Procedimiento Nº: A/00247/2014

RESOLUCIÓN: R/02372/2014

En el procedimiento A/00247/2014, instruido por la Agencia Española de Protección de Datos a la entidad SMAP CELIACS DE CATALUNYA, vista la denuncia presentada por DÑA. ***B.B.B.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 22/10/2013, tuvo entrada en esta Agencia un escrito de Dña. ***B.B.B.*** (en lo sucesivo la denunciante) en el que denuncia a la entidad SMAP Celiacs de Catalunya (en lo sucesivo CELIACS DE CATALUNYA), de la que es miembro como tutora de su hijo menor de edad, socio de la misma, por ceder sus datos personales a la entidad Associació de Consumidors de la Provincia de Barcelona, que los utilizó para remitirle un correo electrónico de fecha 07/10/2013 a su dirección ***A.A.A.***, invitándola a una serie de actos como socia, sin serlo. La denunciante manifiesta que contactó con la citada asociación de consumidores y que esta entidad admitió que los datos le fueron cedidos por CELIACS DE CATALUNYA en virtud de un acuerdo. Asimismo, añade que esta última respondió a un correo de la denunciante señalando que llevaría a cabo las investigaciones oportunas, también mediante correo electrónico e 11/10/2013.

Aporta copia del correo electrónico de fecha 07/10/2013 que le remitió la Associació de Consumidors de la Provincia de Barcelona y de la respuesta facilitada por CELIACS DE CATALUNYA en fecha 11/10/2013.

SEGUNDO: A la vista de los hechos denunciados, en fase de investigación previa, por los Servicios de Inspección de esta Agencia se llevaron a cabo las siguientes actuaciones, que constan detalladas en el Informe elaborado:

1. Con fecha 16/06/2014, se solicitó información a la Associació de Consumidors de la Provincia de Barcelona, en el domicilio que figura tanto en la denuncia, en Internet y en el correo electrónico que remitió a la denunciante, siendo devuelta la carta con la indicación “Desconocido”. Asimismo, se realizó una llamada al número de teléfono que consta en la documentación remitida por la Asociación de Celiacos de Catalunya y se comprobó que dicha línea no se encuentra en servicio.
2. Con fecha 02/07/2014, se solicitó información a CELIACS DE CATALUNYA, cuyo domicilio coincide con el de la Associació de Consumidors de la Provincia de Barcelona, que también es el que figura en la denuncia. Esta carta fue igualmente devuelta con la indicación “Desconocido”.
3. Tras diversas gestiones, el requerimiento de información se notificó a CELIACS DE CATALUNYA en un nuevo domicilio. En respuesta al mismo, esta entidad remitió un escrito poniendo de manifiesto lo siguiente:
    3.1. CELIACS DE CATALUNYA remitió un correo electrónico, de fecha 04/10/2013, a la Asociación de Consumidores de la Provincia de Barcelona prohibiéndole expresamente el tratamiento de la Base de Datos de sus asociados. Adjunta dicho correo.

3.2. Con fecha 08/10/2013, CELIACS DE CATALUNYA cambia de ubicación física, ya que compartía los locales con la citada Associació de Consumidors de la Provincia de Barcelona y tuvo noticias de prácticas irregulares.
3.3. Con fecha 17/10/2013 se remite Burofax, que se adjunta, a la Associació de Consumidors de la Provincia de Barcelona, solicitando toda la documentación que pudiera encontrarse en su poder, en cualquier soporte, relativa a CELIACS DE CATALUNYA.
3.4. Se adjunta copia del Acta de fecha 16/11/2013 de la Asamblea General Extraordinaria de la entidad CELIACS DE CATALUNYA, en la que se pone de manifiesto que la otra asociación mencionada obtuvo los datos de forma ilícita, aprobándose en ese momento el cambio de domicilio. En este documento consta que, teniendo en cuenta los hechos reseñados, no se puede seguir compartiendo el "servidor informàtic" en el que se encontraba la base de datos de los socios de CELIACS DE CATALUNYA, que estaba físicamente en el mismo local.
3.5. No cuentan con el consentimiento de la denunciante para la cesión de datos, puesto que se trata de un acceso indebido por parte de la Associació de Consumidors de la Provincia de Barcelona.
3.6. CELIACS DE CATALUNYA ha contratado los servicios de una empresa especializada para realizar una auditoría de los procedimientos para el tratamiento de datos personales y adecuarlos a la normativa aplicable.

TERCERO: Con fecha 29/09/2014, 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 CELIACS DE CATALUNYA 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, 93, 103 o 113 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

Con tal motivo, se concedió a la entidad CELIACS DE CATALUNYA plazo para formular alegaciones, recibiéndose escrito de fecha 08/10/2014, con el que aporta copia del Documento de Seguridad que describe el estado actual de las medidas de seguridad descritas en los artículos del RDLOPD antes reseñados y un informe emitido por la entidad contratada por aquella para la prestación de servicios de auditoría y asesoramiento continuado en materia de protección de datos personales.

En el informe citado, también de fecha 08/10/2014, la entidad Data Protection Privacy Procedures, S.L. manifiesta que realizó una auditoría en este ámbito a CELIACS DE CATALUNYA y después de llevar a cabo un diagnóstico de las necesidades y medidas a implementar por la asociación, elaboró el correspondiente informe con fecha 18/03/2014, con resultado favorable, certificando el correcto cumplimiento de las medidas de seguridad de nivel alto.

Por otra parte, en el citado Documento de Seguridad, en relación con el fichero de gestión de socios de CELIACS DE CATALUNYA, fichero automatizado de nivel alto, se indica que se ha dispuesto el registro de accesos y revisiones con una periodicidad mínima mensual; se definen los perfiles de las personas que tienen acceso a la base de datos de gestión de socios y los trabajadores que pueden visualizar y no modificar; se requiere login y password para el inicio de sesión; se establécela la caducidad anual de las claves personales y el bloqueo de los equipos por inactividad.

HECHOS PROBADOS

1. Los datos personales de la denunciante figuran en los ficheros dela entidad CELIACS DE CATALUNYA como tutora de su hijo menor de edad, socio de la misma.

2. Al menos hasta 08/10/2013, las entidades CELIACS DE CATALUNYA y la Associació de Consumidors de la Provincia de Barcelona compartieron el local que constituía su respectiva sede.

3. Con fecha 04/10/2013, la entidad CELIACS DE CATALUNYA remitió un correo electrónico a la Asociación de Consumidores de la Provincia de Barcelona prohibiéndole expresamente el tratamiento de la Base de Datos de sus asociados.

4. Con fecha 07/10/2013, la entidad Associació de Consumidors de la Provincia de Barcelona remitió un correo electrónico a la denunciante, a la dirección de correo que figura en los ficheros de CELIACS DE CATALUNYA, invitándola a una serie de actos como socia, sin serlo. La denunciante manifiesta que contactó con la citada asociación de consumidores y que esta entidad admitió que los datos le fueron cedidos por CELIACS DE CATALUNYA en virtud de un acuerdo. Asimismo, añade que esta última respondió a un correo de la denunciante señalando que llevaría a cabo las investigaciones oportunas, también mediante correo electrónico e 11/10/2013.

5. Con fecha 17/10/2013, la entidad CELIACS DE CATALUNYA remite un Burofax a la Associació de Consumidors de la Provincia de Barcelona, solicitando toda la documentación que pudiera encontrarse en su poder, en cualquier soporte, relativa a CELIACS DE CATALUNYA.

6. En la Asamblea General Extraordinaria de la entidad CELIACS DE CATALUNYA, celebrada el 16/11/2013, se pone de manifiesto que la Associació de Consumidors de la Provincia de Barcelona obtuvo los datos de forma ilícita, aprobándose en ese momento el cambio de domicilio. En este documento consta que, teniendo en cuenta los hechos reseñados, no se puede seguir compartiendo el “servidor informàtic” en el que se encontraba la base de datos de los socios de CELIACS DE CATALUNYA, que estaba físicamente en el mismo local.

7. La entidad CELIACS DE CATALUNYA ha reconocido que no cuenta con el consentimiento de la denunciante para la cesión de sus datos a la Associació de Consumidors de la Provincia de Barcelona, denunciada por la misma, puesto que se trata de un acceso indebido por parte de esta última asociación.

8. Con fecha 21/11/2013, CELIACS DE CATALUNYA contrató los servicios de Data Protection Privacy Procedures, S.L., empresa especializada, para realizar una auditoría de los procedimientos para el tratamiento de datos personales y adecuarlos a la normativa aplicable.

Consta en las actuaciones un informe de Data Protection Privacy Procedures, S.L., de fecha 08/10/2014, en el que se indica que realizó una auditoría a CELIACS DE CATALUNYA y después de llevar a cabo un diagnóstico de las necesidades y medidas a implementar por la asociación, elaboró el correspondiente informe con fecha 18/03/2014, con resultado favorable, certificando el correcto cumplimiento de las medidas de seguridad de nivel alto.

9. La entidad CELIACS DE CATALUNYA ha aportado a las actuaciones el Documento de

Seguridad que recoge las medidas de seguridad actuales. En este Documento, en relación con el fichero de gestión de socios de CELIACS DE CATALUNYA, fichero automatizado de nivel alto, se indica que se ha dispuesto el registro de accesos y revisiones con una periodicidad mínima mensual; se definen los perfiles de las personas que tienen acceso a la base de datos de gestión de socios y los trabajadores que pueden visualizar y no modificar; se requiere login y password para el inicio de sesión; se establécela la caducidad anual de las claves personales y el bloqueo de los equipos por inactividad.

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

Se imputa a la entidad CELIACS DE CATALUNYA 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.

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 contenidos en los ficheros de la

entidad CELIACS DE CATALUNYA, correspondiendo adoptar las de nivel alto en atención al tipo de información que contiene, 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.

Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104, del Reglamento de desarrollo de la LOPD.

Los artículos 91 y 93 del citado Reglamento, aplicable a todos los ficheros y tratamientos automatizados, y el artículo 103 del mismo Reglamento, aplicable a los ficheros con nivel alto de seguridad, establecen:

"Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio".

Este artículo desarrolla las previsiones que deberá establecer el responsable del fichero para garantizar que los usuarios con accesos 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.

"Artículo 103. Registro de accesos.
1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:
a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.
La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad".

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".*

En definitiva, la entidad CELIACS DE CATALUNYA está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para sus ficheros, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en los mismos. Sin embargo, ha quedado acreditado que la citada entidad incumplió esta obligación, al haberse constatado la posibilidad de acceder, sin restricción alguna, a los datos personales aportados por las personas inscritas en dicha asociación.

En este caso, consta que la entidad CELIACS DE CATALUNYA compartía local con la Associació de Consumidors de la Provincia de Barcelona, así como el servidor informático en el que se encontraba el fichero automatizado de los socios de aquélla, de nivel alto de seguridad. Asimismo, consta que la Associació de Consumidors de la Provincia de Barcelona pudo acceder a los datos personales de los socios de CELIACS DE CATALUNYA, y que los utilizó para remitir a los mismos correos electrónicos. En concreto, con fecha 07/10/2013, la entidad Associació de Consumidors de la Provincia de Barcelona remitió un correo electrónico a la denunciante invitándola a diversos actos.

Este acceso por parte de la Associació de Consumidors de la Provincia de Barcelona a los datos personales de los socios de CELIACS DE CATALUNYA supone la comisión, por parte de ésta entidad, de una infracción del artículo 9.1 de la LOPD, al haberse constatado que tales hechos se producen por una deficiente implementación de las medidas de seguridad obligatorias

según la naturaleza y el nivel de seguridad asignado al fichero en cuestión (nivel alto).

Esta irregularidad, es decir, la posibilidad de acceder a la información por parte de la Associació de Consumidors de la Provincia de Barcelona debido a un fallo de seguridad, ha sido reconocida por la propia entidad imputada. En dos correos remitidos por CELIACS DE CATALUNYA a la citada asociación de consumidores, aquella entidad solicita expresamente a la misma el cese en el tratamiento de los datos de sus asociados y la devolución de toda la documentación que pudiera encontrarse en su poder, en cualquier soporte.

Asimismo, las deficiencias de seguridad en los sistemas de información de CELIACS DE CATALUNYA quedan igualmente probadas considerando las medidas implementadas como consecuencia del incidente de seguridad reseñado. CELIACS DE CATALUNYA contrató a una entidad tercera para la prestación de servicios de auditoría y asesoramiento continuado en materia de protección de datos personales y se dispuso, entre otras medidas, el registro de accesos y el establecimiento de perfiles de las personas que pueden acceder o modificar la base de datos de gestión de socios.

Así, los datos personales de los socios de CELIACS DE CATALUNYA resultaron accesibles a terceros, concretamente a la Associació de Consumidors de la Provincia de Barcelona por una insuficiente o ineficaz implementación de las medidas de seguridad detalladas. Por tanto, dado que existió una vulneración del *"principio de seguridad de los datos"*, se considera que CELIACS DE CATALUNYA ha incurrido en la infracción grave descrita.

III

Por otra parte, se tuvo en cuenta que la entidad CELIACS DE CATALUNYA no ha sido sancionada o apercibida con anterioridad por esta Agencia.

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

El citado 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".

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado artículo 45.6 de la LOPD, por lo que procedería apercibir a CELIACS DE CATALUNYA.

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 citado 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…, 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, ha quedado acreditado que CELIACS DE CATALUNYA ha adoptado medidas para evitar que los datos personales de sus socios puedan ser accedidos por terceros no autorizados. En concreto, según consta en el Documento de Seguridad aportado, se ha dispuesto el registro de accesos y revisiones con una periodicidad mínima mensual; se definen los perfiles de las personas que tienen acceso a la base de datos de gestión de socios y los trabajadores que pueden visualizar y no modificar; se requiere login y password para el inicio de sesión; se establece la caducidad anual de las claves personales y el bloqueo de los equipos por inactividad.

En consecuencia, deben estimarse adoptadas ya las medidas correctoras pertinentes, por lo que debe procederse a resolver el archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la entidad 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/00247/2014** seguido contra la entidad SMAP CELIACS DE CATALUNYA, 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.

2.- NOTIFICAR el presente Acuerdo a la entidad SMAP CELIACS DE CATALUNYA y a DÑA. ***B.B.B.***.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (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.

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