Procedimiento nº.: PS/00698/2010

ASUNTO: Recurso de Reposición Nº RR/00523/2011

Examinado el recurso de reposición interpuesto por la entidad ***HOSPITAL NTRA. SRA. DE LA SALUD*** contra la resolución dictada por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00698/2010, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 10 de junio de 2011, se dictó resolución por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00698/2010 , en virtud de la cual se imponía a la entidad denunciado, una sanción de 18.000 €, por la vulneración de lo dispuesto en el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), infracción tipificada como grave en el artículo 44.3.h, de conformidad con lo establecido en el artículo 45 de la citada Ley Orgánica.

Dicha resolución, que fue notificada al recurrente en fecha 13/6/11, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en el artículo 127 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00698/2010, quedó constancia de los siguientes:

<<<<HECHOS PROBADOS

1º *Consta escrito de denuncia, de fecha 28/12/09, de la Dirección General de la Policía y la Guardia Civil* ***(****SEPRONA****)****, en el que declara que, con fecha 14 de octubre de 2009, se recibió en la Jefatura del SEPRONA escrito dimanante de la Productora "Cuarzo Producciones, S.L.", mediante el que se ponían en conocimiento supuestas irregularidades en materia de gestión de residuos biosanitarios en que pudieran hallarse implicadas diversas clínicas, entre las que se encontraba El Sanatorio Nuestra Señora de la Salud de Granada, S.A (en lo sucesivo la denunciada) aportando documentos y grabaciones obtenidas acerca de la investigación periodística llevada a cabo. Con el citado escrito se aportaba un CD que contenía fotos de toda la documentación hallada en las Clínicas investigadas.*

2º *Consta inspección realizada, el día 15/2/10, en los locales de la Productora "Cuarzo Producciones, S.L." en la que se puso de manifiesto lo siguiente:*

** Durante el periodo comprendido entre 15 de septiembre y 15 de octubre de 2009, la Productora comenzó la realización de un reportaje de investigación sobre gestión de residuos biosanitarios en diferentes clínicas de Andalucía, entre las clínicas investigadas se encuentra el Sanatorio Nuestra Señora de la Salud de Granada, en el cual se detectó que dicha clínica depositaba bolsas con residuos en un contenedor ubicado en la vía pública, en el que depositaban las bolsas de basuras los vecinos de las viviendas de la zona.*

******* *Los reporteros, procedieron a la recogida de las citadas bolsas, comprobándose la*

existencia de diferentes residuos, así como documentos con datos personales y de salud.

** La representante de la Productora hace entrega de la siguiente documentación, perteneciente al Sanatorio Nuestra Señora de la Salud:*

2.3.1 Cinco hojas de atención a pacientes en el Servicio de Urgencias.

2.3.2 Solicitudes de análisis clínicos

2.3.3. Imágenes de varias ecografías.

2.3.4. Varios documentos con etiquetas con los datos de los pacientes

2.3.5. Escrito de remisión a un Juzgado con relación a un paciente atendido en el servicio de Urgencias.

2.3.6. Cinco o seis juegos de etiquetas de varios pacientes

***3º** Consta inspección realizada en los locales del Sanatorio Nuestra Señora de la Salud de Granada S.A., con fecha 25/3/10.*

***4º** El Sanatorio Nuestra Señora de la Salud de Granada S.A. es un hospital perteneciente al Grupo ADESLAS, no obstante en el mismo se atienden pacientes pertenecientes a diferentes sociedades médicas así como consultas privadas.*

***5º** Todos los documentos correspondientes cuentan con el anagrama del mismo en el encabezamiento, así como la denominación, dirección postal y número de fax.*

***6º** Que la entidad cuenta, entre otros, con el fichero denominado PACIENTES, inscrito en el Registro General de Protección de Datos, con el código ###COD.1, descrito como REGISTRO OBLIGATORIO DE PACIENTES PARA CONFECCION HISTORIA CLINICA Y DATOS ADMINISTRATIVOS, donde se incluyen todos los datos de los pacientes que son atendidos en el Centro.*

7º** Consta las siguientes aclaraciones realizadas a los documentos mostrados en el transcurso de la inspección**:

***- Documento 6**: corresponde a una impreso autocopiativo de color amarillo, de solicitud de analítica de uso interno del hospital, en cuya cabecera existe una etiqueta con los datos identificativos del paciente, el facultativo que los solicita y la compañía aseguradora a la que pertenece el paciente. Se verifica que en el sistema de información, consta que los datos que aparecen en la etiqueta corresponden a un paciente del SANATORIO. En el documento recuperado aparecen el nombre y apellidos del paciente y del facultativo, domicilio, Nif, y pruebas diagnósticas solicitadas*

***- Documento 9**: corresponde a una hoja de citación de pacientes de un facultativo, este documento se le entrega al mismo para cada consulta. Se verifica que en el sistema de información consta que los datos que aparecen en el listado relativo a cinco pacientes, se corresponden con pacientes del SANATORIO. En el documento recuperado aparece el*

nombre y apellidos de cinco pacientes, junto al del facultativo, así como el tipo de prestación: "estudio preoperatorio".

***- Documento 11:** corresponde a una hoja recordatorio de citación que se entrega al paciente para que acuda a la consulta. Se verifica que los datos de dicho paciente constan en el sistema de información. Los datos personales que constan son el nombre y apellidos del paciente, la edad, el número de historia clínica, el apellido del facultativo y el servicio: "urología".*

***- Documento 13**: corresponde a un sobre con una etiqueta identificativa con los datos de una persona, el cual ha sido entregado al mismo por el SANATORIO con un ECG supuestamente en su interior. Se verifica que los datos que aparecen en la etiqueta constan en el sistema de información.*

***- Documento 15**: corresponde a varias etiquetas con datos personales relativos a cuatro personas. Se verifica que en el sistema de información, que los datos de los mismos corresponden a cuatro pacientes del SANATORIO. Los datos que constan en las etiquetas son el nombre y apellidos de los pacientes, edad, fecha de nacimiento, teléfono y NASS. Consta también el nombre y apellidos del facultativo, el domicilio y el NIF.*

***- Documento 17**: corresponde a dos informes denominados "Hoja de Urgencias", con sus correspondientes etiquetas en la cabecera de los mismos, estas hojas de color blanco, pertenecen al modelo autocopiativo que se utiliza en el Servicio de Urgencias y son las que se entregan al paciente cuando es atendido. Se verifica que en el sistema de información, consta que los datos que aparecen en la etiquetas corresponden a pacientes atendidos en el SANATORIO.*

***- Documento 20**: corresponde a dos documentos que no han sido emitidos por el SANATORIO, por lo que se supone que los ha traído el propio paciente de otro Centro. Se verifica que los datos de ambas personas constan en el sistema de información.*

***- Documento 22**: corresponde al original de un Informe de un paciente, emitido por un facultativo y que ha sido solicitado por un Juzgado, ante lo que los representantes del SANATORIO manifiestan que estos Informes son emitidos por el propio facultativo, siendo remitidos mediante escrito al Juzgado y no quedando ninguna copia del Informe adjunta al citado escrito en los Archivos. Se verifica que en el sistema de información, consta que los datos que aparecen en el Informe corresponden a un paciente del SANATORIO. En dicho informe aparece el nombre y apellido del paciente, la fecha del accidente sufrido y el resultado de la exploración y tratamiento. Por los representantes de la entidad se señala que se desconocen el motivo por el que ha aparecido otro Informe original fuera de la consulta del facultativo.*

***8º** Con relación a las medidas de seguridad se realizan las siguientes manifestaciones*

- Que la entidad cuenta con una normativa de seguridad relativa a la destrucción de la documentación con datos de pacientes y que no es incluida en las historias clínicas. Toda la documentación que no es necesaria se destruye en las máquinas destructoras de papel existentes en diversos departamentos de Centro: Admisión, Urgencias y Controles de enfermería. Una vez triturados se traslada a contenedores de papel que luego son recogidos por los servicios municipales, pero que se encuentran ubicados dentro del

recinto del SANATORIO cerrados con llave. Se comprobó la existencia de dichos contenedores dentro del recinto del hospital.

***9º** Se comprobó que existen contenedores de papel cerrados con llave, en los que se puede depositar documentación sin destruir. Dichos contenedores son recogidos periódicamente una empresa de prestación de servicios con la que el Sanatorio tiene suscrito un contrato de prestación de servicios con esta finalidad, la cual emite un Certificado de recogida y destrucción por cada servicio realizado.*

***10º** Que todo el personal del SANATORIO tiene firmado un documento de confidencialidad, en el que se comprometen al cumplimiento de todas las normas de seguridad establecidas en el Documento de Seguridad.*

***11º** En relación a las historias clínicas, manifiestan, que dada la gran cantidad de papel acumulado, se manifiesta que se tiene suscrito un contrato de prestación de servicios, con la finalidad de recogida y custodia de historias clínicas.*

***12º** Se comprueba que en el Sistema de Información existe una carpeta común para todo el personal denominada "SEGURIDAD", en la que están incluidos todos los Procedimientos y Normativa relacionada con la Protección y Seguridad de la información.*

***13º** Por parte de Los representantes del SANATORIO, se manifestó que toda la documentación mostrada y especificada, pertenecen a una misma zona del Centro (Consultas externas), donde existen papeleras para uso de los pacientes, por lo que la documentación mostrada que correspondería a los pacientes ha podido ser depositada por ellos en las mismas. En ningún se deposita documentación del SANATORIO ni ningún tipo de residuo, fuera de los contenedores que se encuentran en el recinto de este Centro, los cuales son recogidos todos los días por los Servicios municipales.>>>>*

TERCERO: ***HOSPITAL NTRA. SRA. DE LA SALUD*** ha presentado en fecha 11/7/11, en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo, básicamente, en las cuestiones ya alegadas y tenidas en cuenta en la tramitación del procedimiento sancionador.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC).

II

Se alega como motivo del recurso la caducidad de las actuaciones previas y consecuente ausencia de fundamento para imputar a la denunciada una responsabilidad infractora. Se han constatado las siguientes fechas en relación a dichas actuaciones previas:

28/12/09. Entrada en la AEPD del escrito de Seprona por el que se denuncian los hechos que dan origen al expediente.
14/12/10. Por el Director de la Agencia se dicta el Acuerdo de Inicio
25/01/11. Notificación a la denunciada del Acuerdo de Inicio.

No obstante lo anterior, consta en el expediente (folio 151) un intento de notificación de fecha 18/12/09 (por lo tanto anterior a la fecha de caducidad de las actuaciones previas), certificando el servicio de correos que dicho Acuerdo de Inicio no fue retirado en lista. Por consiguiente, al existir un intento de notificación debidamente acreditado en fecha 18/12/09 se debe acudir a este y no a la fecha de 25/01/11 donde se produjo la notificación, en segundo intento, del Acuerdo de Inicio. Tal como ha establecido el Tribunal Supremo, en Sentencia de 17/11/03, fijando la siguiente doctrina legal: "*Que el inciso intento de notificación debidamente acreditado que emplea el artículo 58.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se refiere al intento de notificación personal por cualquier procedimiento que cumpla con las exigencias legales contempladas en el artículo 59.1 de la Ley 30/1992, pero que resulte infructuoso por cualquier circunstancia y que quede debidamente acreditado. De esta manera, bastará para entender concluso un procedimiento administrativo dentro del plazo máximo que la ley le asigne, en aplicación del referido artículo 58.4 de la Ley 30/1992, el intento de notificación por cualquier medio legalmente admisible según los términos del artículo 59 de la Ley 30/1992, y que se practique con todas las garantías legales aunque resulte frustrado finalmente, y siempre que quede debida constancia del mismo en el expediente. En relación con la práctica de la notificación por medio de correo certificado con acuse de recibo, el intento de notificación queda culminado, a los efectos del artículo 58.4 de la Ley 30/1992, en el momento en que la Administración reciba la devolución del envío, por no haberse logrado practicar la notificación, siempre que quede constancia de ello en el expediente*".

Por lo tanto procede desestimar este motivo de la reclamación, al no haberse producido la caducidad de las actuaciones previas de investigación.

III

En relación con las manifestaciones efectuadas por ***HOSPITAL NTRA. SRA. DE LA SALUD***, a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho del II AL X ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

<<<<II

El artículo 68 de la Ley de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común, establece que "los procedimientos podrán iniciarse de oficio o solicitud de persona interesada". En el artículo 69 se indica que los procedimientos se inician de oficio "por acuerdo del órgano competente, bien por propia iniciativa o como consecuencia de orden superior, a petición razonada de otros órganos o por denuncia".

Es al Director de la Agencia de Protección de Datos a quien incumbe iniciar de oficio el

procedimiento sancionador, obedeciendo dicha iniciación a cualquiera de las formas mencionadas. La denuncia, con carácter general, no requiere la condición de interesado, pudiendo ser denunciante cualquier persona, que tiene por tanto, la posibilidad de poner en conocimiento del órgano administrativo competente, la existencia de un determinado hecho que pudiera constituir infracción administrativa, siendo en la fase de actuaciones previas cuando por parte de la Agencia se procede a analizar la veracidad de los hechos denunciados, y en base a las mismas opta por iniciar, de oficio, expediente sancionador o archivar las mismas.

En el presenta caso las actuaciones inspectoras fueron promovidas en base al informe remitido por el Equipo Central Operativo de la Jefatura del Servicio de Protección de la Naturaleza de la Guardia Civil, que actúa por tanto en calidad de denunciante.

III

Se aduce por la entidad denunciada la caducidad de las actuaciones previas por el transcurso de más de doce meses desde que tuvo entrada la denuncia hasta que ha sido notificado el acuerdo de inicio del procedimiento sancionador.

En el caso que nos ocupa no se ha producido la caducidad del periodo de actuaciones previas de investigación, teniendo en cuenta la fecha de entrada del escrito de denuncia: 28/12/09 y la fecha del acuerdo de inicio: 16/12/10. Sin que pueda considerarse la existencia de unas dilaciones indebidas en dicho trámite, al existir una serie de motivaciones que justifican las mismas.

La jurisprudencia del Tribunal Constitucional (SSTC 324/1994, de 1 de diciembre y73/1992, de 13 de mayo, entre otras) ha admitido que, en el ámbito del derecho a la tutela judicial efectiva, el artículo 24.2 de la Constitución incorpora un derecho con contenido propio y específico, como es el derecho a un proceso sin dilaciones indebidas que se refiere "(...) no a la posibilidad de acceso a la jurisdicción ni a la obtención práctica de una respuesta jurídica a las pretensiones formuladas, sino a una razonable dimensión temporal del procedimiento necesario para resolver y ejecutar lo resuelto" (STC 324/1994, antes citada).

La vigencia de este derecho se ha vinculado, en particular, al ámbito de los procesos penales cuyas garantías tienen, según el propio Tribunal Constitucional, una íntima relación con los procedimientos administrativos sancionadores.

Según esta jurisprudencia el concepto de "dilaciones indebidas" es, pues, un "concepto jurídico indeterminado o abierto" (STC 36/1984), que ha ido perfilándose por el propio Tribunal atendiendo a las circunstancias específicas de cada caso admitiéndose como criterios que perfilan su contenido, entre otros, "los márgenes ordinarios de duración de litigios del mismo tipo" y "la consideración de los modos disponibles" (STC 324/1994).

Se reconoce, así, la posibilidad de que no se aprecien "dilaciones indebidas" cuando concurran causas objetivas que justifiquen un retraso coyuntural e involuntario por parte del órgano que ha de resolver relacionadas con los medios disponibles, máxime si estas circunstancias se producen en un marco en el que "los márgenes de duración de litigios del mismo tipo" sean homogéneos.

Las denuncias de los ciudadanos que tienen por objeto el ejercicio de la potestad sancionadora atribuida a la AEPD por la LOPD, la LSSI y la LGT han tenido un crecimiento exponencial en los últimos años como acreditan sus Memorias anuales.

Así, entre 2003 y 2007, la actividad de la AEPD se ha incrementado un 120,03% en las actuaciones previas de inspección; un 224,03% en los procedimientos por infracción de la LOPD iniciados y un 194,30% en los resueltos; un 57,74% en los procedimientos de tutela de derechos iniciados y un 56,93% en los resueltos y un 162,38% en las resoluciones de archivo de las actuaciones.

Todo ello con unos recursos humanos que han pasado de 35 a 58 personas (Δ65%) en el mismo período.

Asimismo es relevante resaltar que en 2008 se acelera la actividad de la Agencia tanto en lo que se refiere a iniciación como a resolución de procedimientos sancionadores en su ámbito competencial.

Así, en comparación con 2007, debe subrayarse que en 2008 el número de procedimientos sancionadores iniciados con la apertura de actuaciones de inspección ha crecido un 45.5% y el de procedimientos resueltos un 94.1%.

Ambas actividades, es decir, las de inspección –dirigidas a verificar la existencia de base racional para entender producido el hecho infractos e imputárselo a persona determinada de forma que "la decisión de incoar el procedimiento sancionador sea fundada y asentada en sólidas razones que exijan dicha incoación" (SAN de 17 de octubre de 2007, FD 5)- como "garantía encaminada a asegurar el correcto ejercicio de la potestad sancionadora" (SAN citada), y las de instrucción de los procedimientos sancionadores –con las garantías contempladas en el RD 1398/1993, de 4 de agosto, se encuentran indisolublemente unidas en las competencias atribuidas a la Subdirección General de Inspección por el Real Decreto 428/1993, de 26 de mayo, por el que se aprueba el Estatuto de la Agencia de la Protección de Datos (arts. 27 a 29). Hasta el punto de que un incremento exponencial de las actuaciones de inspección, como se ha producido, puede generar dilaciones, considerando los medios disponibles, para la propuesta de iniciación de procedimientos sancionadores o de archivo de las actuaciones por parte de los instructores; dilaciones que responden a causas objetivas, aunque sean coyunturales, y comunes a la duración de los litigios del mismo tipo, pues la especificidad de las funciones de la AEPD como entidad independiente de derecho público para la tutela del derecho fundamental a la protección de datos no resulta fácilmente comparable con otros órganos administrativos por lo que el punto de comparación debe referirse, a la menos inicialmente, al conjunto de los procedimientos tramitados por la AEPD.

Las consideraciones sobre el carácter coyuntural de la situación descrita se fundan en razones objetivas.

Por una parte porque a lo largo de 2007 han tenido lugar incrementos de los medios adscritos a la Subdirección General de Inspección que ascienden a un total de 20 personas, lo que supone un incremento del 41% sobre las dotaciones del año 2006.

De otro, porque el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, aprobado por Real Decreto 1720/2007, de 21 de diciembre, establece que las actuaciones previas de inspección "tendrán una duración máxima de 12 meses a contar desde la fecha de la denuncia", la petición razonada de otro órgano o el acuerdo del Director de la AEPD.

Transcurrido dicho plazo "sin que se haya dictado y notificado acuerdo de inicio de procedimientos sancionador [se] producirá la caducidad de las actuaciones previas". Con lo que la norma de desarrollo reglamentario ha limitado el plazo temporal para la realización de actuaciones inspectoras incrementando las garantías de los responsables de ficheros de tratamientos.

En el presente caso se han desarrollado las actuaciones previas de inspección y las conexas de iniciación del procedimiento por infracción de la LOPD conforme a los fundamentos jurídicos que se han expuesto.

La Sentencia de la Audiencia Nacional de 19/11/2008, señala, en su Fundamento de Derecho Tercero, lo siguiente:

"En el presente supuesto, y si bien transcurrió también un plazo excesivo de paralización de las actuaciones iniciadas en la Agencia tras la denuncia presentada (de casi año y medio), paralización que tuvo lugar en dicha fase de "diligencias previas" , resulta sin embargo que las alegaciones de la defensa de la Administración han resultado acreditadas mediante la documentación adjuntada. El importantísimo aumento del volumen de trabajo en la AEPD, que se prueba mediante la referida documentación, necesariamente hace quebrar, en el caso, el presupuesto o elemento básico para entender existente tal Fraude de Ley, cual es la utilización de la institución de dichas diligencias previas con fines torticeros o antijurídicos. Lo anterior puesto que ha quedado probado que concurre un motivo que, si bien no justifica tal paralización de la fase previa, si al menos excluye que pueda conceptuarse la misma como fraudulenta, al no ser posible sostener, dado el llamativo incremento del número de asuntos registrados y resueltos por la AEPD, que la demora y paralización, y en definitiva, la prolongación de la duración de las repetidas actuaciones preliminares responda a la intención antijurídica de evitar la caducidad del expediente sancionador. Razones que conllevan que la anterior doctrina de la Sala no pueda ser apreciada en el caso, al que tampoco resulta de aplicación el plazo máximo de doce meses de duración que el artículo 122 del RD 1720/2007, de 21 de diciembre, prevé en la actualidad para dichas "actuaciones previas", tomando en consideración que tal norma reglamentaria solo es de aplicación a actuaciones iniciadas con posterioridad a su entrada en vigor (es decir, a partir del 19 de abril de 2008)".

IV

El art. 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"Seguridad de los datos:
Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados."

El Art 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo

que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:
1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

La ley Orgánica de Protección de Datos (en lo sucesivo LOPD), traspuso al ordenamiento interno el contenido de la Directiva 95/46. En el art. 32.1 de la citada Directiva se daba un plazo de tres años desde la adopción de la misma para la aprobación de las disposiciones legales que dieran cumplimiento a lo establecido en ella. Plazo que se extendía hasta los 12 años en relación a "el tratamiento de los datos que ya se encuentran incluidos en ficheros manuales en la fecha de entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva". En virtud de ello la disposición adicional primera de la LOPD establece un plazo de 12 años para la adecuación a la ley de los ficheros y tratamientos no automatizados, plazo que finalizó en octubre de 2007.

V

La LOPD en su artículo 1 dispone que "la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

El artículo 2.1 de la misma ley orgánica establece: "1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados".

El artículo. 3 de la LOPD establece las definiciones de responsable de fichero o tratamiento, de encargado de tratamiento y de cesión de datos:

"d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento
…...
g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento
……
I) Cesión o comunicación de datos: toda revelación de datos realizada a la persona distinta del interesado."

La vigente LOPD atribuye la condición de responsables de las infracciones a los responsables de los ficheros (art. 43), concepto que debe integrarse con la definición que de los mismos recoge el artículo 3.d), arriba citado, que incluye en el concepto de responsable tanto al que lo es del fichero como al del tratamiento de datos personales. En el presente caso, Atocha Ginecológica SL es responsable de los ficheros y tratamientos, derivados de su actividad laboral, y en conformidad con las definiciones legales está sujeto al régimen de responsabilidad recogido en el Título VII de la LOPD.

VI

El artículo 9 de la LOPD, dispone:

"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 la alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, 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."

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de "fichero" y "tratamiento" contenidas en la LOPD.

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso, –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

La documentación encontrada entra en la consideración de documentación en soporte papel, contiene datos personales, debiéndosele aplicar las medidas de seguridad previstas reglamentaria a este tipo de ficheros y que han sido contempladas en el documento de seguridad de la denunciada.

La entidad denunciada es un hospital perteneciente al Grupo ADESLAS, no obstante en el mismo se atienden pacientes pertenecientes a diferentes sociedades médicas así como consultas privadas. Cuenta con un fichero denominado PACIENTES, inscrito en el Registro General de Protección de Datos, con el código ###COD.1, descrito como REGISTRO OBLIGATORIO DE PACIENTES PARA CONFECCION HISTORIA CLINICA Y DATOS ADMINISTRATIVOS, donde se incluyen todos los datos de los pacientes que son atendidos en el Centro. Los documentos utilizados por el centro cuentan con el anagrama del mismo en el encabezamiento, así como la denominación, dirección postal y número de fax.

Según el relato de los hechos fue una productora de televisión, "Cuarzo producciones S.L." la que puso en conocimiento de Dirección General de la Policía y la Guardia Civil (SEPRONA), supuestas irregularidades en materia de gestión de residuos biosanitarios en que pudieran hallarse implicadas diversas clínicas, entre las que se encontraba, sacados a la luz en el transcurso de un reportaje de investigación. En el Acta de Inspección levantada por los Inspectores de esta Agencia ante Cuarzo Producciones, el representante de la productora manifestó que: " Durante el periodo comprendido entre 15 de septiembre y 15 de octubre de 2009, la Productora comenzó la realización de un reportaje de investigación sobre gestión de residuos biosanitarios en diferentes clínicas de Andalucía, entre las clínicas investigadas se encuentra el Sanatorio Nuestra Señora de la Salud de Granada, en el cual se detectó que dicha clínica depositaba bolsas con residuos en un contenedor ubicado en la vía pública, en el que depositaban las bolsas de basuras los vecinos de las viviendas de la zona".

Esta documentación, que fue entregado por la productora a los inspectores de la Agencia consta de:
- Solicitudes de análisis clínicos
- Imágenes de varias ecografías.
- Varios documentos con etiquetas con los datos de los pacientes
- Escrito de remisión a un Juzgado con relación a un paciente atendido en el servicio de Urgencias.
- Cinco o seis juegos de etiquetas de varios pacientes

Parte de esa documentación aparecía troceada y ha sido reconstruida, pero el hecho de poder haber realizado dicha reconstrucción con relativa facilidad demuestra que no se había procedido a su destrucción completa de modo que hubiese sido imposible su recuperación posterior.

Se manifiesta por la entidad denunciada que "toda la documentación mostrada y especificada, pertenecen a una misma zona del Centro (Consultas externas), donde existen papeleras para uso de los pacientes, por lo que la documentación mostrada que correspondería a los pacientes ha podido ser depositada por ellos en las mismas. En ningún se deposita documentación del SANATORIO ni ningún tipo de residuo, fuera de los contenedores que se encuentran en el recinto de este Centro, los cuales son recogidos todos los días por los Servicios municipales", en el supuesto de que esto fuera así, que toda la documentación encontrada hubiese sido tirada a las papeleras por los pacientes o facultativos de la entidad, debería haberse asegurado su destrucción al tener datos de carácter personal, algunos de ellos con la consideración de especialmente protegidos.

La documentación localizada dentro de un contenedor situado en la vía pública, y

procedente de la entidad denunciada, entra en la consideración de documento de trabajo, incorporando información derivada de un fichero automatizado, que contiene datos personales, debiéndosele aplicar las medidas de seguridad previstas reglamentaria a este tipo de ficheros. Existe pues un tratamiento de datos, volcándose en formato papel una información derivada de ficheros automatizados, que contiene datos de carácter personal. En consecuencia, deberían de haberse adoptado, por parte de la entidad denunciada, las medidas suficientes para impedir el acceso a la información contenida en los mismos, así como su posible recuperación posterior

Debe tenerse en cuenta las obligaciones específicas que se establecen en los artículos 108 (custodia de soportes) y 112 (copia y reproducción de documentos) del RD 1720/07 por el que se aprueba el Reglamento de Desarrollo de la LOPD. Debe deducirse que los criterios de archivo deben garantizar la correcta conservación de los documentos, la localización y consulta de la información, y que mientras la documentación con datos de carácter personal no se encuentra archivada, por que se encuentre en un proceso de tramitación, la persona que se encuentre a cargo de la misma deberá custodiarla e impedir que pueda ser accedida por persona no autorizada.

De los hechos probados en este procedimiento, se deduce que el Sanatorio de Nuestra Señora de la Salud en su calidad de responsable del tratamiento, debió adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información de carácter personal que contenían dichos documentos. Tales medidas no fueron adoptadas totalmente en el presente caso, como lo acredita el hecho que dicha documentación fuese recuperada por un tercero, al estar dentro de un contenedor situado en la vía pública. Esta necesidad de especial diligencia en la custodia de la documentación ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: "Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor.

Se alega por parte de la denunciada que cuenta con una normativa de seguridad relativa a la destrucción de la documentación con datos de pacientes y que no es incluida en las historias clínicas. Además de una serie de medidas y medios técnicos para la destrucción de la documentación, existiendo máquinas destructoras de papel en diversos departamentos de Centro. Al mismo tiempo existen contenedores de papel cerrados con llave, en los que se puede depositar documentación sin destruir. Dichos contenedores son recogidos periódicamente una empresa de prestación de servicios. Dichas circunstancias, sin perjuicio que deban tenerse en cuenta a la hora de graduar la sanción no exonera la responsabilidad de la entidad denunciada, en base a la interpretación dada por la Audiencia Nacional, en la recurso 559/2007, que desestimaba el recurso de una entidad basado en la existencia de responsabilidad de unos de sus empleados:

"Es cierto que dicha entidad bancaria acredita el cumplimiento de las medidas de seguridad, tanto en sus sucursales, como respecto de su personal, en los términos exigidos por la LOPD, y también es cierto que fue un empleado de dicha entidad el que

provocó los hechos ahora sancionados. Más esta Sala ha declarado con reiteración, en las sentencias reseñadas en el fundamento jurídico anterior e igualmente en la SAN de 14-2-2007 (Rec. 229/2005 , entre otras) que no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Así, de nada sirve que se aprueben unas instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales si luego no se exige a los empleados del banco la observancia de aquellas instrucciones. Por lo que necesariamente te ha de concluir que… debió adoptar las medidas necesarias para impedir cualquier recuperación por terceros no autorizados de la información reservada a la que tuvo acceso la empresa de limpieza, y al no efectuarlo así, no observó la diligencia necesaria, pues de otro modo no se explica que un importante volumen de documentos de uso interno de la entidad (a la denuncia se acompañaba una gran caja), en muchos de los cuales figuraban datos personales, fueran a parar a manos de tal concesionaria de la recogida de basura"

VII

El hecho constatado en el presente procedimiento, relativo a la aparición de documentación procedente de la entidad denunciada en un contenedor situado en la vía pública supone una inobservancia del deber de adoptar las medidas de seguridad pertinentes por parte de la responsable del tratamiento.

El artículo 44.3 h) califica como infracción grave: "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". De acuerdo con los fundamentos anteriores, se deduce que por parte de Sanatorio de Nuestra Señora de la Salud se ha producido una vulneración de la de seguridad de los datos, que ha tenido como consecuencia que los datos personales pudieran ser vistos por un tercero, infracción que procede calificarla en el grado señalado.

La exigencia de la "culpabilidad" deriva de lo que señala el artículo 130 de la Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Publicas y del Procedimiento Administrativo Común – LRJPAC- cuando dice que: "Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia".

Si bien en materia sancionadora rige el principio de culpabilidad, la expresión "simple inobservancia", del art. 130.1 de la Ley 30/92, permite la sanción por inobservancia del deber de cuidado. Existe una obligación de resultado, que no se ha cumplido al haberse encontrado documentación procedente de ese centro hospitalario en un contenedor de basuras accesibles a terceros, de la que se desprende una falta de negligencia del responsable del tratamiento, obligado a implementar las medidas de seguridad.

VIII

El artículo 10 de la LOPD establece que: "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".

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que

intervenga en cualquier fase del tratamiento. Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así el Tribunal Superior de Justicia de Madrid ha declarado en su Sentencia de 19 de julio de 2001: "El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)".

En este sentido, la sentencia de la Audiencia Nacional de fecha 18 de enero de 2002, recoge en su Fundamento de Derecho Segundo, y tercer párrafo: "El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable –en este caso, la entidad bancaria recurrente- de los datos almacenados –en este caso, los asociados a la denunciante- no puede revelar ni dar a conocer su contenido teniendo el "deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo" (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE. En efecto, este precepto contiene un "instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, 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" (STC 292/2000). Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino" (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, "es decir, el poder de resguardar su vida privada de una publicidad no querida"

Ahora bien la obligación impuesta por el artículo 10 debe entenderse como una obligación de resultado, donde lo relevante, tal como lo ha entendido la Audiencia Nacional, entre otras en la sentencia de 18/06/09, es que se llegue a producir la divulgación de un secreto, no siendo relevante (a los efectos de la violación del deber de secreto), que exista o no una omisión de las medidas de seguridad. En el caso que nos ocupa, la entidad denunciada es responsable de la custodia de la documentación relativa a sus pacientes, que ha sido recabada por personas de la productora Cuarzo que vieron los documentos y pegaron los que estaban rotos, existiendo pues, una omisión del deber de secreto, produciéndose una ausencia de confidencialidad, por lo que se considera que se ha cometido una infracción del transcrito artículo 10 de la LOPD.

El artículo 44.3 d) califica como infracción grave: "La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley". De acuerdo con los fundamentos anteriores, se deduce que por parte de Sanatorio de Nuestra Señora de la Salud se ha producido una vulneración de la de seguridad de los datos, que ha tenido como consecuencia que los datos personales pudieran ser vistos por un tercero, infracción que procede calificarla en el grado señalado.

X

El hecho constatado de la difusión de datos personales especialmente protegidos fuera del ámbito del denunciado, establece la base de facto para fundamentar la imputación de las infracciones de los artículos 9 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto en el que un mismo hecho deriva en dos infracciones, dándose la circunstancia que la comisión de una implica necesariamente la comisión de la otra. Esto es, si un documento interno que contiene información sobre datos personales sale del ámbito de la entidad responsable de su confidencialidad, se está produciendo un incumplimiento de las medidas de seguridad exigidas a dicho responsable que, a su vez, deriva en una vulneración del deber de secreto.

Por lo tanto, aplicando el artículo 4.4 del Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora que señala que "en defecto de regulación específica establecida en la norma correspondiente, cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida", procede subsumir ambas infracciones en una. Dado que, en este caso, se ha producido una vulneración de las medidas de seguridad, calificada como grave por el artículo 44.3.h) de la LOPD y también un incumplimiento del deber de guardar secreto referido a datos especialmente protegidos, calificado como grave en el artículo 44.3.d) de la misma norma, procede imputar únicamente la infracción del artículo 9 de la LOPD.>>>>

III

Por lo tanto, en el presente recurso de reposición, ***HOSPITAL NTRA. SRA. DE LA SALUD*** no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por ***HOSPITAL NTRA. SRA. DE LA SALUD*** contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 10 de junio de 2011, en el procedimiento sancionador PS/00698/2010.

SEGUNDO: NOTIFICAR la presente resolución a la entidad ***HOSPITAL NTRA. SRA. DE LA SALUD***.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa, se podrá interponer en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto según lo previsto en el artículo 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta del referido texto legal.

Madrid, 16 de septiembre de 2011

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: José Luis Rodríguez Álvarez