Procedimiento nº.: PS/00084/2015

ASUNTO: Recurso de Reposición Nº RR/00671/2015

Examinado el recurso de reposición interpuesto por la entidad ***D. A.A.A.*** contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00084/2015, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 20 de julio de 2015, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00084/2015 , en virtud de la cual se imponía a la entidad D. ***A.A.A.***, una sanción de 6.000 €, por la vulneración de lo dispuesto en el artículo 9 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 45.5 y 4 de la citada Ley Orgánica.

Dicha resolución, que fue notificada al recurrente en fecha 28/7/15, 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/00084/2015, quedó constancia de los siguientes:

<<<<< 1º Consta denuncia presentada con fecha 6/3/14 por la Agencia escrito de la AGENCIA TRIBUTARIA-DELEGACION ESPECIAL DE ILLES BALEARES, *poniendo de manifiesto irregularidades en la protección de datos relativos a la salud de sus pacientes por parte de D.* ***A.A.A.*** *(NIF* ***B.B.B.****).*

2º Constan los siguientes hechos puestos en manifiesto por el Acta de Inspección levantada el día 19/2/14 y que se ha aportado junto al escrito de denuncia:

** Que el Sr.* ***A.A.A.*** *viene ejerciendo la actividad de odontólogo en el local sito en la calle* ***D.D.D.*** *del municipio de* ***C.C.C.****.*

** Mediante diligencia de constancia de hechos de fecha 28 de octubre de 2013, esta Inspección requirió al Sr.* ***A.A.A.*** *que aportara, entre otra, la siguiente documentación:*

- Que indicara el número de visitas, fechas y tratamientos realizados a cada uno de ellos, durante los años 2011 y 2012, según consta en el historial médico de cada paciente. Con el fin de garantizar el anonimato de los pacientes en cumplimiento de la Ley de Protección de Datos, cada paciente debía ser identificado exclusivamente según el número de su historial clínico.

- Que dicha información es necesaria para determinar el volumen de ingresos obtenidos por el contribuyente.

- Mediante diligencia de constancia de hechos de fecha 11 de noviembre de 2013, el representante del contribuyente manifestó a esta Inspección, en relación a los historiales médicos, lo siguiente:

- Que como consecuencia de una tormenta eléctrica, que se produjo en el mes de septiembre del año 2013, se rompió el ordenador utilizado en la consulta profesional. Este tuvo que ser

reparado, realizándose el cambio de placa base, disco duro y fuente de alimentación e instalación de Software. Debido a este daño, desapareció toda la información relativa a los historiales médicos de cada uno de los pacientes atendidos por el contribuyente. El único justificante, que posee el contribuyente, para justificar tal manifestación es la fotocopia de la factura de reparación del ordenador y varios email enviados a la compañía aseguradora.

- Que hasta la fecha, el contribuyente no ha comunicado la desaparición de los historiales médicos a persona alguna.

- Mediante diligencia de constancia de hechos de fecha 26 de noviembre de 2013, el representante del contribuyente manifestó a esta Inspección lo siguiente:

- En relación a los historiales médicos se ratifica en la manifestación realizada en la anterior diligencia: Que como consecuencia de una tormenta eléctrica se rompió el ordenador donde constaba toda la información relativa a los historiales médicos de cada uno de los pacientes atendidos por el contribuyente hasta el mes de septiembre del año 2013 desapareciendo dicha información y sin que tuviera copia de seguridad de la misma. La pérdida de dicha información no ha sido comunicada a terceras personas.

.- Mediante diligencia de constancia de hechos de fecha 13 de diciembre de 2013, el actuario se persono en el local donde el Sr. ***A.A.A.*** *ejerce su actividad profesional, y en relación a los historiales médicos de sus pacientes, el Sr.* ***A.A.A.*** *manifestó lo siguiente:*

- Se ratificaba en la manifestación realizada por el representante del contribuyente: Que como consecuencia de una tormenta eléctrica se rompió el ordenador donde constaba toda la información relativa a los historiales médicos de cada uno de los pacientes atendidos por el contribuyente hasta el mes de septiembre del año 2013 desapareciendo dicha información y sin que tuviera copia de seguridad de la misma y que la pérdida de toda la documentación relativa a los historiales médicos de sus pacientes no fue comunicada a terceras personas >>>>>

TERCERO: ***D. A.A.A.*** ha presentado en fecha 14/8/15, en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo, básicamente, en el documento en que se basa la resolución sancionadora por pérdida de información se aprecia la falta de una página de dicho informe que indica "*que el contribuyente puede reconstruir los historiales médicos los pacientes en base a las facturas emitidas por el sujeto pasivo".* Considerando por tanto que no ha habido fuga de información porque todos los datos son recuperables desde los soportes físicos disponibles.

Se manifiesta que el sistema de gestión de información contaba con un soporte de respaldo (back up) que se ejecutaba de forma automática una vez por semana en un disco duro y que se vio afectado por el incidente.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso la Directora 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

En relación con las manifestaciones efectuadas por ***D. A.A.A.***, reiterándose básicamente, en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho del (II al VI) ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

<<<<< II

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, D. ***A.A.A.*** *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.*

III

Se analiza en el presente procedimiento si la desaparición de documentación, cuya custodia era responsabilidad del denunciado, (con datos de carácter personal, que además tiene el carácter de especialmente protegidos por contener datos de salud), sin que tuviera copia de seguridad de los mismos, supone una omisión del deber de adoptar o de observar las medidas técnicas y organizativas que garanticen las seguridad de dichos datos, contempladas en el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RD 1720/2007)

El art. 7 de la Ley 41/2002 establece:

"El derecho a la intimidad:

1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la ley.

2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes"

El art 16 detalla los posibles usos que podrán realizarse de la historia clínica, con independencia del soporte en que se encuentre recogida
El artículo 17.5 y 6 de la citada norma establecen:

5. Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen

6. "Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y en general, por la Ley Orgánica 15/99, de Protección de Datos de Carácter Personal."

Los hechos denunciados entran en el campo de aplicación de la LOPD, teniendo en cuenta la remisión que el art. 17.6 de la ley 41/2002 realiza a la LOPD en lo relativo a las medidas técnicas de seguridad que han de cumplirse, y la obligación de custodia de la documentación clínica contemplada en el artículo 17.5.

Se desprende, además, de lo establecido en los mencionados preceptos, la existencia de un deber de conservación de la historia clínica por parte del facultativo, y la obligación de la conservación de la información médica (que al tratarse de datos de salud tienen la consideración de especialmente protegidos), al menos el periodo mínimo establecido por la ley, sin perjuicio en todo caso de lo que pidiera establecer la normativa autonómica.

IV

El art 7.3 de la LOPD establece:

"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"

En la LOPD no se define que se entiende por datos de salud, por lo que para precisar este concepto se acude a las normas internacionales y comunitarias, así en el apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa, se define datos de salud como "Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo, pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido". Se deduce por tanto que el denunciante trata datos de salud de personas perfectamente identificables, estando obligado a la conservación de la información médica de los pacientes, información que posteriormente pasará a engrosar su historia clínica aunque esta no sea custodiada por el denunciado

El artículo 7.6 introduce una excepción al principio del consentimiento: exceptuándolo cuando el tratamiento de los datos resulte necesario para la prevención o diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional,

V

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 LOPD, traspuso al ordenamiento interno el contenido de la Directiva 95/46. En el artículo 9 de la citada LOPD se dispone lo siguiente:

"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".

El trascrito artículo 9 de la LOPD establece el "principio de seguridad de los datos" imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el "acceso no autorizado" por parte de terceros.

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.

En lo que respecta al concepto de "fichero" el artículo 3.b) de la LOPD lo define como "todo conjunto organizado de datos de carácter personal", con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la "comunicación" o "consulta" de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Y el artículo 3.a) de dicha Ley añade que se entenderá por datos de carácter personal "cualquier

información concerniente a personas físicas identificadas o identificables". En este mismo sentido se pronuncia el artículo 2 a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos profesionales y a la libre circulación de estos datos, que dispone "toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Para completar el sistema de protección en lo que a la seguridad afecta, el artículo 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros "...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

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.

Partiendo de tales premisas, procede analizar a continuación las previsiones contenidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, para garantizar la seguridad de los datos personales y, en concreto, que no se produzcan accesos no autorizados.

De acuerdo con lo establecido en dicho Reglamento, las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104, del Reglamento de desarrollo de la LOPD.

Los artículos 91 y 92 del citado Reglamento, aplicables a todos los ficheros y tratamientos automatizados, establecen:

"Artículo 91. Control de acceso.
1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá

conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio".

Este artículo desarrolla las previsiones que deberá establecer el responsable del fichero para garantizar que los usuarios con acceso a datos personales o recursos, por haber sido previamente autorizados, sólo puedan acceder a tales datos y recursos. Para ello es necesario que se implanten mecanismos de control para evitar que un usuario pueda acceder a datos o funcionalidades que no se correspondan con el tipo de acceso autorizado para el mismo, en función del perfil de usuario asignado.

Y el citado artículo 92 del Reglamento establece:

Artículo 92. Gestión de soportes y documentos.
"4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior".

En definitiva, el denunciado está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para los ficheros de la naturaleza indicada, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros.

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, porque 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.

En particular es de aplicación al caso que nos ocupa el art. 102 del ya citado RLOPD que establece:

Artículo 102. Copias de respaldo y recuperación.

"Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación".

*Dicho artículo establece, para los ficheros y tratamientos automatizados calificados de nivel alto, la obligación de conservar una copia de respaldo de los datos y de los procedimientos que se deberán aplicar, en el caso de ser necesaria su recuperación, en un lugar diferente de aquel en que se encuentran los equipos informáticos que los trate**n**.*

Sin embargo, ha quedado acreditado en el procedimiento que se incumplieron estas obligaciones, en base a lo declarado por el denunciado que ha manifestado que en "en el mes de

septiembre de 2013 se rompió el ordenador utilizado en la consulta profesional…debido a este daño desapareció toda la información relativa a los historiales médicos"

En consecuencia, se desprende que D. ***A.A.A.*** *no había garantizado la seguridad de los datos personales (historias clínicas) de sus pacientes, realizando al menos una copia de respaldo de las mismas que garantizase su conservación, lo que supone la comisión de una infracción del artículo 9.1 de la LOPD,*

En esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deban salvaguardar, entre otras cosas, la integridad y custodia de dicha información. Esta necesidad de especial diligencia en la custodia de la información por el responsable 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 deduce por consiguiente que D. ***A.A.A.*** *debió por ello, adoptar las medidas necesarias (realización de copia de respaldo) que evitaran la pérdida de las historia clínicas de sus pacientes de cuya custodia era responsable. Esa falta de diligencia supone una inobservancia del deber de adoptar las medidas de seguridad pertinentes por parte del denunciado como responsable 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".

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 borrado documentación médica cuya responsabilidad de conservación corresponde al facultativo denunciado de la que se desprende una falta de negligencia del responsable del tratamiento, obligado a implementar las medidas de seguridad pertinentes.

VI

El artículo 45 apartados 2,4 y 5 de la LOPD dispone:

"3. Las infracciones graves serán sancionadas con multa de 60.101,21€ a 300.506,05 €.

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para

determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora"

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate".

En relación a los hechos acreditados y su valoración jurídica, debe tenerse en cuanta, en primer lugar, lo establecido en el art. 45.5, que trata de hacer efectivo hasta sus últimas consecuencias el principio de proporcionalidad, mediante la aplicación de la sanción correspondiente relativa a la escala inferior y ello cuando se aprecie disminución de la culpabilidad del imputado o de la antijuricidad del hecho. Estos dos criterios no son sino criterios jurídicos indeterminados que deben concretarse en cada supuesto en el que se pretenda su aplicación. Debe tenerse en cuenta la interpretación establecida la Audiencia Nacional, en sus Sentencias, entre otras, de 24/05/2002 y 16/02/2005, "la presente regla debe aplicarse con exquisita ponderación y solo en los casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas atendidas las circunstancias del caso concreto, de forma que repugne a la sensibilidad jurídica, siempre guiada por el valor justicia, la imposición de la sanción correspondiente al grado. Lo cual insistimos puede darse, por excepción, en casos muy extremos y concretos."

Debe valorarse para la aplicación de dichas circunstancias al presente caso, que puede apreciarse una cualificada disminución de la culpabilidad del imputado como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 5, por lo que debe entenderse que operan dichas circunstancias atenuantes de la responsabilidad; aplicadas ya por esta Agencia, en otros procedimientos relativos a incumplimiento de las medidas de seguridad.

En segundo lugar, el art. 45.4 recoge una serie de criterios relativos a la aplicación del principio de proporcionalidad en la graduación del importe de la sanción, según las indicaciones del art. 131.3 de la LRJPAC (Ley 30/92 de 26 de noviembre). Pues bien la secuencia de hechos expuesta en esta resolución, deben aplicarse los siguientes criterios para fijar la sanción:

a) El carácter continuado de la infracción. (En este caso se trata de un hecho puntual)
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza. (No existe reincidencia)
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de un error o descuido que concluyó con la eliminación de una documentación con datos de carácter personal como si fuera material a desechar.

Teniendo en cuenta los hechos probados a lo largo de este procedimiento, y los criterios definidos por la legislación con objeto de adecuar la sanción en base al principio de proporcionalidad, se considera procedente, en este caso, imponer una sanción en 6.000 euros por la infracción cometida. >>>>>>

III

Por lo tanto, en el presente recurso de reposición, ***D. A.A.A.*** no ha aportado nuevos hechos o

argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada. Debe tenerse en cuenta que el art 102 del RLOPD exige, para los ficheros y tratamientos automatizados calificados de nivel alto, la obligación de conservar una copia de respaldo de los datos y que tiene que estar en un lugar diferente de aquel en que se encuentran los equipos informáticos que los traten. Circunstancias que no se han producido en este caso y constituyen el hecho sancionable.

Vistos los preceptos citados y demás de general aplicación,

la Directora de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por ***D. A.A.A.*** contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 20 de julio de 2015, en el procedimiento sancionador PS/00084/2015.

SEGUNDO: NOTIFICAR la presente resolución a la entidad ***D. A.A.A.***

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.

Mar España Martí
Directora de la Agencia Española de Protección de Datos