Procedimiento Nº: A/00223/2013

RESOLUCIÓN: R/00108/2014

En el procedimiento A/00223/2013, instruido por la Agencia Española de Protección de Datos a la entidad FUNDACIÓN XXXXXXXXXXXX, vista la denuncia presentada por D. ***D.D.D.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 06/09/2013, tuvo entrada en esta Agencia un escrito de D. ***C.C.C.*** (en lo sucesivo el denunciante) en el que denuncia a la entidad FUNDACIÓN XXXXXXXXXXXX (en lo sucesivo FERP) por permitir el acceso público a través de Internet a sus datos de carácter personal contenidos en su CV, relativos a sus datos identificativos, líneas de telefonía, dirección, correo electrónico, DNI, historial académico y profesional. Según expone, dicho CV resulta públicamente accesible al teclear su nombre y apellidos en el buscador Google, que ofrece como resultado la referencia *" **A.A.A.**".*

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. Con fecha 11/09/2013, por la Inspección de Datos se accede a internet y se realiza una búsqueda en *Google* con el nombre y apellidos del denunciante como criterio, obteniendo una lista de resultados, en cuya primera página figura un enlace a un documento asociado al dominio *fundacionXXXXXXXXXXXX.es*, cuyo acceso está restringido, requiriéndose identificación y contraseña. El resumen del resultado (*snippet*) contiene el nombre y apellidos del denunciante. Se verifica asimismo que resulta públicamente accesible la versión caché que almacena el buscador asociada a dicho resultado, documento con el nombre "*XXXXXXXX.pdf*", que fue indexado desde la carpeta *" **A.A.A.**"* en fecha no determinada.

2. El documento obtenido por la Inspección, de diez páginas, contiene el DNI, fecha de nacimiento, domicilio particular y los datos académicos y profesionales del denunciante.

3. Con fecha 15/10/2013, por la Inspección se reiteró la búsqueda, obteniendo nuevamente un resultado vinculado al citado dominio, de acceso también restringido con identificador de usuario y contraseña, cuyo *snippet* no contiene ya datos del denunciante sino el texto: "*No hay disponible una descripción de este resultado debido al archivo XXXX.txt de este sitio. Más información*". La versión caché del documento asociado al resultado ya no resulta tampoco accesible. Al accederse al archivo "*XXXX.txt*" enlazado desde el citado resultado se verifica que contiene, entre otras, las líneas:

Disallow: ***A.A.A.***
Disallow: ***A.A.A.***
Disallow: ***A.A.A.*.pdf***

4. De lo anterior se obtienen las siguientes conclusiones:

El documento con los datos curriculares del denunciante fue indexado por los robots de rastreo del motor de búsqueda de *Google* en un momento en el que su acceso no había sido convenientemente restringido.

En la actualidad, para acceder al documento se requiere la identificación y autenticación de un usuario autorizado.

Desde el sitio web se han dado instrucciones a los buscadores para que no indexen ningún documento que pudiera resultar accesible en la carpeta en la que se almacena el documento.

TERCERO: Con fecha 25/11/2013, el Director de la Agencia Española de Protección de Datos, por virtud de 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 lo sucesivo LOPD), acordó someter a la entidad FERP a trámite de audiencia previa al apercibimiento, en relación con la denuncia por infracción del artículo 9 de la LOPD, en relación con los artículos 91 y 93 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 entidad FERP, que presentó escrito solicitando el archivo del expediente en base a las siguientes consideraciones:

. En relación con los hechos, manifiesta que, en el desarrollo de las actividades que le son propias, como entidad sin ánimo de lucro dedicada a promover el estudio, la investigación y promoción científica, en el año 2013 ofertó una serie de becas a profesionales y titulares del ámbito científico, recabando los datos personales de los interesados a través de la página web, habiendo conocido a través de un correo del denunciante de fecha 05/09/2013, que existía la posibilidad de captar sus datos mediante el buscador Google.

Esta incidencia fue comunicada a su proveedor de servicios informáticos, con la que tiene suscrito un contrato ajustado a los términos del artículo 12 de la LOPD, procediendo a reparar la incidencia. Así, con fecha 10/09/2013 se informó al denunciante afectado sobre la adopción de las medidas de seguridad que solventaron la incidencia.

. Considera que debe declararse el archivo de las actuaciones por la concurrencia de la totalidad de las circunstancias de atenuación establecidas en el artículo 45.4 de la LOPD:

. Ausencia de carácter continuado de la infracción, por cuanto se trata de una única incidencia que fue rápidamente resuelta.
. Se trata de un único afectado, frente al importante volumen de peticiones de beca.
. No vinculación de la actividad del infractor con el tratamiento de datos personales.
. La entidad no tiene ánimo de lucro.
. Ausencia de beneficios.
. Ausencia de intencionalidad.
. Ausencia de reincidencia.
. La situación se produce por un mal funcionamiento técnico no imputable a la Fundación.
. Falta de actuación u omisión imputable a la Fundación.
. Ausencia de responsabilidad directa alguna.

HECHOS PROBADOS

1. La entidad FERP es responsable del sitio web *fundacionXXXXXXXXXXXX.es*.

2. FERP ha manifestado es una entidad sin ánimo de lucro dedicada a promover el estudio, la investigación y promoción científica, y que, en el desarrollo de su actividad, durante el año 2013 ofertó una serie de becas a profesionales y titulares del ámbito científico, recabando los datos personales de los interesados a través de su página web.

3. El denunciante registró sus datos personales y curriculares en la web de FERP.

4. Con fecha 06/09/2013, el denunciante formuló denuncia ante la Agencia Española de Protección de Datos contra la entidad FERP por permitir el acceso público a través de Internet a sus datos de carácter personal contenidos en su CV (datos identificativos, líneas de telefonía, dirección, correo electrónico, DNI, historial académico y profesional), que resultaron públicamente accesible al teclear su nombre y apellidos en el buscador Google, obteniendo como la referencia *" **A.A.A.**"*.

5. Con fecha 11/09/2013, por la Inspección de Datos de la Agencia Española de Protección de Datos se realizó una consulta a través del buscador Google, verificando que era públicamente accesible la versión caché del CV del denunciante que almacena el buscador, documento con el nombre "*XXXXXXXX.pdf*", que fue indexado desde la carpeta *" A.A.A."* en fecha no determinada. El documento obtenido por la Inspección, de diez páginas, contiene el DNI, fecha de nacimiento, domicilio particular y los datos académicos y profesionales del denunciante.

6. Con fecha 11/09/2013, por la Inspección de Datos se accede a internet y se realiza una búsqueda en *Google* con el nombre y apellidos del denunciante como criterio, obteniendo una lista de resultados, en cuya primera página figura un enlace a un documento asociado al dominio *fundacionXXXXXXXXXXXX.es*, cuyo acceso está restringido, requiriéndose identificación y contraseña. El resumen del resultado (*snippet*) contiene el nombre y apellidos del denunciante.

7. Con fecha 15/10/2013, por los Servicios de inspección de la Agencia se reiteró la búsqueda en *Google* con el nombre y apellidos del denunciante como criterio, obteniendo nuevamente un resultado vinculado al dominio *fundacionXXXXXXXXXXXX.es*, de acceso también restringido con identificador de usuario y contraseña, cuyo *snippet* no contiene ya datos del denunciante sino el texto: "*No hay disponible una descripción de este resultado debido al archivo XXXX.txt de este sitio. Más información*". La versión caché del documento asociado al resultado tampoco resulta accesible.

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

Se imputa a la entidad FERP 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.

Asimismo, 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.

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 FERP a través de la web *fundacionXXXXXXXXXXX.es* relativos a los usuarios que se inscribieron en la misma como solicitantes de unas becas convocadas por la Fundación. Los responsables de los ficheros

deben adoptar las medidas previstas reglamentariamente, en atención a la naturaleza de la información que contiene los ficheros respectivos, tal como se especifica en el art. 80 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD. El artículo 81.1 del citado Reglamento señala que *"Todos los ficheros o tratamiento 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, del Reglamento de desarrollo de la LOPD.

El artículo 91 del citado Reglamento, aplicable a todos los ficheros y tratamientos automatizados, 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".

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.

"Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".

El artículo 5.2.b) del citado Reglamento define la autenticación como el procedimiento de comprobación de la identidad de un usuario; y el mismo artículo, letra h), se refiere a la

identificación como el procedimiento de reconocimiento de la identidad de un usuario. Corresponde al responsable del fichero o tratamiento comprobar la existencia de la autorización exigida en el citado artículo 91, con un proceso de verificación de la identidad de la persona (autenticación) implantando un mecanismo que permita acceder a datos o recursos en función de la identificación ya autenticada. Cada identidad personal deberá estar asociada con un perfil de seguridad, roles y permisos concedidos por el responsable del fichero o tratamiento.

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

En este caso, los hechos expuestos, en relación con el acceso por parte de terceros a datos personales y documentos curriculares del denunciante contenidos en la base de datos de FERP, aportados con su solicitud de una beca registrada a través del sitio web *fundacionXXXXXXXXXXX.es*, que además pudieron ser indexados por buscadores de Internet, suponen la comisión, por parte de dicha entidad, de una infracción del artículo 9.1 de la LOPD, al haberse constatado que tales hechos se producen por un error en el sistema de información diseñado por la propia entidad, que no había restringido convenientemente el acceso a dicho sistema de información en el momento en que aquel documento fue indexado por los robots de rastreo del motor de búsqueda de Google. Dicho fallo posibilitó que los datos personales relativos al denunciante permanecieran abiertos a cualquier persona, incluso con la posibilidad de descargar el curriculum vitae, con detalle de datos personales relativos a nombre, apellidos, DNI, fecha de nacimiento, domicilio particular y los datos académicos y profesionales del denunciante.

Por tanto, los datos personales del denunciante resultaron accesibles a terceros, siendo ello consecuencia de una insuficiente o ineficaz implementación de las medidas de seguridad. Dado que ha existido vulneración del *"principio de seguridad de los datos"*, se considera que e FERP ha incurrido en la infracción grave descrita.

IV

En esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deben impedir, de forma efectiva, el acceso a la información por parte de terceros. 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".*

El principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisible en el ámbito del Derecho administrativo sancionador una responsabilidad sin culpa. Pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada y a este respecto el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone *"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."

El Tribunal Supremo (STS 16 de abril de 1991 y STS 22 de abril de 1991) considera que del elemento culpabilista se desprende *"que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable."* El mismo Tribunal razona que *"no basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa" sino que es preciso "que se ha empleado la diligencia que era exigible por quien aduce su inexistencia."* (STS 23 de enero de 1998).

A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que *"basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..."* (SAN 29de junio de 2001).

V

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 FERP ha incurrido en la infracción grave descrita.

VI

La Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de fecha 25/02/2010, en relación con un caso en el que se examina un posible fallo de seguridad en los sistemas de información, señala lo siguiente:

"…la recurrente no realizó actividad alguna, pese a que era consciente del riesgo de una posible revelación o publicidad del fichero…".

"… un comportamiento adecuado y activo de la misma pudo impedir o, al menos, minimizar el riesgo real de revelación de los datos personales de los usuarios. Es decir, su comportamiento omisivo (no advirtiendo de la fuga a los usuarios, no presentando denuncia, no cambiando la contraseña etc.) facilitó o, al menos, no obstaculizó la revelación de los datos…".

"La recurrente, como garante de los datos personales de terceros que figuraban en sus ficheros, no tuvo la diligencia exigible sino que propició la revelación como cooperador necesario por omisión. Siendo ello así, la Sala entiende cometida, como también recoge la resolución impugnada, la infracción del artículo 10 de la LOPD, tipificada en el artículo 44.3.g) de la citada norma, es decir la vulneración del deber de guardar secreto…".

Los criterios contenidos en la Sentencia citada se han tenido en cuenta para no imputar a FERP una infracción de lo dispuesto en el artículo 10 de la LOPD, por incumplimiento del deber de secreto en relación con los datos personales del denunciante, considerando la actuación

desarrollada por la misma con posterioridad al incidente para regularizar la situación y minimizar los riesgos, que consta detallada en los hechos probados sexto y séptimo.

VII

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 establecen 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 negocio o la actividad del infractor, la ausencia de beneficios y el grado de intencionalidad apreciado, que sirven, conforme a los expuesto, para motiva la no apertura de procedimiento sancionador, pero no el archivo de las actuaciones solicitado por FERP, considerando la infracción cometida.

Asimismo, se tiene en cuenta la diligencia mostrada por la entidad FERP para regularizar la incidencia. Los Servicios de Inspección comprobaron que por parte de la citada Fundación se adoptaron medidas para evitar que los datos personales de las personas registradas a través de su web puedan ser indexados en el futuro por buscadores de Internet y se ha dispuesto el acceso previa identificación y autenticación.

Por tanto, se entiende que FERP ha adoptado las medidas correctoras adecuadas para la seguridad de los datos personales registrados en sus ficheros, por lo que 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/00223/2013**) a la entidad FUNDACIÓN XXXXXXXXXXXX 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 regulariada, 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 la entidad FUNDACIÓN XXXXXXXXXXXX.

4.- NOTIFICAR el presente Acuerdo a D. ***D.D.D.***.

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