cobro de las percepciones, remuneraciones u honorarios profesionales cuando el colegiado lo solicite libre y expresamente, en los casos en que el Colegio tenga creados los servicios adecuados y en las condiciones que se determinen en los Estatutos de cada Colegio.

q. Visar los trabajos profesionales de los colegiados, cuando así se establezcan expresamente en los Estatutos generales. El visado no, comprenderá los honorarios ni las demás condiciones contractuales cuya determinación se deja al libre acuerdo de las partes.

r. Organizar, en su caso, cursos para la formación profesional de los postgraduados.

s. Facilitar la solución de los problemas de vivienda de los colegiados, a cuyo efecto, participarán en los Patronatos oficiales que para cada profesión cree el Ministerio de Vivienda.

t. Cumplir y hacer cumplir a los colegiados las Leyes generales y especiales y los Estatutos profesionales y Reglamentos de Régimen Interior, así como las normas y decisiones adoptadas por los Órganos colegiales, en materia de su competencia.

u. Cuantas otras funciones redunden en beneficio de los intereses profesionales de los colegiados.”

Parece ser el apartado “b” en el cual se encuentra la legitimidad de los Colegios Oficiales de Farmacéuticos para el tratamiento del fichero “facturación de recetas”. Y es que es imprescindible que los mismos colaboren con el Sistema Nacional de Salud.

⁶⁹ Establece el art. 12 de la LOPD.:

“1. 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.

La protección de datos sanitarios en el sector farmacéutico

-Las Oficinas de Farmacia están obligadas a colaborar con los Sistemas Autonómicos de Salud.⁷⁰ Esta colaboración se canaliza a través de los Colegios Oficiales y, en su caso, a través del Consejo General. La Ley 16/2003 reserva en exclusiva al estado determinadas competencias encaminadas a determinar qué medicamentos serán financiados por el Sistema Nacional de Salud y cuál será el precio de los mismos.⁷¹ Es por ello por lo que para la determinación de los precios, será preciso que la Administración General del Estado tenga conocimiento de la información referida al

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.”

⁷⁰ En los siguientes términos se pronuncia la STS del 7 de Octubre de 2003:

“En todo caso, la dispensación de medicamentos para su aplicación fuera de las Instituciones a que se refiere el número anterior se efectuará a través de las oficinas de farmacia legalmente establecidas, que estarán obligadas a efectuar tal dispensación”

La Ley 25/1990, del Medicamento, establece que:

“Con independencia de las obligaciones establecidas en esta Ley y las que reglamentariamente se determinen, las oficinas de farmacia, podrán ser objeto de concertación en el Sistema Nacional de Salud, de acuerdo con el Sistema General de Contratación Administrativa y conforme a los criterios generales a que se refiere el art. 93.3”

Por último, la Ley 16/2003, de 28 de Mayo, de Cohesión y Calidad del Sistema Nacional de Salud, establece en su art. 33.2 lo siguiente:

“...se establecerán los criterios generales y comunes para el desarrollo de la colaboración de las oficinas de farmacia, por medio de conciertos que garanticen a los ciudadanos la dispensación en condiciones de igualdad efectiva en todo el territorio nacional, independientemente de su Comunidad Autónoma de residencia...”

⁷¹ Establece el art. 30 de la Ley 16/2003:

“Corresponde al Ministerio de Sanidad y Consumo el ejercicio de las competencias del Estado en materia de evaluación, registro, autorización, vigilancia y control de los medicamentos de uso humano y veterinario y de los productos sanitarios, así como la decisión sobre su financiación pública y la fijación del precio correspondiente, en los términos previstos en la Ley 25/1990, de 20 de diciembre, del Medicamento, sin perjuicio de las competencias ejecutivas de las comunidades autónomas”

La protección de datos sanitarios en el sector farmacéutico

gasto farmacéutico. Esta información es suministrada a través de las Oficinas de Farmacia, a través de los Colegios Oficiales de Farmacéuticos.⁷²

4.1.3.- El carácter de “fuente accesible al público” de algunos ficheros.

Existe una categoría especial de datos, los considerados como “fuente accesible al público”. La Ley 15/99, de Protección de Datos de Carácter Personal (en adelante LOPD), contiene una regulación específica de los mismos, entre los que sitúa los listados de personas pertenecientes a grupos profesionales. En el art. 3.j) de la citada norma, encontramos la siguiente definición:

“Fuente accesible al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.”

La calificación de un fichero como fuente accesible al público permite que estos datos sean recabados, utilizados y cedidos a terceras personas, sin necesidad del consentimiento de las personas titulares de los datos (interesados).

En los Colegios Profesionales uno de los ficheros considerados como “públicos” y al mismo tiempo “Fuente Accesible al Público” es el fichero “colegiados”. De este fichero se suele obtener el listado de colegiados. Es necesario señalar que los listados de personas pertenecientes a grupos profesionales no se pueden considerar siempre “fuente accesible al público”. En primero lugar el art. 28.3 señala que “...las fuentes de acceso

⁷² El art. 98 de la mencionada Ley 25/1990, del Medicamento, establece que “la información agregada resultante del procesamiento de las recetas del Sistema Nacional de Salud es de dominio público, salvando siempre la confidencialidad de la asistencia sanitaria y de los datos comerciales de empresas individualizadas, así como el secreto estadístico. Su gestión corresponde a los Servicios de Salud de las Comunidades Autónomas en su ámbito territorial y al Estado en la información agregada del conjunto del Sistema Nacional de Salud”.

público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique. En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención”⁷³.

Por otro lado, no todos los datos son considerados de tal forma (esto es, Fuente Accesible al Público). Las listas de personas pertenecientes a grupos profesionales son los descritos en el art. 3.j) de la LOPD. Así, las listas de personas pertenecientes a grupos de profesionales deben contener “únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo”. Este sería el tratamiento de datos en los listados de grupos profesionales que sería respetuoso con el principio de calidad –art. 4 LOPD-. En consecuencia, datos como el teléfono (profesional o de otra índole) no es considerado fuente accesible al público. Ello es congruente con lo especificado en el art. 28 de la LOPD.:

“...los datos personales que figuren en el censo promocional o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3 j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento...”.

Se está señalando expresamente que si los Colegios Profesionales desean incluir otros datos adicionales –p.ej., teléfono- a los enumerados en el art. 3.j) de la LOPD, deberán contar con el consentimiento del colegiado, el cual podrá ser revocado en cualquier momento.

⁷³ Este precepto es congruente con lo establecido en la Ley 44/2003, de 21 de Noviembre, de Ordenación de las Profesiones Sanitarias, texto que establece dentro de los principios generales de la relación entre los profesionales sanitarios y las personas atendidas por ellos que:

“...los colegios profesionales, consejos autonómicos y consejos generales, en sus respectivos ámbitos territoriales, establecerán los registros públicos de profesionales que, de acuerdo con los requerimientos de esta Ley, serán accesibles a la población y estarán a disposición de las Administraciones sanitarias. Los indicados registros, respetando los principios de confidencialidad de los datos personales contenidos en la normativa de aplicación, deberán permitir conocer el nombre, titulación, especialidad, lugar de ejercicio y los otros datos que en esta Ley se determinan como públicos”

La protección de datos sanitarios en el sector farmacéutico

Consecuencia de ello es que los datos contenidos en las guías profesionales pueden ser consultados por cualquier persona, no impedida por una norma limitativa con la sola exigencia, en su caso, del abono de una contraprestación. De hecho, el art. 30 de la LOPD, relativo a los tratamientos con fines de publicidad y prospección comercial, permite a quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades utilizar los nombres, direcciones y otros datos de carácter personal de quienes figuren en fuentes accesibles al público.

Sin embargo, el interesado siempre puede anticiparse y oponerse a este tratamiento. El art. 28.2 de la LOPD establece que los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios Profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial. Incluso se establece un plazo –diez días- por el que el Colegio deberá de hacer efectiva la no inclusión del colegiado en el listado a efectos de publicidad. Si el colegiado no se opone expresamente al tratamiento de datos para fines de publicidad, el cesionario de los datos –esto es, empresa que ha recibido el listado del Colegio y realiza el envío publicitario- deberá informar al colegiado en cada comunicación que le dirija cuál es el origen de los datos y la identidad del responsable del tratamiento, así como los derechos que le asisten (art. 30.2 LOPD).

En consecuencia de todo lo anteriormente señalado, el Colegio debería tomar algunas precauciones a la hora de ceder el listado de colegiados, ello a pesar de tener la consideración de “Fuente Accesible al Público”:

-El listado a ceder sólo deberá contener los datos contenidos en el art. 3.j), esto es: nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. En ningún caso es recomendable ceder el dato “teléfono” u otras informaciones. Si el Colegio se planteara ceder mas datos que los anteriormente citados, se debería recabar el consentimiento del colegiado (es por ello que parte de la documentación entregada en el dossier incide en estos aspectos). Sin embargo, después de haber revisado muchos expedientes de la Agencia de Protección de Datos que hacen referencia a Colegios Profesionales, la recomendación es que se extremen las

La protección de datos sanitarios en el sector farmacéutico

precauciones en este aspecto. La cesión ilícita de datos lleva aparejada una sanción que oscila entre los 300.000 y 600.000 €(art. 44.4 LOPD).

-Es muy recomendable ceder datos a terceros después del compromiso por escrito de la empresa cesionaria. Ello puede evitar problemas futuros.

-En todo caso, el Colegio tiene la obligación de informar a los colegiados. El envío de comunicaciones, cláusulas en los formularios de recogida de datos y/o documentos explicativos a la vista del público hacen cumplir con este precepto. En todo caso el colegiado puede oponerse al envío de comunicaciones comerciales de terceros.

-El Colegio debe facilitar en todo caso el ejercicio de los derechos de acceso, cancelación, rectificación y oposición a los colegiados. A pesar de que la Ley no lo exige, es muy recomendable que los Colegio tengan formularios preparados para el ejercicio de estos derechos, que añada cláusulas en los formularios de recogidas de datos donde se haga referencia a ello y que todo el personal administrativo conozca el procedimiento a seguir en el caso de que algún colegiado ejercite sus derechos en esta materia. La Instrucción de la AEPD que hace referencia (Instrucción 1/98) a ello es taxativa: el Responsable del Fichero está obligado a conocer el procedimiento a seguir en el caso de que se ejercite este derecho. Si por alguna razón se produjera una cesión ilícita de datos, el Colegio siempre podrá alegar en el correspondiente expediente abierto por la AEPD que el colegiado siempre pudo ejercitar su derecho de cancelación y oposición a recibir publicidad de terceros, y que el Responsable del Fichero cumplía con todas las obligaciones en este aspecto.

-Finalmente resulta interesante la firma de convenios de colaboración donde se haga referencia a la protección de datos de carácter personal y, en todo caso, extremar las precauciones con las empresas que ofrecen bienes y servicios que no guardan relación con la actividad del colegiado.

4.1.4.- Otros aspectos.

La protección de datos sanitarios en el sector farmacéutico

La especialidad de muchos de los ficheros de los Colegios Profesionales no acaba aquí. A la hora de registrar los considerados “ficheros públicos”, es necesario seguir unos trámites distintos al procedimiento seguido para los privados.

En relación a los ficheros de carácter público, según el art. 20.1 de la Ley 15/99, “la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o diario oficial correspondiente”. En todo caso, las disposiciones de creación o de modificación de ficheros deberán indicar, la finalidad del fichero y los usos previstos para el mismo, las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos de carácter personal, la estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo, las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros, los órganos de las Administraciones responsables del fichero, los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición y las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

Dada la especialidad de los ficheros, es recomendable que la disposición de creación del fichero se someta a dictamen jurídico favorable por parte de la AEPD. El procedimiento a seguir sería el siguiente:

-Acuerdo de creación del fichero de datos de carácter personal de titularidad pública correspondiente adoptado por el órgano Colegial que en virtud del correspondiente Estatuto tenga capacidad para ello (Junta General, Junta de Gobierno, etc...).

-El Acuerdo en todo caso debe ajustar su contenido a lo dispuesto en el art. 20 de la LOPD y disposiciones de desarrollo, en particular al RMS.

-El Acuerdo ha de someterse a informe preceptivo favorable de la AEPD, con carácter previo a su publicación en el Boletín o Diario Oficial correspondiente.

-Una vez publicado en el Boletín o Diario Oficial el Acuerdo de creación, modificación o supresión del fichero correspondiente, se dará traslado del mismo, conforme a lo dispuesto en el art. 39.2 de la LOPD y el R.D. 1332/1994, de 20 de Junio, a la AEPD. Se procederá a completar los modelos normalizados preparados al efecto⁷⁴. Se acompañará copia del Boletín o Diario Oficial correspondiente donde se publica el Acuerdo.

4.2.- La especialidad en la Oficina de Farmacia.

Si hay un establecimiento sanitario donde se producen una gran cantidad de tratamientos de datos de carácter personal es en las Oficinas de Farmacia. Los profesionales farmacéuticos realizan actividades sanitarias tales como dispensación de medicamentos, atención farmacéutica, elaboración de fórmulas magistrales, realización de análisis clínicos, pueden vender productos ortopédicos, realizar dietas personalizadas, están obligados a reflejar en libros oficiales la dispensación de ciertos medicamentos (libro de contabilidad de estupefacientes), colaboran con los Servicios Autonómicos de Salud y ceden datos relativos a la facturación a sus colegios respectivos. En la mayoría de los casos todos estos tratamientos están permitidos –es mas, son obligados- por las correspondientes leyes sanitarias, bien estatales o autonómicas. Sin embargo, ello no está exento de problemas. Sobre los mismos se va a intentar profundizar en este apartado. En la mayoría de los casos, y gracias al avance de las Tecnologías de la Información y Comunicación (TIC), todas las Oficinas de Farmacia se han informatizado. Ello conlleva el tratamiento de datos de carácter personal de forma automatizada en la mayoría de los casos. En otros, el tratamiento es solo en papel (libro recetario oficial y/o libro de contabilidad de estupefacientes), pero por el grado de sensibilidad de los datos tratados es muy conveniente que los Responsables de Ficheros adopten todas las precauciones precisas.

El ámbito geográfico específico es el de la Región de Castilla La Mancha. La legislación autonómica al respecto la encontramos en la Ley 4/1996, de 26 de diciembre de 1996, de Ordenación del Servicio Farmacéutico de Castilla-La Mancha. Lo más destacable de la norma es el encuadramiento, una vez más, de la Oficina de Farmacia

⁷⁴ Resolución de 30 de mayo de 2000, de la AEPD, por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático, para la inscripción de los ficheros.

La protección de datos sanitarios en el sector farmacéutico

como un “establecimiento sanitario de interés público autorizado, en el que, bajo la dirección de un farmacéutico”, donde se realizan algunas funciones sanitarias.⁷⁵ Esta Ley ha sido modificada por la 4/1998 y 10/2000.

4.2.1.- La receta electrónica: el caso de Castilla La Mancha.

Se ha considerado que la implantación del visado electrónico es el primer paso para la llegada de la receta electrónica.

Castilla-La Mancha se convirtió el 1 de Junio de 2003 en la primera comunidad autónoma en visar sus medicamentos en las propias Oficinas de Farmacia. La experiencia piloto se desarrolló en primer lugar en Toledo a través de un concierto entre el Servicio de Salud de Castilla-La Mancha (SESCAM) y los cinco Colegios Oficiales de Farmacéuticos provinciales.

⁷⁵ Entre ellas:

“a) La adquisición, conservación, custodia y dispensación de medicamentos y productos sanitarios y de aquellos otros utensilios y productos de carácter sanitario que se utilicen para la aplicación de los anteriores, o de utilización o carácter tradicionalmente farmacéutico.

b) La elaboración y dispensación de fórmulas magistrales y preparados oficinales de acuerdo con los procedimientos y controles de calidad establecidos.

c) La colaboración en el control del uso individualizado de los medicamentos, a fin de detectar las reacciones adversas que puedan producirse y notificarlas a los organismos responsables de la farmacovigilancia.

d) La colaboración en los programas sanitarios que promueva la Administración sanitaria y en concreto en los establecidos en los artículos 10 y 11 de esta Ley.

e) Actuar coordinadamente, a nivel de las áreas y zonas básicas de salud y colaborar con la atención especializada para garantizar un uso racional del medicamento.

f) Dar consejo farmacéutico a los usuarios.

g) Elaboración de historias farmacoterapéuticas de los usuarios, seguimiento de tratamientos e información sobre la medicación a los mismos.

h) Control de recetas dispensadas y custodia de las mismas, así como de documentos sanitarios.

i) En las oficinas de farmacia se podrán asimismo realizar aquellas otras funciones profesionales o sanitarias que tradicionalmente o por estar contempladas en normas específicas pueda desarrollar el farmacéutico, de acuerdo con su titulación y especialidad.”

La protección de datos sanitarios en el sector farmacéutico

El funcionamiento es muy sencillo, haciéndose uso de las Tecnologías de la Información y Comunicación. El paciente solo tiene que ir una vez a sus servicios de inspección. Para una prolongación en el tiempo en el suministro del fármaco se podrá recurrir al fármaco, que consultará a través de la red, en una macro-base de datos preparada al efecto, si el paciente efectivamente tiene derecho a la prestación.

Así, el paciente tiene diez días para ir a la Oficina de Farmacia con su receta e, introduciendo el número de asegurado o el NIF, fármaco o dolencia en el programa informático, el profesional farmacéutico accederá a una base de datos en la que figura la información necesaria para saber si a ese paciente le corresponde el fármaco de la prescripción. El paciente ahorra tiempo y desplazamientos y el profesional farmacéutico se convierte en un agente de salud más activo. Para poder poner en marcha el sistema, los técnicos y el personal del SESCAM han introducido los informes médicos y las recetas en esa base de datos a la que anteriormente se hacía referencia.

La transmisión de datos a través de las redes de telecomunicaciones de los pacientes (datos personales que vienen contenidos en las recetas y que son considerados de nivel alto, ya que vienen acompañadas del fármaco a dispensar) deberá, en todo caso, de respetar la normativa de protección de datos. Así se establece claramente en preceptos como el art. 5.4 del concierto regulador:

“Al objeto de garantizar la confidencialidad de los datos de carácter personal y el cumplimiento de lo dispuesto en la LOPD, la Organización Farmacéutica Colegial solamente podrá disponer y utilizar la información procedente de la mecanización de las recetas del Sistema Nacional de Salud para dar cumplimiento a las condiciones de facturación de las recetas que se establecen en el Anexo F. Cualquier otro uso deber ser autorizado por el SESCAM. Las empresas susceptibles de ser contratadas o concertadas por los Colegios Oficiales de Farmacéuticos para la grabación de los datos contenidos en las recetas, tienen expresamente prohibido cualquier uso de estos datos, excepto los de su entre a los Colegios Oficiales de Farmacéuticos”.

Todo lo expuesto es congruente con, entre otros, el “Principio de Calidad” de los datos (art. 4 LOPD) y la “Prohibición de acceso a terceros” (art. 11 LOPD). Del mismo modo, se deja abierta la posibilidad de la contratación por parte de empresas que

realicen las tareas de mecanización de las recetas para los colegios. Ello se correspondería en todo caso con un acceso a datos de carácter personal, regulada en el art. 12 LOPD.⁷⁶ Hay que decir que la contratación de empresas para la realización de estas tareas es muy usual. Desgraciadamente, no lo es tanto la firma del correspondiente “contrato de encargado de tratamiento” donde se especifique claramente lo dispuesto en el art. 12 LOPD. Ello supone una vulneración de la normativa vigente que tiene una importancia adicional, por el grado de sensibilidad de los datos tratados.

Llama la atención el que no se haga referencia al RMS. Los datos de los pacientes son enviados y “visados” de forma electrónica con el uso de las TIC y las redes de telecomunicaciones. El art. 26 del RMS establece que:

“La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.”

En el Concierto no se habla en ningún momento de las medidas de seguridad que se deberán de implantar, lo cual es criticable. El uso de la criptografía asimétrica u otros sistemas que garanticen la confidencialidad de la información gracias al cifrado se hace

⁷⁶ Establece el art. 12 LOPD.:

Artículo 12. Acceso a los datos por cuenta de terceros.

1. 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.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente

La protección de datos sanitarios en el sector farmacéutico

imprescindible y obligatoria. A nadie escapa los peligros que entraña en la actualidad el uso de las TICs en conjunción con las redes públicas de telecomunicaciones (Internet).

4.2.2.- La cesión de datos para la elaboración de fórmulas magistrales. El caso de Castilla La Mancha.

La elaboración de fórmulas magistrales por parte de profesionales sanitarios en las Oficinas de Farmacia ha sido, tradicionalmente, uno de los servicios sanitarios más característicos por parte de estos profesionales.

El procedimiento para la realización de fórmulas se encuentra muy regulado, y sometido a unas altas exigencias tanto de gestión como de control del proceso de formulación. Al respecto, y como legislación nacional, hay que destacar el Real Decreto 175/2001, de 23 de febrero, por el que se aprueban las normas de correcta elaboración y control de calidad de fórmulas magistrales y preparados oficinales. El 1 de Enero del 2004 acabó el plazo de carencia establecido en la norma. En la misma se hace referencia a los distintos procesos, normas y estándares que los farmacéuticos deberán seguir en lo referente a personal, utillaje, documentación, materias primas y material de acondicionamiento así como su elaboración y dispensación. En la norma, si bien no se hace referencia a la LOPD, si encontramos preceptos encaminados a garantizar la seguridad de los datos a tratar, dada la confidencialidad de los mismos:

-En el párrafo 2.2.4, se establece que “Los aparatos de medida han de ser controlados y calibrados periódicamente para asegurar la exactitud de los datos leídos o registrados. Se deben conservar los resultados de estos controles periódicos. Antes de iniciar cualquier operación, se recomienda efectuar una verificación de los aparatos de medida que lo precisen, especialmente las balanzas”. Ello es congruente con el art. 4 LOPD, en lo referente al principio de calidad de los datos.

-En el capítulo 3, al referirse a la documentación de registro necesaria para la elaboración magistral, se establece que “la documentación constituye una parte fundamental del sistema de garantía de calidad de los medicamentos preparados en la Oficina de Farmacia o servicio farmacéutico, evitando los errores inherentes a la comunicación oral o derivados de operar con datos retenidos en la memoria y

permitiendo, al finalizar las operaciones, la reconstrucción histórica de cada preparación. Los documentos deben ser elaborados, fechados y firmados por el farmacéutico. En el caso de tratarse de una Oficina de Farmacia o servicio farmacéutico con más de un farmacéutico, podrán ser elaborados por cualquiera de ellos, pero tendrán que ser ratificados por el farmacéutico responsable del mismo, puestos al día periódicamente y, si fuese necesario introducir modificaciones, éstas también estarán fechadas y firmadas por el farmacéutico. La documentación fuera de uso ha de ser retirada para evitar confusiones. Los documentos tendrán un título que exprese claramente su objetivo y contenido y deberán estar escritos de forma que sean perfectamente legibles. Los documentos se redactarán de forma clara y concisa, debiendo ser fácilmente comprensibles por el personal que los va a manejar y estar en todo momento a su disposición. Toda la documentación se archivará y conservará hasta, al menos, un año después de la fecha de caducidad sin perjuicio de aquellos casos regulados por normativa específica.” Se intenta en todo caso garantizar la verosimilitud de la información tratada. No se conservará por mas tiempo del necesario. Todo ello es congruente, una vez más, con el Principio de Calidad del anteriormente mencionado art. 4 de la LOPD.

-El texto propone en sus respectivos anexos unas fichas que han de completarse en el proceso de elaboración de la fórmula. En dichas fichas existen campos para recoger la identificación de los profesionales que han participado en la elaboración. Así mismo, existe la posibilidad de que el profesional recoja datos de carácter personal referidos al paciente (en diversos campos no específicos, como el de “observaciones”). Lo cierto es que no se observa la preceptiva cláusula de información que establece el art 5 LOPD, incumpliendo por ello el “Deber de Información” en la recogida de datos.

Tres meses después de la entrada en vigor del RD 175/2001, Castilla-La Mancha se convirtió en la novena autonomía que aprobaba oficialmente la norma que desarrolla las exigencias específicas para sus farmacias y servicios de hospital.

El documento reproduce prácticamente por completo el borrador y confirma que, "con objeto de garantizar el control de elaboración por terceros", estas solicitudes de fórmulas "deberán realizarse entre oficinas y servicios de la propia autonomía", salvo casos en los que allí "no exista ninguna farmacia ni servicio autorizado para elaborar a

terceros en el nivel al que corresponda la preparación". Entre las normas publicadas hasta la fecha, esta limitación se incluye también en Extremadura y La Rioja.

Por lo demás, el texto fija cuatro niveles de elaboración con el mínimo en el etiquetado y dispensación de fórmulas de terceros y prevé la publicación de un censo anual de Oficinas de Farmacia y hospitales por niveles.

Es de destacar la previsión que la norma realiza para aquellos profesionales farmacéuticos que no tengan el nivel necesario para la elaboración de las fórmulas. El texto prevé la posibilidad de que exista un contrato entre profesionales farmacéuticos para la elaboración de las mismas. Ello está regulado en el art. 5 de la Orden:

“Artículo 5.- Elaboración por terceros

1.- Las Oficina de Farmacia y servicios farmacéuticos adscritos a un determinado nivel, en caso de tener que dispensar una fórmula magistral o preparado oficial correspondiente a niveles superiores al que están adscritos o que, excepcionalmente, no puedan realizar todas las fases de la elaboración de una fórmula magistral o preparado oficial de su nivel, deberán encargar la elaboración y el control de dichas preparaciones a alguna de las Oficinas de Farmacia o servicios farmacéuticos que estén adscritos a un nivel igual o superior al que pertenezca la forma farmacéutica solicitada y que, además, estén autorizados para la elaboración para terceros.

3.- En los casos en que la elaboración o el control de calidad de una fórmula magistral o preparado oficial se encomiende a otra Oficina de Farmacia o servicio farmacéutico autorizado, deberá disponerse de un documento contractual, por duplicado, firmado por ambas partes, donde deberán establecerse claramente las obligaciones de cada uno.”

En puridad, pueden existir cesiones de datos de pacientes entre dos farmacias para la elaboración de las fórmulas magistrales. No sólo de pacientes, sino también de auxiliares y profesionales sanitarios. Se entendería en todo caso que estaríamos ante una

cesión de datos permitida, ya que se podría encuadrar en el art. 11.2.C de la LOPD⁷⁷, o incluso en el art. 11.2.A⁷⁸, ya que existe la correspondiente previsión legal (esto es, una ley está habilitando la cesión). También se podría encuadrar en el art. 12, siendo entonces un “acceso a datos por parte de terceros” y necesitando en todo caso el correspondiente “contrato de encargado de tratamiento”, con todos los requisitos del precepto, en puntos anteriores ya comentado.

Lo cierto es que en la Orden se hace referencia a la necesidad de que entre las farmacias cedente y cesionaria exista una autorización por escrito, pero no se especifica las medidas a cumplir en materia de Protección de Datos. Es muy recomendable que en esa autorización exista la correspondiente cláusula de protección de datos, con todos los requerimientos del art. 12, especialmente si existen cesiones de datos referidos a pacientes o interesados que solicitan fórmulas magistrales a la farmacia cedente, que por no tener el nivel necesario se ve obligado a ceder los datos del mismo a una tercera farmacia para la elaboración.

4.2.3.- La aplicación del Real Decreto 994/1999, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

El tratamiento de datos especialmente sensibles por parte de los profesionales farmacéuticos hace que los mismos están específicamente obligados a cumplir con el RMS.

El art. 9 de la LOPD establece:

“1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán 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

⁷⁷ Establece el art. 11.2.C:

“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. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.”

⁷⁸ “Cuando la cesión está autorizada en una Ley”

o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.”

El art. 9 establece el llamado “Principio de Seguridad” de los datos de carácter personal. El no someterse a este precepto implica una “falta grave”, tipificada en el art. 44.3:

“Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.”

El RMS establece las medidas técnicas y organizativas que los Responsables de Ficheros han de implantar, en particular en sus Sistemas de Información.⁷⁹

⁷⁹ No obstante, el RMS también ha de aplicarse a los ficheros en soporte papel. La AEPD zanjó la cuestión en los siguientes términos:

“El artículo 1 del Reglamento delimita su ámbito de aplicación estableciendo que será aplicable únicamente a los ficheros automatizados. Esta delimitación resultaba congruente con el sistema de garantías contemplado en la Ley Orgánica 5/1992, de 29 de octubre (LORTAD), en cuyo desarrollo fue aprobado, y que sólo era de aplicación a ficheros automatizados.

La vigente LOPD presenta como una de sus principales novedades la ampliación de su ámbito de aplicación que ahora alcanza “los datos de carácter personal registrados en soporte físico que los hace susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos...” (art. 2). Incluye, por tanto, los datos en soporte papel siempre que estén estructurados como ficheros.

La Disposición Transitoria Tercera de la LOPD mantiene la vigencia de las normas reglamentarias preexistentes, entre las que se cita el Reglamento de Medidas de Seguridad, en cuanto no se oponga a la nueva Ley.

La previsión del Reglamento de aplicarse sólo a los ficheros automatizados se opone a la vigente LOPD, al haberse ampliado su ámbito de aplicación, como se ha expuesto, por lo que debe considerarse derogada.

La protección de datos sanitarios en el sector farmacéutico

Hoy en día no resulta especialmente complicado implantar las medidas de seguridad referenciadas en el RMS. Para ello, la apuesta por un software de calidad y adaptado a la LOPD facilita mucho la tarea.⁸⁰ En la actualidad, las casas fabricantes de software han adaptado sus productos en la mayoría de los casos a la legalidad vigente,⁸¹ aunque, desgraciadamente, las Oficinas de Farmacia no se han actualizado a la misma velocidad.

A continuación se especifican los requerimientos del RMS, junto con los principales problemas –si existen- para su implantación en una Oficina de Farmacia:

-Existencia de uno o varios “Documento/s de Seguridad”.

El responsable del fichero deberá elaborar e implantar la “Política de Privacidad” mediante la implantación de 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. El mismo podrá contener la normativa de seguridad para todos los ficheros de los que es responsable la Oficina de Farmacia o por

En consecuencia, desde la entrada en vigor de la LOPD, resulta aplicable dicho Reglamento a los ficheros en soporte no automatizado que se hubieran creado con posterioridad a la entrada en vigor de la Ley Orgánica, el 14 de enero de 2000. Los ficheros en soportes no automatizados que existieran antes de dicha fecha dispondrán, a estos efectos, del período de adaptación establecido en la Disposición Adicional Primera (que finaliza en octubre de 2007).

No obstante, cuando resulte de aplicación el Reglamento de Medidas de Seguridad, conforme a los criterios expuestos, sólo deberán implantarse las medidas de seguridad que, pese a estar previstas para tratamientos automatizados, por su naturaleza sean también aplicables a ficheros no automatizados como, por ejemplo, la elaboración e implantación del Documento de Seguridad.”

⁸⁰ La excelente obra “La protección de datos personales: soluciones en entornos Microsoft”, título gratuito para su descarga y de libre acceso, es un buen ejemplo de las posibilidades de adaptación de los modernos sistemas operativos. Con una configuración correcta, los Sistemas de Información pueden guardar los “logs” de acceso, implantar las oportunas contraseñas, impedir el acceso a los recursos protegidos, llevar la gestión de las incidencias y, en definitiva, gestionar correctamente los requerimientos del RMS.

⁸¹ Cabe hacer referencia a los siguientes productos:

-Farmatic de la casa “Consoft”. Este producto integra todos los requerimientos del RMS.

-Infarm, de la casa “Farmagés”. El producto, además, incluye modelos de notificación de los ficheros automatizados que el propio programa genera, además de la impresión de cláusulas informativas para dar cumplimiento a los deberes de información, así como otras características.

-Cifarma, del grupo Cofares. Producto que permite, como no podía ser de otra forma, la implantación de contraseñas, el registro de accesos, auditorías y la implantación de derechos de uso a archivos, entre otros.

el contrario se podrán redactar tantos documentos como ficheros se tengan. Ello no lo especifica el RMS, tratándose solamente de un aspecto de gestión. En la práctica, lo lógico y recomendable es redactar un único documento de seguridad que abarque todos los ficheros de datos, no obstante sí parece recomendable la redacción de otros documentos de seguridad que engloben a los ficheros en soporte papel u otros ficheros con distintos niveles de seguridad. Todo ello con el objetivo de no repetir injustificadamente las normas y preceptos.

Es muy recomendable que todo el personal acceda en su totalidad al contenido del documento de seguridad. En caso de inspección, el Responsable del Fichero ha de probar que los trabajadores conocían las normas contenidas en el mismo.

Las menciones mínimas que deben constar en el documento son:

- a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- b) Las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
- c) Funciones y obligaciones del personal.
- d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan⁸².
- e) Procedimiento de notificación, gestión y respuesta ante las incidencias⁸³.
- f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos⁸⁴.

⁸² En el apartado 1 del artículo 2 del RMS define sistema de información como el “conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal”.

⁸³ El apartado 9 del artículo 2 del RMS define incidencia como “cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos”.

⁸⁴ El apartado 12 del artículo 2 del RMS define copia de respaldo como “la copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación”.

Es necesario señalar que el Documento de Seguridad se referirá, en muchos casos, a ficheros de Nivel Alto. Es por ello por lo que el mismo deberá hacer referencia a:

“la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.”⁸⁵

Por último conviene destacar la exigencia legal de que el documento se mantenga en todo momento actualizado, y en su caso, adecuado a las disposiciones vigentes en materia de seguridad de datos de carácter personal, así como la necesidad de que sea revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Es muy recomendable que el Responsable de Seguridad realice unos “controles periódicos de verificación del cumplimiento”, verificando que lo contenido en el documento de seguridad se corresponde con la realidad de la gestión diaria de los ficheros.

-Funciones y obligaciones del personal.

Las funciones y obligaciones del personal con acceso a los datos de carácter personal deberán estar claramente definidas y documentadas. Así mismo, 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 así como las consecuencias que se deriven de su incumplimiento, en su caso.

-Registro de Incidencias

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del Fichero, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos. El mantener un registro de las incidencias que comprometan la seguridad de un Fichero es una

⁸⁵ Art. 15 RMS

herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para persecución de los responsables de los mismos.

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar 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 que se hubieran derivado de la misma.

Al tratarse datos de Nivel Alto, el Registro de Incidencias deberá cumplir también con el resto de disposiciones:

“deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.”

Además:

“Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.”

Hay que destacar que los propios sistemas operativos o el software de gestión empleado por el profesional suele cumplir con este requerimiento, ya que integra un sistema de registro de incidencias. En concreto, sistemas como Microsoft Windows 2000 o XP permite la obtención de un registro detallado de las acciones realizadas en el sistema, configurables por el administrador que, junto con el servicio de alertas, puede ser utilizado para la creación de un sistema de registro.

En cualquier caso, es necesario hacer mención que pueden existir otro tipo de incidencias “no informáticas” (robos, desastres naturales) que pueden afectar a la integridad y confidencialidad de los ficheros, y que es preciso señalar, al menos manualmente, en el mencionado Registro.

- Identificación y autenticación.

La protección de datos sanitarios en el sector farmacéutico

El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

En este sentido, destaca que cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Además las mismas deberán cambiarse con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Nuevamente, al tratarse de datos de “Nivel Alto”, es preciso cumplir con el resto de preceptos. Así, “el responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado”. Por último, “se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.”

Los sistemas operativos, en la mayoría de los casos, ofrecen un sistema de relación de usuarios con acceso al sistema y diversos procedimientos de autenticación. En otros casos, el software de gestión puede hacer cumplir con este requerimiento.

La política de asignación de contraseñas en este sentido es primordial. El RMS, para este tipo de datos, está pidiendo que el acceso a la información sea “inequívoca y personalizada”. Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

Un periodo razonable para el cambio de las contraseñas parecer ser el de 6 meses. Ello se recomienda en la norma ISO 17799.

La protección de datos sanitarios en el sector farmacéutico

Algunas normas recomendables a la hora de asignar contraseñas son las siguientes:

-Prescindir de números de teléfono, direcciones, años o fechas completas de nacimiento.

-Intercalar, si el sistema lo permite, mayúsculas con minúsculas, caracteres y signos.

-Ha de evitarse colocar palabras convencionales, que puedan existir en un diccionario. Tampoco conviene escoger palabras escritas al revés, nombres propios, etc..

-Prescindir de números de teléfono, direcciones, años o fechas completas de nacimiento.

-Utilizar claves con la mayor longitud posible (se recomienda un mínimo de 6 caracteres).

-Utilizar contraseñas imaginativas.

-No deben seleccionarse contraseñas que se utilicen con otros fines (ejemplo: utilizar la misma contraseña para acceder al sistema y al correo web).

-Control de acceso y Control de acceso físico

Los usuarios deben tener acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. El responsable del fichero deberá establecer los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos o permisos distintos de los autorizados. La relación actualizada de usuarios que tengan acceso autorizado al sistema de información deberá contener además el acceso autorizado para cada uno de ellos.

La protección de datos sanitarios en el sector farmacéutico

Sólo el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

Además, una vez más, al tratarse de datos sensibles, exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Respecto al “control de acceso informático”, decir que en la actualidad no plantea mayor problemas que el uso del software adecuado y sistemas operativos modernos. En Windows 2000 y XP, el sistema se basa en las listas de control de acceso. Siempre que exista el sistema de ficheros NTFS se guardarán registro de accesos a ficheros y se establecerán permisos para acceder a los mismos. Este sistema asegura que el acceso a los recursos únicamente se produce por los usuarios definidos.

Mas difícil resulta dar cumplimiento al “control de acceso físico”, consecuencia del tratamiento de datos de “nivel alto”. En puridad, el RMS no autoriza al profesional farmacéutico a tratar datos de nivel alto “en un lugar físico público”, o “con acceso a otras personas”. El RMS es tajante a este respecto al afirmar que “exclusivamente el personal recogido en el Documento de Seguridad” puede acceder al lugar físico donde estén situados los “Sistemas de Información”. Sin embargo, a nadie escapa que, hoy en día, las Oficinas de Farmacia tienen sus sistemas informáticos a la vista y con apenas protección. En el peor de los casos se pueden acceder a historiales clínicos, ficheros de facturación, etc, a través de la mera visualización en la pantalla de estos Sistemas de Información. A mayor abundamiento, es común que dichos datos se guarden junto con otros elementos, como puede ser el material de papelería o de limpieza, que en muchas ocasiones es utilizado por personal externo a la propia entidad por estar externalizados dichos servicios

En el Documento de Seguridad debe figurar el personal que podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal. Y dicho personal será el único que pueda acceder.

La protección de datos sanitarios en el sector farmacéutico

Varias son las recomendaciones que se pueden dar al respecto, aunque ninguna de ellas haría cumplir con la legalidad vigente en un punto óptimo. La primera de ellas es la protección del servidor que contengan los programas informáticos, ya que será en ese Sistema de Información donde se encuentren los ficheros automatizados que contengan datos de carácter personal “de nivel alto”. Esta protección ha de producirse tanto a “nivel físico” como a “nivel informático”. El servidor ha de situarse en un lugar con acceso restringido, a ser posible protegido en un armario bajo llave o con un sistema análogo de protección. En todo caso, el servidor –o Sistema de Información que contenga los datos automatizados de carácter personal- ha de estar situado en un lugar físico distinto a donde se encuentren los terminales “públicos”. A nivel informático, el servidor debe tener un registro de acceso, contraseñas, sistemas de cifrado etc.

El Responsable del Fichero podría, en todo caso, prohibir la entrada a todo el personal ajeno a la entidad mediante la colocación de cláusulas informativas en la propia Oficina de Farmacia. Esta es una medida que se está aplicando ya en algunas Oficinas de Farmacia de Castilla La Mancha, que han sido conscientes no sólo de la necesidad de dar cumplimiento a este precepto, sino de “probar” el mismo ante una Inspección de la AEPD. No olvidemos que la “carga de la prueba”, según toda la jurisprudencia de la Audiencia Nacional, órgano judicial que se encarga de enjuiciar las resoluciones de la AEPD en caso de recurso contra las mismas, corresponde al Responsable del Fichero (como ya se ha repetido anteriormente).

-Gestión de Soportes.

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. Además, la salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

Al tratarse datos de Nivel Alto, deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que

contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada. Se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario. Por último, cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Se trata de muchas indicaciones encaminadas todas ellas a proteger la información tratada. La consecuencia del cumplimiento de este precepto es la necesaria “documentación” que el Responsable del Fichero ha de tener siempre a punto. En el precepto se hace referencia a registros de entrada y salida y autorizaciones. El Documento de Seguridad ha de prever estas necesidades, con la consiguiente creación de campos preparados al efecto, donde se especifiquen todos y cada uno de los aspectos recogidos en este completo artículo del RMS.

En el caso particular en que los soportes vayan a salir de los centros de trabajo, el Responsable del Fichero ha de autorizarlo y asegurarse de que no se van a producir accesos indebidos. El RMS define “soporte” “como objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos”,⁸⁶ olvidándose del supuesto por el cual el propio Sistema de Información haya de salir del centro de trabajo. Si el “Sistema de Información” es el “sistema informático” que trata al “soporte”, es lógico pensar que la intimidad de los interesados se puede vulnerar si se producen la salida de ambos, ya que en los propios “Sistemas de

⁸⁶ Art. 2, apartado 10 del RMS.

Información” existirán, con toda seguridad, ficheros que contengan datos de carácter personal que, además, tendrán la consideración de “ficheros de nivel alto”.⁸⁷

El Responsable del Fichero ha de asegurarse de la información que contienen los soportes informáticos cuando estos vayan a salir de los centros de trabajo. La recomendación más usual al respecto es que los soportes sean formateados o se entreguen sin ningún tipo de información, y mucho menos información de carácter personal. También podría cumplirse con este precepto si se entregan cifrados o bajo contraseña. En la actualidad, no es difícil encontrarse con cláusulas de confidencialidad firmadas por las empresas informáticas comprometiéndose a no acceder a datos de carácter personal, lo cual aporta la “prueba documental” necesaria en caso de inspección por parte de la AEPD.

-Copias de Seguridad.

El Responsable del Fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Una vez más, al tratarse datos de nivel alto, existen unas recomendaciones adicionales: deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

⁸⁷ Piénsese por ejemplo en los discos duros de los Sistemas de Información, donde se pueden almacenar datos de carácter personal. Sin embargo, la definición del RMS invita más a considerar a los “Sistemas Informáticos” como “Sistemas de Información”, no como meros “soportes”, habida cuenta de las facultades que tienen los primeros para tratar los segundos, esto es, para escribir, procesar, alterar o actualizar la información contenida en los “soportes” propiamente dichos (por ejemplo, cd, cintas de back-up, unidades zip, dvd, etc...). Pues bien, en este artículo, el RMS se centra en los “soportes”, no en los “Sistemas de Información”, cuando es lógico pensar que es muy fácil acceder –también– a información sensible en los segundos.

La protección de datos sanitarios en el sector farmacéutico

La realización de copias de seguridad debería ser un elemento fundamental en cualquier empresa, si bien, en muchas ocasiones, esto no siempre es así, y ello a pesar de que los actuales sistemas de elaboración de copias de seguridad facilitan mucho la labor.

Hay que señalar que cualquier software o sistema operativo actual “proporciona su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción”. Otra cosa es que existan datos de carácter personal sobre los cuales el Responsable del Fichero no haga copias por considerarlos de importancia limitada. Ello supone una vulneración del RMS, ya que el texto no hace este tipo de distinciones.

El procedimiento de realización de copias de seguridad debe estar señalado en el Documento de Seguridad, donde, además, se establecerá la periodicidad –semanal-, el soporte y cualquier otra información que guarde relación con la misma.

Hoy en día, todos los sistemas operativos actuales y/o el software de gestión viene preparado para automatizar estas tareas.

El RMS no incide en el tipo de soporte en el cual deben de almacenarse las copias de seguridad, pero si incide –al tratarse de datos de nivel alto- en el lugar físico donde deben permanecer: en un lugar diferente de aquél en que se encuentren los equipos informáticos. Ello es una medida de seguridad básica, casi de sentido común, pero se ha de advertir que existe un alto grado de incumplimiento. En efecto: muchos Responsables de Ficheros optan por realizar copias de seguridad en el mismo disco duro, o en soportes que son almacenados en el mismo sistema informático. Ello supone una clara vulneración del RMS, además de un peligro inmediato a la seguridad e integrada de la información tratada.

-Responsable de Seguridad

El Responsable del Fichero debe designar uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. Se entiende que el Responsable de Seguridad puede ser tanto personal interno como terceras personas, físicas o jurídicas, es decir, que se puede externalizar la

La protección de datos sanitarios en el sector farmacéutico

seguridad del sistema de información. En ningún caso la designación del responsable de seguridad supone una delegación de la responsabilidad que corresponde al responsable del fichero.

La figura del Responsable de Seguridad tiene una especial importancia dentro del efectivo cumplimiento del RMS ya que se encargará de coordinar y controlar las medidas de seguridad aplicables, analizar los informes de auditoría y, en su caso, controlar los mecanismos que permiten llevar el registro de accesos a los datos sanitarios.

El Responsable de Seguridad en una Oficina de Farmacia debe ser alguien que tenga un conocimiento general de la administración de la misma, y también alguien con suficientes conocimientos técnicos o informáticos. En la mayoría de los casos, el Responsable de Seguridad debe ser el Titular de la Oficina de Farmacia.

-Auditoría de los Sistemas de Información

Los Sistemas de Información deben someterse, al menos cada dos años, a una auditoría interna o externa, con la finalidad de verificar el cumplimiento del RMS y de los procedimientos e instrucciones vigentes en materia de seguridad de datos.

La auditoría debe plasmarse en un informe que deberá dictaminar sobre la adecuación de las medidas y controles al mencionado RMS, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

Asimismo, debe incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas. Estos informes deben ser analizados por el Responsable de Seguridad competente, quien, a su vez, está obligado a elevar las conclusiones al Responsable del Fichero para que adopte las medidas correctoras adecuadas.

Los informes quedan a disposición de los inspectores de la AEPD.

La protección de datos sanitarios en el sector farmacéutico

A pesar de que la auditoría puede ser interna o externa, es recomendable que sea externa o en caso de que sea interna, que, al menos, la misma sea realizada por un departamento de auditoría independiente del departamento auditado. En cualquier caso, en una Oficina de Farmacia no solemos encontrar personas con los conocimientos técnicos necesarios para realizar una correcta y adecuada auditoría.

Se ha discutido bastante sobre las capacidades del auditor, y sobre la necesidad de que exista una titulación oficial, como existe por ejemplo en la figura de la “auditoría de cuentas”. Lo cierto es que no encontramos en ninguna disposición ni en ninguna recomendación de la AEPD recomendación alguna al respecto. Parece claro que el auditor ha de tener una sólida formación informática y jurídica.⁸⁸

La Auditoría ha de tener por objeto:

- dictaminar sobre la adecuación de las medidas y controles al RMS
- identificar deficiencias
- proponer las medidas correctoras necesarias.

Una observación importante al respecto es que la Auditoría ha de tratar sobre los Sistemas de Información que traten datos de Nivel Medio o Alto, ya que no se exige para fichero con datos de Nivel Básico.

- Pruebas con datos reales.

Con relación a las pruebas anteriores a la implantación o modificación de los Sistemas de Información que contengan ficheros o tratamientos con datos de carácter personal, los mismos no podrán realizarse con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

⁸⁸ No obstante, hay que decir que existe una certificación, internacionalmente reconocida, que parece muy apropiada. Nos referimos a la certificación CISA (“Certified Information Systems Auditor”, Auditor Certificado de Sistemas de Información). La Institución ISACA (Information Systems Audit and Control Association, Asociación de Auditoría y Control de Sistemas de Información) es la que proporciona la titulación. Hay que señalar que todos los inspectores de la AEPD son CISA.

-Cifrado

La distribución de los soportes que contengan datos de carácter personal 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 los datos de carácter personal se realice a través de redes de telecomunicaciones, se deberá llevar a cabo cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

La AEPD en su Memoria del año 2000 dispuso que las medidas a las que se refiere el artículo 26 del RMS son de aplicación a la transmisión de datos entre distintas dependencias de la entidad cuando sea necesaria para dicha transmisión la utilización de redes de telecomunicaciones cuya titularidad sea ajena a la propia empresa, no siendo preciso el cifrado de los datos en caso de que las comunicaciones en ningún momento accedan a dicha red. Y es que es lógico pensar que el grado de vulneración de privacidad es distinta en una mera transmisión de información en la propia intranet de la Oficina de Farmacia o al enviar un correo electrónico utilizando Internet.

La tecnología en este punto ha avanzado a pasos agigantados. En Internet, existen dos protocolos muy distintos (SSL, secure socket layer y SET, secure electronic transfer) pero con finalidades semejantes: cifrar la información y hacerla indisponible a terceros cuando se transmite por la red. El software P.G.P. (Pretty Good Privacy) es casi un estándar de hecho por la cantidad de usuarios que tiene. Utiliza la llamada criptografía de clave pública, funciones resumen y algoritmos avanzados con la misma finalidad anteriormente mencionada (también existen versiones de código abierto, GNUPG). También la legislación ha avanzado,⁸⁹ si bien a menor velocidad.

⁸⁹ En nuestro país contamos con cierta tradición legislativa en este aspecto, ya que España fue el primer miembro de la Unión Europea en tener un Real Decreto (en concreto, el R.D. 14/99) que regulara el uso de la Firma Electrónica. Real Decreto que, por cierto, entró en vigor incluso antes de que se promulgara la Directiva de Firma Electrónica, la 1999/93/CE. El resultado fue que el texto al cual antes se aludía se tuvo que modificar. En esta ocasión, el medio utilizado ha sido la Ley Ordinaria, en concreto la 59/2003. La tecnología de firma electrónica es un complemento excelente al cifrado, y proporciona las notas de autenticidad, integridad y no repudio inherentes a la misma.

El Responsable del Fichero ha de proteger los soportes que contengan datos sanitarios. Los soportes no sólo han de situarse en un lugar distinto a donde se encuentren los Sistemas de Información, se requiere un nivel de protección adicional. Es recomendable que se guarden en armarios bajo llave, cajas de seguridad o utilizando un sistema análogo.

4.2.4.- Otros aspectos.

La política de privacidad a implantar en una Oficina de Farmacia tiene otros aspectos relevantes.

En primer lugar, el profesional está obligado a proceder con la inscripción de los ficheros de carácter personal de los cuales sea titular. El criterio de la AEPD es el considerar a cualquier información relativa a la salud de las personas como información especialmente sensible y de “nivel alto”. Entre los mismos, podríamos destacar una serie de ficheros que se pueden dar con bastante facilidad en una Oficina de Farmacia:

-Fichero “clientes”. Informaciones relativas a clientes con los bienes y servicios suministrados. Es de “nivel alto” si el mismo se refiere a medicamentos y/o bienes y servicios sanitarios suministrados por el profesional, aunque si solo existen datos identificativos el nivel es “básico”.

-Fichero “pacientes”. Es el relativo a la atención farmacéutica dispensada. Obviamente, el fichero tiene el nivel “alto” porque contiene historiales farmacoterapéuticos de los interesados.

-Fichero “formulación magistral”. Es el relativo a los bienes y servicios suministrados en relación con la formulación magistral. Nuevamente, el fichero tiene el nivel “alto”.

La protección de datos sanitarios en el sector farmacéutico

-Ficheros “vacunas”, “dietas”, “ortopedia”, etc. Se repite lo anteriormente señalado. Si se identifica al interesado estaremos ante ficheros de “nivel alto”.

-Fichero “personal”. Se trata de informaciones relativas a auxiliares, trabajadores, personal administrativo u otros profesionales sanitarios. Puede conllevar el tratamiento de datos relativos a las nóminas de los empleados, teniendo entonces la consideración de “nivel alto”.

-Fichero “proveedores”. Hay que destacar que en muchas ocasiones no nos encontramos ante un fichero de datos de carácter personal, ya que las informaciones de este fichero hacen referencia ante todo a proveedores farmacéuticos (cooperativas). Sin embargo, si existen datos de contacto sí estaremos ante un fichero a proteger.

-Ficheros “Libro Recetario Oficial” y “Libro de Contabilidad de Estupefacientes”. Los profesionales farmacéuticos están obligados a contabilizar en estos libros ciertos medicamentos o estupefacientes dispensados. En la mayoría de las Oficinas de Farmacia estos dos ficheros se gestionan de forma manual, esto es, en soporte papel, aunque muchos programas farmacéuticos permiten su gestión de forma automatizada. El segundo de ellos tendrá la consideración, en todos los casos, de fichero de “nivel alto”, ya que se identifica al interesado. En el primero de ellos, nuevamente si se identifica al interesado, se tendrá la consideración de fichero de “nivel alto”. En caso contrario, sólo existirían identificaciones de los médicos o facultativos prescriptores de medicamentos, por lo que estaríamos ante un fichero de nivel básico.⁹⁰

-Fichero “Facturación”. Los profesionales farmacéuticos, como ya se ha señalado anteriormente, están obligados a colaborar con el Sistema Nacional de Salud y con los correspondientes servicios autonómicos, recaban información relativa a la

⁹⁰ Y esto plantea un problema de difícil solución. El art. 5 apartado 4 de la LOPD establece lo siguiente:

“Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.”

En puridad, estamos ante una situación en la cual el profesional farmacéutico está obligado a informar a los médicos prescriptores de medicamentos de todos los extremos contenidos en el art. 5 de la LOPD.

La protección de datos sanitarios en el sector farmacéutico

“facturación de recetas”, y por tanto gestionando el correspondiente fichero. Sin embargo, la AEPD ya se ha pronunciado al respecto, considerando Responsables del Tratamiento del mismo al Servicio Autónomo de salud y/o Servicio Nacional de Salud, además de a los propios Colegios Oficiales de Farmacéuticos. Los profesionales farmacéuticos están obligados a recabar esta información, pero son unos meros transmisores de la misma a estas dos instituciones. Si el profesional realiza cualquier otra tarea con este fichero será considerado Responsable del fichero o Tratamiento, ya que está decidiendo sobre una nueva “finalidad del fichero”, todo ello en consonancia con el mejor criterio de la AEPD y el art. 3 de la LOPD. Sin embargo, en la mayoría de los casos esto no es así, recayendo la obligación de inscripción en su caso, en los Colegios Oficiales de Farmacéuticos y/o en el Servicio de Salud, bien autonómico, bien nacional.

-Otros ficheros. La Oficina de Farmacia puede gestionar otro tipo de informaciones comunes a cualquier otro establecimiento mercantil. De hecho, la misma tiene la consideración de establecimiento mercantil.⁹¹ Como tal, podemos encontrar informaciones relacionadas con los recursos humanos (Currículum Vitae), contabilidad, correo electrónico, control horario, impagados, etc. Todos y cada uno de estos ficheros

⁹¹ De hecho, un informe del Tribunal de Defensa de la Competencia de 1995 se refiere a las mismas en los siguientes términos:

“...en general, las funciones del farmacéutico tradicional las llevan a cabo hoy los laboratorios farmacéuticos. La tradicional oficina de farmacia va evolucionando hacia un establecimiento comercial de naturaleza mercantil, -cuya titularidad se alcanza mediante la correspondiente licencia administrativa de carácter vitalicio, en el que se venden especialidades farmacéuticas junto con otros productos”, indicando más adelante que “el farmacéutico ofrece un servicio, pero también vende un producto, una mercadería”

Por su parte, al AEPD, en un informe relativo a la cesión de datos de facturación de las Oficinas de Farmacia, se pronuncia en los siguientes términos:

“se viene a configurar la oficina de farmacia como un establecimiento mercantil, concebido como el conjunto de bienes y servicios que permiten a un empresario desarrollar su actividad empresarial, en los términos previstos en el Código de Comercio o en el Capítulo Segundo de la Ley de 16 de diciembre de 1954 de Hipoteca Mobiliaria y Prenda sin Desplazamiento de la Posesión, o como industria o negocio, en el sentido que definía el artículo 3.2 de la derogada Ley de Arrendamiento Urbanos, de 24 de diciembre de 1964”

A efectos de la LOPD, ha que destacar que no todos los datos tratados por los profesionales farmacéuticos serán considerados datos de carácter personal. Todo ello siguiendo el criterio de la AEPD. En el anterior informe al que se hacía referencia, se pronuncia en los siguientes términos:

“...debe recordarse que la doctrina y las distintas resoluciones e informes de órganos de naturaleza administrativa y jurisdiccional han venido a recalcar la necesaria diferenciación que debe efectuarse entre la persona física del farmacéutico, que ostenta la condición de miembro de una profesión colegiada y el establecimiento del que es titular, que ostenta la condición de establecimiento mercantil...”

La protección de datos sanitarios en el sector farmacéutico

podrá ser tratado en la medida en que responda a una finalidad legítima, en relación con el objeto social del profesional farmacéutico, no presentando ninguna peculiaridad respecto de otras empresas o Responsables de Ficheros.

Por otro lado, el profesional farmacéutico debe extremar las precauciones con la información en soporte papel, ya que la misma es especialmente sensible. Existen datos relativos a libros oficiales, facturación o recetas sobre la que hay que extremar las precauciones. El titular de la Oficina de Farmacia debería emitir un comunicado al personal de su establecimiento donde se hiciera mención, entre otros, a extremos tales como:

-La necesidad de que estos datos en soporte papel sean tratados sólo cuando esté justificado teniendo en cuenta las finalidades para las cuales fueron recabados.

-Que el uso y tratamiento de este tipo de datos personales debe ser llevado a cabo exclusivamente por personal autorizado para ello, cuando sea necesario para el desarrollo de sus funciones.

-El personal ha de ser consciente de que estos ficheros tienen reconocidos los derechos de acceso, modificación y cancelación.

-El titular debe dar instrucciones al personal acerca de la prohibición expresa de mantener, datos personales en soporte físico cuando los mismos ya no sean útiles ni necesarios para el fin que justificó su recogida y conservación. En este supuesto se debe proceder a su destrucción física, siempre que no existan obligaciones legales que señalen lo contrario,

-El titular debe advertir de la necesidad de que bajo ningún concepto se comunicarán, intercambiarán o cederán, en todo o en parte, los datos personales recogidos en soporte físico a personas que no precisen tratar dichos datos para el desempeño de sus funciones profesionales, y a salvo siempre de las obligaciones legales que la empresa tiene

La protección de datos sanitarios en el sector farmacéutico

Estas normas específicas para este tipo de ficheros vienen derivadas de la obligación de secreto recogida en nuestra LOPD.⁹²

Otro aspecto importante es el deber de información que tiene el profesional farmacéutico para dar cumplimiento al art. 5 LOPD. Hay que precisar lo siguiente: una cosa es que el profesional farmacéutico pueda tratar datos de salud como establece los arts. 7 y 8, así como la legislación farmacéutica, y otra muy distinta es la obligación de información que tiene todo interesado sobre el destino de los datos de los que es titular.

Así, es muy recomendable que el profesional informe mediante las correspondientes cláusulas de privacidad. Las mismas pueden ir contenidas en facturas, contratos y/o notas informativas en el establecimiento. En particular, es necesario que se informe sobre las posibles cesiones de datos al SESCAM, a los Colegios Oficiales de Farmacéuticos y/o al Servicio Nacional de Salud.

En relación a lo anterior, es obligatorio que el titular de la Oficina de Farmacia conozca el procedimiento a seguir en el caso de que algún interesado ejercite sus derechos de acceso, cancelación y rectificación. La Instrucción 1/98 de la AEPD obliga a los Responsables de Ficheros a que conozcan los procedimientos a seguir y cómo actuar en todo momento.⁹³

⁹² El precepto 10 de la LOPD recoge lo siguiente:

“El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.”

Por su parte, el código español de ética farmacéutica establece que:

“El farmacéutico protegerá el derecho del paciente a la confidencialidad de sus datos.”

⁹³ La Norma Primera de la mentada Instrucción 1/98 establece:

“El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.”

Ello obliga a que el titular farmacéutico de las correspondientes instrucciones a auxiliares y demás personal de su establecimiento y que accedan a datos de carácter personal para que actúen convenientemente.

La protección de datos sanitarios en el sector farmacéutico

Otro aspecto capital es la creación de ficheros temporales en las Oficinas de Farmacia. Hay que recordar que este tipo de ficheros son creados para finalidades muy concretas, y que no tienen la vocación de perdurar en el tiempo. Además, los datos han sido recogidos de los “ficheros”, propiamente dichos. Estos ficheros temporales han de cumplir igualmente el deber de secreto, sin embargo, no se estima necesaria la obligación de inscripción de los mismos en la AEPD, habida cuenta de que han sido creados a partir de otros, todo ello siguiendo el mejor criterio de la AEPD. Sin embargo, el profesional farmacéutico debe igualmente extremar las precauciones, ya que estos ficheros pueden contener información sensible.

Por último, el profesional farmacéutico debe igualmente pedir el consentimiento e informar a todos sus trabajadores de la necesidad de proceder al tratamiento de sus datos de carácter personal, ya que ello es imprescindible para el mantenimiento de la relación laboral. Ello conllevará en la mayoría de las ocasiones la firma del “contrato de encargado de tratamiento” con la empresa que preste servicios laborales al “Responsable del Fichero”, y también el deber de información por parte de este Responsable para con sus empleados.

BIBLIOGRAFÍA

-ALVAREZ-CIENFUEGOS SUÁREZ, J., “*La aplicación de la firma electrónica y la protección de datos relativos a la salud*”, Actualidad Informática Aranzadi, núm 39/2001.

-ALVAREZ-CIENFUEGOS SUÁREZ, J., “*La defensa de la intimidad e los ciudadanos y la tecnología informática*, ed. Aranzadi, Pamplona, 1999.

-CASTAÑEDA GONZALEZ, A., BONADEO FIORONI, R., SANCHEZ ECHEVERRÍA, J. “*Guía Práctica de Protección de Datos de Carácter Personal*”, ed. Ediciones Experiencia, Barcelona, 2002.

-DAVARA RODRIGUEZ, M., “*Factbook de comercio electrónico*”, ed. Aranzadi, Madrid, 2002.

-DAVARA RODRIGUEZ, M., “*La protección de datos en España; principios y derechos*”, Actualidad Informática Aranzadi, núm. 13.

DAVARA RODRÍGUEZ, M.: “*XIII Encuentros sobre informática y Derecho*”, Elcano, Aranzadi, 2000.

-ECIJA ABOGADOS, “*Factbook de protección de datos*”, ed. Aranzadi, 2003.

-GALÁN CORTÉS. J.: “*El consentimiento informado del usuario de los servicios sanitarios*,”ed. Colex, Madrid, 1997.

-GONZALEZ GUINZA, A., “*Recurso de amparo sobre el acceso a ficheros públicos automatizados de carácter personal*”, Actualidad Informática Aranzadi, núm 10.

-LUCAS MURILLO DE LA CUEVA, P., “El derecho a la autodeterminación informativa”, ed. Tecnos, Madrid, 1990.

-“*Manual de Protección de Datos para Colegios Profesionales*”. Agencia de Protección de Datos de la Comunidad de Madrid, ed. Civitas. 2004.

-Memorias de la Agencia Española de Protección de Datos.

-Memorias de la Agencia de Protección de Datos de la Comunidad de Madrid.

-ORTÍ VALLEJO, A., “*Derecho a la intimidad e informática, Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada*”, ed. Comares, Granada, 1994.

-“*Protección de Datos de Salud: criterios y plan de seguridad*”, autores varios, ed. Díaz de Santos, 2001.

-RUIZ CARRILLO, A., “Los datos de carácter personal”, ed Bosh, Barcelona, 1999.

-RUIZ FERRÁN, J., ZAMANILLO SARMIENTO, C., “*Confidencialidad de datos clínicos y aseguramiento sanitario privado*”, Actualidad Informática Aranzadi, núm. 39/2001.

-SÁNCHEZ CARAZO, C., “*La intimidad y el secreto médico*”; ed. Díaz de Santos, Madrid, 2000.

-SERRANO PEREZ, M., “*El derecho fundamental a la protección de datos. Derecho español y comparado*”, ed. Civitas, 2003.

SERRANO PEREZ, M., “*La protección de datos relativos a la salud en la legislación española y en la normativa comunitaria*”, Noticias de la Unión Europea, nº 187/188.

La protección de datos sanitarios en el sector farmacéutico

-ULL PONT, E., “Legislación Informática”, ed. Universidad Nacional de Educación a Distancia, 1997.

-VIZCAINO CALDERON, M., “*Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*”, ed. Civitas, Madrid, 2001.