Expediente Nº: E/01085/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos, en virtud de denuncia presentada por la ASOCIACION EL DEFENSOR DEL PACIENTE (Doña ***B.B.B.***), y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 8 de febrero de 2017, tuvo entrada en esta Agencia de un correo electrónico remitido por la ASOCIACION EL DEFENSOR DEL PACIENTE, en el que informa de las noticias recogidas en la prensa relativas a la aparición de una bolsa de basura con documentación que contiene datos personales. Parece que pertenece a la RESIDENCIA GERIATRICA GERIATROS.

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:

La Consejería de Políticas Sociales y Familia de la Comunidad de Madrid, realizó un informe sobre los hechos denunciados del que se desprende lo siguiente:

1. Incidencia: el día 26 de enero de 2017, a las 22.45 horas, la RESIDENCIA GERIATRICA GERIATROS recibe una llamada desde la misma, de la enfermera del turno de noche, informándole que dos policías se habían personado en el centro, alertadas por un vecino, para comprobar que en una bolsa de basura, situada en el exterior de la Residencia, había documentación con información médica de los residentes.

2. Al día siguiente, la Directora de la Residencia comprobó, mediante las cámaras de seguridad, que la basura se sacó el jueves 26 de enero de 2017, a las 22.03 horas y la Policía llegó al centro a las 22.16 horas.

3. Ante estos hechos, la Directora de la Residencia acudió a la Comisaria a poner una denuncia por la presunta sustracción de documentación por parte de trabajadores del Centro con la clara intención de dañar la imagen del mismo.

4. El Centro dispone de un contenedor precintado y dos destructoras de papel. El contenedor precintado se encuentra en la farmacia. La Directora cree que la documentación depositada en la calle por un trabajador provenía del servicio de farmacia. La documentación contenía datos de la medicación del día 23 de enero de 2017 y cajas/blíster vacíos de medicación.

El informe referente a la actuación inspectora efectuado por la Subdirección General de Control de Calidad, Inspección, Registro y Autorizaciones lo siguiente:

1. En relación con la custodia de documentos que contienen datos de carácter personal el programa informático obliga a identificarse y existen distintos perfiles para los trabajadores. Es necesario volver a introducir la clave de acceso al programa a los 4 minutos de inactividad.

2. Los contratos de admisión (plazas privadas de residentes) o informes de derivación (plaza concertada) se guardan en un armario metálico con llave, situado en el despacho de administración, que permanece cerrado cuando la administrativa no está. En ese armario cerrado con llave se guardan los documentos administrativos de los residentes, tales como copias del DNI, número de cuenta bancaria, cláusulas de consentimiento, etc.

3. Los expedientes de atención especializada están en el despacho del médico, el cual dispone de cerradura con llave y permanece cerrado cuando no está en el interior el facultativo.

4. Las hojas de tratamiento las imprime el médico o la enfermera y las custodian ellos mismos o el personal auxiliar. Se facilita al personal de farmacia que rellena los pastilleros de medicación.

5. Los libros de incidencias y cuadernos de hojas de cuidados diarios se custodian en una habitación cerrada con llave. La llave la pueden coger las auxiliares que rellenan las incidencias; en un registro en papel se recoge la persona que ha recogido la llave.

6. Las cajas de medicamentos tienen escrito el nombre del residente que los consume. Se custodia en la farmacia de la Residencia junto con los pastilleros diarios. La puerta cuenta con un mecanismo de acceso mediante clave que conocen las personas relacionadas con la administración de medicamentos y la reposición de los mismos.

7. El archivo de la documentación referida a residentes que hayan causado baja o ex trabajadores se encuentra en un archivo cerrado con llave. De esa llave solo dispone la Directora y la coordinadora del centro residencial.

8. En la farmacia de la residencia hay un bidón o recipiente metálico suministrado por una entidad de destrucción y reciclado. En ese bidón se echan las hojas de tratamiento que ya no sirven y los envases de medicamentos con el nombre del paciente. En otra bolsa se tira lo que no lleva datos personales.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

El artículo 126.1, apartado segundo, del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal establece:

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

II

El artículo 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 artículo 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"

III

La LOPD traspuso al ordenamiento interno el contenido de la Directiva 95/46, y 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 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: *"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 9 de la LOPD 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 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.

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

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

El art. 9 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 aquélla, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado".*

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 a los ficheros el art. 3.b) los define como *"todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"*.

Por su parte la letra c) del mismo artículo permite considerar tratamiento de datos a las "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*."

Para completar el sistema de protección en lo que a la seguridad afecta, el art. 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.

El RLOPD, en su artículo 81.1 señala que "*Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico*". 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. El artículo 88, en su punto 3, se refiere al documento de seguridad.

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. En el caso que nos ocupa como establece el artículo 81.3.a) del Reglamento de desarrollo de la LOPD, además de las medidas de nivel básico y medio, deberán adoptarse las medidas de nivel alto a los ficheros o tratamientos de datos de carácter personal que se refieran a datos de salud.

El artículo 91 del Reglamento de desarrollo de la LOPD establece:

"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."

El programa informático utilizado, Resiplus, tiene perfiles de acceso para el personal que trabaja en la Residencia y en los ordenadores exige contraseña para autenticarse.

IV

El presente procedimiento trae causa de las noticias aparecidas en prensa sobre documentación en papel, conteniendo datos de los residentes, que se dejó en la calle, en lugar de proceder a su destrucción.

El Reglamento de desarrollo de la LOPD, indica las medidas de seguridad de nivel alto aplicables a los ficheros y tratamientos no automatizados, siendo relevantes en el supuesto presente, las siguientes:

<<Artículo 111 Almacenamiento de la información

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 113 Acceso a la documentación

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.>>

Analizando las medidas de seguridad, la Subdirección General de Control de Calidad, Inspección, Registro y Autorizaciones, tras efectuar una inspección a la Residencia denunciada, señaló en su informe que los trabajadores tienen un perfil de acceso para el desarrollo de sus funciones que son garantizar la asistencia sanitaria y protección de los residentes; toda la documentación que contiene datos personales se encuentra en despachos cerrados con llave, que permanecen abiertos cuando se encuentra en él su responsable. Asimismo, se anotan en un libro registro las solicitudes de la llave y el acceso a qué documentación tendrá lugar.

En cuanto a la destrucción de los documentos en papel con datos personales, tienen un sistema de destructoras y contenedores-bidón. Tras los hechos denunciados, se constató, y así consta en la denuncia efectuada en la Comisaria, que un trabajador de la Residencia no siguió el protocolo de destrucción de documentos, depositándolos en la vía pública y avisando a las fuerzas de seguridad.

Por tanto debe concluirse que no se aprecia incumplimiento de las medidas se seguridad exigidas por la normativa referenciada por cuanto los usuarios pueden acceder a recursos autorizados habida cuenta que el sistema establece perfiles determinados, tendentes a evitar accesos no autorizados (art. 9 de la LOPD) al

acreditarse que se dispone de un control y un registro de accesos a los documentos personales de los residentes; asimismo, dispone de un sistema de destrucción de documentos. Al existir estos controles, pudieron identificar a la persona que depositó la documentación clínica de los residentes en la vía pública, procediendo a denunciarle.

Conforme a los anteriores hechos y fundamentos de derecho procede en el presente caso el archivo del presente procedimiento por no apreciarse infracción de lo dispuesto en el artículo 9 de la LOPD, en relación con los artículos 91, 111 y 113 del RLOPD.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución a la RESIDENCIA GERIATRICA GERIATROS S.A., a la ASOCIACION EL DEFENSOR DEL PACIENTE (Doña ***B.B.B.***), y a la Dirección General de Atención a la Dependencia y al Mayor (Don ***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 Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora 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 este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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 del referido texto legal.

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