Procedimiento Nº: A/00239/2013

RESOLUCIÓN: R/00157/2014

En el procedimiento A/00239/2013, instruido por la Agencia Española de Protección de Datos a DÑA. ***D.D.D.***, vista la denuncia presentada por D. ***A.A.A.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 25/12/2012, tuvo entrada en esta Agencia un escrito de D. ***A.A.A.*** (en lo sucesivo el denunciante) en el que denuncia a Dña. ***D.D.D.*** (en lo sucesivo la denunciada), por haberle remitido a través de un email de 01/07/2012 un informe confidencial relativo a la hija del denunciante, menor de edad, sin ningún tipo de encriptación o limitación de acceso. Dicho informe, de fecha 29/06/2012, que fue elaborado por la denunciada en su condición de pedagoga, corresponde a la asistencia que la misma prestaba a la hija del denunciante y contiene los detalles sobre diagnóstico médico y terapia aplicada y seguimiento de la misma.

El denunciante aporta copia del correo electrónico objeto de la denuncia, remitido en fecha 01/07/2012 (18:49) desde la cuenta ***D.D.D.***@ **E.E.E.** con destino a la cuenta ***F.F.F.***, con el asunto "Informe", conteniendo un fichero anexo denominado "*Informe* ***G.G.G.*** *juny 2012.pdf".* Asimismo, aportó copia del citado fichero, en el que se describe que la hija de la denunciante recibió determinado diagnostico en el año 2006 y que los padres solicitaron otra valoración a una asociación, que dio un diagnostico distinto. Posteriormente se realiza una descripción del itinerario de tratamientos a que ha sido sometida la menor, la situación inicial y los resultados obtenidos. En el informe aparece el membrete " ***C.C.C. H.H.H. I.I.I.***", y apareciendo en la firma " ***D.D.D.. B.B.B.***".

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se tuvo conocimiento de los siguientes extremos, que constan detallados en el Informe de Actuaciones Previas elaborado:

1. Mediante la correspondiente diligencia se comprobó que:
    a. En la web ***E.E.E.*** no figura entidad alguna como responsable del sitio web, y en el apartado "¿Quiénes somos?" se limita a decir "Somos un equipo de profesionales del ámbito educativo y terapéutico…".
    b. Realizada una búsqueda en el Registro Mercantil Central respecto a entidades con el nombre " ***C.C.C.***" no ha aparecido ninguna que se corresponda o sea similar a dicha denominación.
2. Solicitada a SISTELIA CLOUDWORKS, S.L. la identificación de la persona a la que se facturas los servicios de registro del dominio ***E.E.E.***, informa la entidad que dicha facturación se emite a nombre de la denunciada.
3. Solicitada al denunciante copia de las facturas recibidas por los servicios de atención sicológica recibidos por su hija, aporta copia de dos facturas de fechas 30/05/2012 y de fecha 30/06/2012 en las cuales aparece el membrete y sello de " ***C.C.C. H.H.H. I.I.I.***", sin que conste CIF alguno.
4. De la información y documentación aportada por la denunciada se desprende:

a. Manifiesta que la remisión del documento por correo electrónico fue debida a que éste era el modo de comunicación habitual con el denunciante, habiéndole solicitado éste, de modo expreso, la remisión de dicho informe a la mayor brevedad posible.
b. Aporta copia de correos electrónicos intercambiados con el denunciante, en los que consta la petición expresa del cliente (correo electrónico de fecha 18/06/2013) de remisión del informe.

Aporta la denunciada correos electrónicos posteriores, de fechas 19, 23, 24, 25 y 30/06/2012, así como del 1 y 04/07/2012, manifestando la denunciada que se constata que el medio habitual de comunicación con aquél era el correo electrónico, adjuntándose con el mismo los documentos y facturas que el propio cliente solicitaba mediante correo de fecha 28/06/2012, e informando que por parte del cliente denunciante no se puso la menor objeción o se cuestionase siquiera dicho modo de remisión de documentos.

Manifiesta la denunciante que, dentro de la buena fe, entendió que tenía la autorización implícita del cliente para enviar la documentación por aquél solicitada mediante documento anexo al correo electrónico de respuesta a dicha petición, sin que fuese necesaria su encriptación.

Constatado por la denunciada que el modo proceder era erróneo, ha aprendido a cifrar los documentos adjuntos remitidos con el correo electrónico, y adaptado su operativa habitual desde septiembre de 2013.

c. Manifiesta igualmente que ha realizado un curso sobre envío por correo electrónico de documentos cifrados, remitiendo desde septiembre de 2013 toda la información a sus clientes por correo electrónico cifrado y remitiendo la clave de acceso al móvil del destinatario.
d. Solicitado a la denunciante copia del Documento de Seguridad, no ha sido aportado.

TERCERO: Con fecha 10/12/2013, el Director de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 45.6 de la LOPD, acordó someter a la denunciada a trámite de audiencia previa al apercibimiento, por la presunta infracción del artículo 9 de la LOPD, en relación con los artículos 88 y 104 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la citada Ley Orgánica, tipificada como grave en el artículo 44.3.h) de la misma norma.

Con tal motivo, se concedió plazo para formular alegaciones a la misma, que presentó escrito en el que solicita que se tenga por presentada la documentación que aporta y se estime suficiente para no acordar la apertura de procedimiento sancionador, en base a las siguientes consideraciones:

. Desde septiembre de 2013 cualquier informe relativo a los pacientes es remitido debidamente encriptado y con pasword al móvil facilitado al efecto por el cliente destinatario.
. Se ha procedido a elaborar el Documento de Seguridad con el contenido del artículo 88 del Reglamento de desarrollo de la LOPD.
. La denunciada recibirá la formación precisa en el uso y manejo de los datos.
. Ha procedido a la declaración del fichero “Pacientes” en el Registro General de Protección de Datos.
. Durante el mes de enero se realizará un análisis de las medidas implementadas para evaluar la adaptación a la normativa.

La denunciada, con su escrito de alegaciones, aporta copia del Documento de Seguridad,

fechado en diciembre de 2013, el programa de formación al que se refiere en sus alegaciones sobre la LOPD, que incluye varios capítulos relativos al envío de información confidencial, copia e la solicitud de inscripción del fichero y el protocolo de estudio de la adaptación a la normativa de protección de datos personales.

El denunciante, por su parte, remitió correo electrónico de personación en el procedimiento, en el que plantea diversas consideraciones relativas a la asistencia profesional que la denunciada prestaba a la hija del denunciante, ajenas al ámbito competencial de la Agencia Española de Protección de Datos.

HECHOS PROBADOS

1. La denunciada es titular del dominio ***E.E.E.***.

2. Con fecha 01/07/2012, la denunciada remitió un correo electrónico desde la cuenta ***D.D.D.***@**E.E.E.**, dirigido al denunciante con la cuenta de destino ***F.F.F.***, y como asunto "Informe". Este correo electrónico contenía un fichero anexo sin cifrar denominado "*Informe* ***G.G.G.*** *juny 2012.pdf*", en el que se detalla el diagnóstico médico de la hija de la denunciante, una segunda valoración del mismo, itinerario de tratamientos a que ha sido sometida la menor, la situación inicial y los resultados obtenidos. Dicho informe está firmado por la denunciada en calidad de " ***B.B.B.***".

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

El Titulo VII sobre *Infracciones y sanciones*, el artículo 43 de la LOPD establece:

"1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley."

III

En el supuesto examinado, se constata que la denunciada dispone de un fichero en el que se recoge datos de carácter personal especialmente protegidos relativos a sus clientes, que utiliza para el desarrollo de su actividad profesional. Asimismo, consta acreditado que la citada entidad no dispuso del preceptivo documento de seguridad del fichero hasta diciembre de 2013 y que remitió documentación confidencial sin cifrar mediante correo electrónico.

Se imputa a la denunciada el incumplimiento del principio de seguridad de los datos personales que constan en sus ficheros.

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. Dichas medidas, en el caso que nos ocupa, deben salvaguardar la confidencialidad y seguridad de los datos de carácter personal recabados por la denunciada, correspondiendo adoptar las calificadas de nivel alto, en atención al tipo de información que contiene (datos de salud), tal como se especifica en los artículos 80 y 81 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

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.

Además, el artículo 88 del Reglamento obliga a los responsables de los ficheros a elaborar 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", con el contenido mínimo establecido en dicho artículo.*

Entre las medidas de seguridad específicas de los ficheros y tratamientos de nivel alto, el artículo 104 del citado Reglamento se refiere a transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas y establece lo siguiente:

"Artículo 104. Telecomunicaciones
Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros".

En definitiva, la denunciada 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.

Sin embargo, ha quedado acreditado en el procedimiento, y así lo ha reconocido la propia denunciada, que incumplió estas obligaciones, en lo relativo a la elaboración del Documento de Seguridad previsto en el citado artículo 88 del Real Decreto 1720/2007, y por enviar un informe confidencial sin cifrar mediante correo electrónico. En este caso, la denunciada no había garantizado la seguridad de los datos personales que figuran en sus ficheros, lo que supone la comisión de una infracción del artículo 9.1 de la LOPD,

IV

El artículo 44.3.h) de la LOPD, considera 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".

Dado que ha existido vulneración del *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, se considera que la denunciada ha incurrido en la infracción grave descrita.

V

El apartado 6 del artículo 45 de la LOPD establece lo siguiente:

"*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".

A este respecto, procede considerar lo establecido en el artículo 45.4 y 5 de la LOPD, que establece lo siguiente:

"4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:
a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
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.
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 una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. 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 los siguientes supuestos:
a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente".

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado artículo 45.6 de la LOPD. Junto a ello se constata una cualificada disminución de la culpabilidad de la entidad denunciada por la concurrencia de varios criterios de los enunciados en el artículo 45.4 de la LOPD, concretamente, el volumen de tratamientos afectados, el grado de intencionalidad apreciado, que no constan beneficios obtenidos como consecuencia de la comisión de la presunta infracción y que la actividad de la denunciada no tiene vinculación con la realización de tratamientos de datos de carácter personal.

Asimismo, se tienen en cuenta las medidas adoptadas por la misma para evitar en el futuro la comisión de infracciones de similar naturaleza, entre otras, la elaboración del documento de seguridad, el envío de los informes relativos a los pacientes debidamente encriptados y con pasword al móvil facilitado al efecto por el cliente destinatario, formación en materia de protección de datos y realización de auditorías. Se entiende que la denunciada ha adoptado las medidas correctoras adecuadas para la seguridad de los datos personales registrados en sus ficheros y no procede requerimiento alguno.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- APERCIBIR (**A/00239/2013**) a DÑA. ***D.D.D.*** 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, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

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.- Debido a que la incidencia quedó regularizada, no se insta por parte de la Agencia la adopción de una concreta medida correctora. No obstante, se solicita se comuniquen las que de forma autónoma decida adoptar sin que quepa realizar valoración alguna por parte de esta institución al no existir medidas específicas cuya adopción garantice que en el futuro no se vuelva a producir infracción como la declarada.

3.- NOTIFICAR el presente Acuerdo a DÑA. ***D.D.D.***.

4.- NOTIFICAR el presente Acuerdo a 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.

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