Procedimiento Nº: A/00029/2015

RESOLUCIÓN: R/01580/2015

En el procedimiento A/00029/2015, instruido por la Agencia Española de Protección de Datos a Doña ***A.A.A.***, vista la denuncia presentada por el Gerente del Departamento de Salud Valencia LA FE, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 11 de julio de 2014, se recibió en esta Agencia un escrito remitido por el Gerente del Departamento de Salud Valencia LA FE, en el que pone de manifiesto que, en junio de 2014 se realizó entrega en la Asesoría Jurídica del Hospital LA FE de documentación correspondiente a pacientes del Hospital, por parte de Don ***B.B.B.***, manifestando que dicha documentación se encontraba en su domicilio, habiendo sido dejada allí por su ex pareja, Doña ***A.A.A.***. Asimismo, entregó copia de documentación que previamente le había remitido a su ex pareja al domicilio de los padres, y que también se encontraba en el domicilio.

Después de una primera valoración, podría tratarse de elementos de descarte de la historia clínica que se generan en el procedimiento de expurgo que se realiza con anterioridad al proceso de integración, ordenación, digitalización y archivado de historia clínica, cuyos Servicios tiene contratados dicho Hospital con la entidad INDRA BMB SERVICIOS DIGITALES, S.L.U (en la actualidad INDRA BPO SERVICIOS, S.L.U)

Asimismo, manifiestan que según el apartado 5 del Pliego de Condiciones (Control y mantenimiento), el punto 5.1 Confidencialidad LOPD, contempla expresamente todas las medidas de seguridad que se deben aplicar, según consta en la copia del mismo aportado a la Agencia por el Gerente del Departamento de Salud Valencia LA FE, así como del contrato suscrito.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. Con fecha 19 de enero de 2015, se realiza inspección en los locales del Centro de Archivo y Logística de la Generalitat Valenciana, donde presta sus servicios la empresa INDRA BPO SERVICIOS, S.L.U (antes INDRA BMB SERVICIOS DIGITALES, S.L.U.), poniéndose de manifiesto los siguientes hechos durante la inspección:

    1.1. Con fecha 10 de diciembre de 2013, se suscribe el contrato de prestación de Servicios, entre La Agencia Valenciana de Salud y la entidad INDRA BMB SERVICIOS DIGITALES, S.L.U, con la finalidad de digitalización de historias

clínicas y custodia y gestión del archivo en el Departamento de Salud Valencia LA FE. El ámbito de los servicios contratados incluye, el Hospital La FE y sus centros dependientes.

1.2. La entidad Indra BMB Servicios Digitales, S.L.U., sufrió un cambio de denominación con fecha 13 de marzo de 2014, pasando a denominarse INDRA BPO SERVICIOS, S.L.U.

1.3. Dña. ***A.A.A.***, prestó servicios para esta entidad desde el 22 de febrero de 2013 al 30 de mayo de 2014, siendo sus funciones las de "Codificador informático", según consta en su contrato, en el que en su cláusula decimocuarta, consta UN COMPROMISO DE CONFIDENCIALIDAD, donde la trabajadora se comprometa a cumplir con la Normativa a la que obliga la LOPD.

1.4. En el mes de junio de 2014 tuvieron conocimiento de los hechos denunciados a través del Hospital LA FE, desde donde se debió pedir a la trabajadora que devolviera la documentación que obrase en su poder; la Sra. ***A.A.A.*** procedió a la remisión al Hospital, de una certificación de fecha 11 de junio de 2014, en la que manifestaba que la documentación había sido destruida, en el mismo escrito, el padre de la trabajadora DA FE de esta manifestación. Dicha certificación fue remitida a INDRA mediante correo electrónico de fecha 17 de julio de 2014

1.5. El Procedimiento establecido para el tratamiento de las historias clínicas es el siguientes:

1.5.1. Cuando el Hospital LA FE contrata los servicios de INDRA, el archivo de historias clínicas se encontraba en los locales donde se realiza la presente inspección.

1.5.2. INDRA solo realiza la digitalización de las historias que son solicitadas desde el Hospital, dicha solicitud puede ser realizada desde los Servicios Médicos directamente, a través de la aplicación o desde La Unidad de Documentación Clínica y Admisión (UDCA), en el caso de que se solicite además la Historia clínica en papel.

En el caso de que se mande la historia en papel solo se entrega a la UDCA, siendo ella la encargada de remitirla al Servicio correspondiente.

1.5.3. La historia a ser digitalizada se encuentra dentro de una carpeta, que dependiendo de su pertenencia son de un color u otro, el operador descarta la documentación que se encuentre deteriorada, así como Hojas de evolución que se encuentren en blanco, y etiquetas, dicha documentación descartada es depositada en unos contenedores metálicos cerrados con candado, que se encuentran en el puesto de trabajo de cada operador.

El resto de la documentación es digitalizada, y depositada posteriormente en una bolsa de plástico con una etiqueta que la identifica, y depositada en el archivo, o enviada al Hospital, en su caso.

1.6. El archivo cuenta con un total aproximado de 1.400.000 historias clínicas, de las cuales unas 330.000 se encuentran en activo y digitalizadas unas 215.000. En la actualidad prestan sus servicios como operadores de digitalización de historias, dos personas, una en turno de mañana y otra de tarde, No obstante

en el momento en que se produjeron los hechos prestaban servicio cuatro personas. En ningún caso está permitida la entrada de bolsos y móviles a los locales donde se encuentran los puestos de trabajo, los cuales deben ser depositados en una sala habilitada al efecto y contigua a dichos locales.

1.7. Se accede a un puesto de trabajo, donde se comprueba:

1.7.1. Verificación de la realización de todo el proceso descrito en el aparato 2.5.

1.7.2. Existencia de varios carteles ubicados en diferentes lugares, donde figura "TODA LO DOCUMENTACION DESECHADA SE DEPOSITARÁ EN LOS CONTENEDORES PARA SU DESTRUCCION".

1.7.3. Existencia de carteles donde se prohíbe la realización de fotografías o grabación de videos.

1.7.4. Existencia de un cartel en la puerta de salida donde figura "ESTA PROHIBIDO EXTRAER DOCUMENTACIÓN DEL CENTRO"

1.7.5. Existencia de un cartel donde figura "ESTA PROHIBIDO ALMACENAR DOCUMENTACIÓN FUERA DE LAS ZONAS HABILITADAS AL EFECTO".

1.7.6. Existencia de contenedores cerrados con un candado en cada puesto de trabajo.

1.8. INDRA, tiene suscrito un contrato de prestación de servicios con la empresa RECUPERACIONES LA CAÑADA, S.L., con fecha 10 de mayo de 2010, con la finalidad de recogida y destrucción de la documentación recogida en los contenedores. Los contenedores son recogidos semanalmente, haciendo entrega de un certificado de destrucción por cada recogida.

1.9. Se adjuntan a este Acta de inspección ejemplares de las carpetas y documentación similares a la extraída de los locales por la Sra. A.A.A., haciendo entrega de la siguiente documentación, parcialmente anonimizada:

1.10. Etiquetas

1.11. Hoja de evolución en blanco

1.12. Carpetas verdes (Hospital infantil y Hospital maternal)

1.13. Carpeta marrón (Hospital General)

1.14. Carpeta naranja (Hospitalización)

1.15. Carpeta azul (Ambulatoria)

1.16. Carpeta roja (Rehabilitación).

1.17. Separadores utilizados dentro de las carpetas, etiquetados con el nombre de la especialidad.

1.18. Asimismo, se adjunta a este Acta la siguiente documentación, relativa a seguridad y confidencialidad de la información y que ya fue remitida a la Agencia por esta entidad en su escrito de fecha 22 de diciembre de 2014:

1.19. Copia de las Normas de seguridad de la aplicación denominado MANUAL MEDIDAS SEGURIDAD LOGICA PLATAFORMA MERLIN LA FE de fecha 15 de octubre de 2014.

1.20. Copia de las Normas dadas a los trabajadores con relación a la Protección y

Confidencialidad de los datos.

1.21. Copia del Manual de Formación de Seguridad a los trabajadores.

1.22. Copia del documento elaborado por la empresa al tener conocimiento de la denuncia presentada en el Hospital La Fe de Valencia de la existencia de carpetas de historias clínicas y otra documentación en el domicilio particular de una ex trabajadora, en el documento se detalla lo siguiente:

1.22.1. Dicha documentación debería haber sido expurgada dentro del proceso normal de ejecución de los servicios contratados.

1.22.2. La incidencia se debe a un hecho ajeno a la voluntad de la empresa y aislado, que se produce por la actuación individual de una persona que no ha aplicado los protocolos de seguridad y ha hecho caso omiso a las directrices de seguridad existentes al respecto.

1.22.3. Desde el principio de la prestación del servicio existían un conjunto de medidas de seguridad con el objeto de canalizar el correcto tratamiento de la documentación, así como para evitar el acceso, tratamiento y sustracción de la documentación clínica por parte de terceros no autorizados.

1.22.4. Entre dichas medidas, se encuentra la instalación de contenedores de destrucción confidencial con cerradura, para evitar la extracción de documentación desechada en su interior.

1.22.5. Tras los hechos, se han adoptado un conjunto de acciones con objeto de reforzar las medidas de seguridad ya existentes, entre ellas: la eliminación de la totalidad de las papeleras, la prohibición a los trabajadores de almacenamiento temporal de documentación en sus puestos de trabajo, instalación de cartelería con mensajes recordatorios a los trabajadores, planificación de una nueva acción formativa sobre aspectos relacionados con la LOPD.

TERCERO: Con fecha 5 de febrero de 2015, el Director de la Agencia Española de Protección de Datos acordó someter a trámite de audiencia previa el presente procedimiento de apercibimiento A/00029/2015. Dicho acuerdo fue notificado al denunciante y a la denunciada.

HECHOS PROBADOS

PRIMERO: Con fecha 11 de julio de 2014, se recibió en esta Agencia un escrito remitido por el Gerente del Departamento de Salud Valencia LA FE, en el que pone de manifiesto que, en junio de 2014 se realizó entrega en la Asesoría Jurídica del Hospital LA FE de documentación correspondiente a pacientes del Hospital, por parte de Don ***B.B.B.***, manifestando que dicha documentación se encontraba en su domicilio, habiendo sido dejada allí por su ex pareja, Doña ***A.A.A.***. Asimismo, entregó copia de documentación que previamente le había remitido a su ex pareja al domicilio de los padres, y que también se encontraba en el domicilio.

SEGUNDO: Después de una primera valoración, podría tratarse de elementos de descarte de la historia clínica que se generan en el procedimiento de expurgo que se realiza con anterioridad al proceso de integración, ordenación, digitalización y archivado

de historia clínica, cuyos Servicios tiene contratados dicho Hospital con la entidad INDRA BMB SERVICIOS DIGITALES, S.L.U (en la actualidad INDRA BPO SERVICIOS, S.L.U)

TERCERO: Con fecha 10 de diciembre de 2013, se suscribió un contrato de prestación de Servicios, entre La Agencia Valenciana de Salud y la entidad INDRA BMB SERVICIOS DIGITALES, S.L.U, con la finalidad de digitalización de historias clínicas y custodia y gestión del archivo en el Departamento de Salud Valencia LA FE. El ámbito de los servicios contratados incluye, el Hospital La FE y sus centros dependientes.

CUARTO: Dña. ***A.A.A.***, prestó servicios para esta entidad desde el 22 de febrero de 2013 al 30 de mayo de 2014, siendo sus funciones las de "Codificador informático", según consta en su contrato, en el que en su cláusula decimocuarta, consta UN COMPROMISO DE CONFIDENCIALIDAD, donde la trabajadora se comprometa a cumplir con la Normativa a la que obliga la LOPD.

QUINTO: La Sra. ***A.A.A.*** procedió a la remisión al Hospital, de una certificación, de fecha 11 de junio de 2014, en la que manifestaba que la documentación había sido destruida; en el mismo escrito, el padre de la trabajadora DA FE de esta manifestación. Dicha certificación fue remitida a INDRA mediante correo electrónico de fecha 17 de julio de 2014.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37.g) en relación con el artículo 36 de la LOPD.

II

En este caso, los hechos expuestos, en relación con que una trabajadora se llevase unas carpetas con algunos datos personales, tras su digitalización, podrían suponer la comisión, por parte del mismo, de una infracción del artículo 9.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), según el cual "*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 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",* en relación con lo dispuesto en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, concretamente en los artículos 88, 89, 91 y 92.4, que establecen lo siguiente:

"Artículo 88. El documento de seguridad.

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del

cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal".

"Artículo 89. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.
También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento".

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".

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".

La vulneración de los preceptos citados aparece tipificada como infracción grave en el artículo 44.3.h) de la LOPD, que considera como tal, "*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".*

III

De acuerdo con lo expuesto, se iniciaron actuaciones contra la denunciada por la presunta vulneración del *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, que se tipifica como infracción grave en el artículo 44.3.h) de la LOPD.

Por otra parte, se tuvo en cuenta que la denunciada no ha sido sancionado o apercibido con anterioridad.

En consecuencia, de conformidad con lo establecido en el artículo 45.6 de la LOPD, se acordó someter a la citada entidad a trámite de audiencia previa al apercibimiento, en relación con la denuncia por infracción del artículo 9 de la LOPD.

La disposición final quincuagésima sexta de la Ley 2/2011 de 4 de marzo de Economía Sostenible (BOE 5-3-2011) ha añadido un nuevo apartado 6 al artículo 45 de la Ley 15/1999 de Protección de Datos en lugar del existente hasta su promulgación del siguiente tenor:

"*Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:*

a) que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento".

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado apartado 6. Junto a ello se constata una cualificada disminución de la culpabilidad de la imputada teniendo en cuenta que no consta vinculación relevante de la actividad de la denunciada con la realización de tratamientos de datos de carácter personal, el carácter puntual del hecho y no constan beneficios obtenidos como consecuencia de la comisión de la infracción.

IV

La sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección Primera, recurso 455/2011, de 29/11/2013, analiza el apercibimiento como un acto de naturaleza no sancionadora, como se deduce del fundamento de derecho SEXTO:

"*Debe reconocerse que esta Sala y Sección en alguna ocasión ha calificado el apercibimiento impuesto por la AEPD, en aplicación del artículo examinado, como sanción (SAN de 7 de junio de 2012, rec. 285/2010), y en otros casos ha desestimado recursos contencioso-administrativos interpuestos contra resoluciones análogas a la recurrida en este procedimiento, sin reparar en la naturaleza no sancionadora de la medida expresada (SSAN de 20 de enero de 2013, rec. 577/2011, y de 20 de marzo de 2013, rec. 421/2011). No obstante, los concretos términos en que se ha suscitado la controversia en el presente recurso contencioso-administrativo conducen a esta Sala a las conclusiones expuestas, corrigiendo así la doctrina que hasta ahora venía presidiendo la aplicación del artículo 45.6 de la LOPD*."

Además, la sentencia interpreta o liga apercibimiento o apercibir con el requerimiento de una actuación para subsanar la infracción, y si no existe tal requerimiento, por haber cumplido las medidas esperadas relacionadas con la infracción, no sería apercibimiento, sino archivo como se deduce del fundamento de derecho SEXTO:

"*Pues bien, en el caso que nos ocupa el supuesto concreto, de entre los expresados en el apartado quinto del artículo 45, acogido por la resolución administrativa recurrida para justificar la aplicación del artículo 45.6 de la LOPD es el primero, pues aprecia "una cualificada disminución de la culpabilidad del imputado teniendo en cuenta que no consta vinculación relevante de la actividad del denunciado con la realización de tratamientos de datos de carácter personal, su volumen de negocio o actividad y no constan beneficios obtenidos como consecuencia de la comisión de la infracción", tal y como expresa su fundamento de derecho VII.*

Por ello, concurriendo las circunstancias que permitían la aplicación del artículo 45.6 de la LOPD, procedía "apercibir" o requerir a la denunciada para que llevara a cabo las medidas correctoras que la Agencia Española de Protección de Datos considerase pertinentes, en sustitución de la sanción que de otro modo hubiera correspondido.

No obstante, dado que resultaba acreditado que la denunciada por iniciativa propia había adoptado ya una serie de medidas correctoras, que comunicó a la Agencia Española de Protección de Datos, y que esta había verificado que los datos del denunciante no eran ya localizables en la web del denunciado, la Agencia Española de Protección de Datos no consideró oportuno imponer a la denunciada la obligación de llevar a cabo otras medidas correctoras, por lo que no acordó requerimiento alguno en tal sentido a ésta.

Recuérdese que al tener conocimiento de la denuncia la entidad denunciada, procedió por iniciativa propia a dirigirse a Google para que se eliminara la URL donde se reproducían la Revista y el artículo, a solicitar a sus colaboradores que suprimieran cualquier nombre de sus artículos o cualquier otra información susceptible de parecer

dato personal y que revisaran las citas del área privada de la web para borrar cualquier otro dato sensible, y, por último, a revisar la configuración de los accesos para que los buscadores no tuvieran acceso a las Revistas.

En consecuencia, si la Agencia Española de Protección de Datos estimaba adoptadas ya las medidas correctoras pertinentes en el caso, como ocurrió, tal y como expresa la resolución recurrida, la actuación administrativa procedente en Derecho era al archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la entidad denunciada, pues así se deduce de la correcta interpretación del artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica.

Por el contrario, la resolución administrativa recurrida procedió a "apercibir" a la entidad PYB ENTERPRISES S.L., aunque sin imponerle la obligación de adoptar medida correctora alguna, lo que solo puede ser interpretado como la imposición de un "apercibimiento", entendido bien como amonestación, es decir, como sanción, o bien como un mero requerimiento sin objeto. En el primer caso nos hallaríamos ante la imposición de una sanción no prevista en la LOPD, con manifiesta infracción de los principios de legalidad y tipicidad en materia sancionadora, previstos en los artículos 127 y 129 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en el segundo supuesto ante un acto de contenido imposible, nulo de pleno derecho, de conformidad con lo previsto en el artículo 62.1.c) de la misma Ley."

En el presente caso, consta acreditado que la denunciada destruyó toda la documentación que había sacado de su lugar de trabajo, vulnerando las medidas de seguridad que debía cumplir.

En consecuencia, deben estimarse adoptadas ya las medidas correctoras pertinentes en el presente caso, por lo que debe procederse a resolver el archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la persona denunciada, en aplicación de lo establecido en el artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica.

De acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1.- ARCHIVAR el procedimiento **A/00029/2015** seguido contra Doña ***A.A.A.***, con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con la denuncia por la infracción del artículo 9 de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido 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, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la

notificación de esta resolución, o, directamente 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 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de esta acto, según lo previsto en el artículo 46.1 del referido texto legal.

2.- NOTIFICAR el presente Acuerdo a Doña ***A.A.A..***

3.- NOTIFICAR el presente Acuerdo a INDRA BPO SERVICIOS, S.L.U.

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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos