Procedimiento Nº: A/00143/2015

RESOLUCIÓN: R/02548/2015

En el procedimiento A/00143/2015, instruido por la Agencia Española de Protección de Datos a la entidad HANSEN & CAWLEY, S.A., vista la denuncia presentada por D. ***B.B.B.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 22/04/2015, tuvo entrada en esta Agencia un escrito de D. ***B.B.B.*** (en lo sucesivo el denunciante), en el que denuncia la divulgación de sus datos personales en Internet, en la carpeta ***" A.A.A."*** accesible a través del sitio Web http:// A.A.A.-cawley.es. Añade que el día 21/04/2015, el mismo en que detectó la incidencia, remitió un correo electrónico a la dirección "atencionalcliente@ A.A.A.-cawley.com" solicitando la eliminación de los datos accesibles con el citado buscador de Internet y que esta petición ya había sido atendida en el momento de la denuncia. En su denuncia detalla la respuesta que manifiesta haber recibido de la entidad responsable el día 21/04/2015:

"En primer lugar queremos pedirle disculpas por la situación producida. Un fallo de seguridad en nuestros sistemas ha hecho que Google publique dicha información. Somos una empresa de transporte y siempre hemos mantenido la confidencialidad de datos de los pedidos de nuestros clientes. Eximimos de toda culpa a la empresa en la usted realizó sus compras, ya que el fallo ha sido en nuestros sistemas. Hemos corregido el fallo, pero Google lo sigue manteniendo en sus resultados de búsqueda (en caché). ¿Sería tan amable de decirnos la url o la búsqueda que realiza para que aparezcan sus datos?".

Aporta impresión de pantalla con los resultados de la búsqueda realizada utilizando el buscador Google, con su primer apellido y número de teléfono como criterio, en la que obtiene como resultado un enlace a la URL ***A.A.A.*** y el apellido, domicilio y número de teléfono del denunciante.

SEGUNDO: Con fecha 22/04/2015, por la Subdirección General de Protección de Datos se realiza una búsqueda en Internet similar a la señalada en la denuncia, no obteniendo ningún resultado.

Asimismo, se accede al sitio web http:// A.A.A.-cawley.es, en el que consta que la entidad HANSEN & CAWLEY, S.A. (en lo sucesivo HANSEN & CAWLEY) es la responsable de dicha web.

TERCERO: Con fecha 09/06/2015, 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 HANSEN & CAWLEY a trámite de audiencia previa al apercibimiento por la presunta infracción del artículo 9 de dicha norma, 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 LOPD, tipificada

como grave en el artículo 44.3.h) de la citada Ley Orgánica.

Con tal motivo, se concedió a la entidad HANSEN & CAWLEY plazo para formular alegaciones, recibiéndose escrito en el que solicita el archivo de las actuaciones, considerando que dispone de protocolos para garantizar la seguridad de la información, que la incidencia resultó de un fallo de estos protocolos que fue corregido inmediatamente y que no ha existido intencionalidad.

Admite que los hechos se produjeron según consta relatado en el acuerdo de apertura, como consecuencia de un fallo en una actualización del sitio web, que provocó la eliminación de los ficheros que protegían varios accesos a las zonas privadas del mismo, y añade que subsanaron la incidencia adoptando las medidas de seguridad siguientes:

- Denegar el acceso a determinadas carpetas del servidor por medio de los permisos de usuario del Sistema Operativo.
- Denegar el acceso a determinadas carpetas del servidor por medio del fichero de protección Web ".htaccess".
- Denegar el acceso a determinadas carpetas del servidor a los buscadores como Google, por medio del fichero "robots.txt".
- Denegar el acceso vía URL colocando un "index.html" que deniega el acceso en todas las carpetas que no forman parte de la parte pública de la web.

Finalmente, señala que en cuanto se tuvo conocimiento del fallo de seguridad solicitaron a Google que eliminara toda la información.

HECHOS PROBADOS

1. La entidad HANSEN & CAWLEY es titular del sitio web A.A.A.-cawley.es.

2. Con fecha 21/04/2015, utilizando el buscador de Internet Google, el denunciante realizó una búsqueda con su primer apellido y número de teléfono como criterio, obteniendo como resultado un enlace a la URL ***A.A.A.***, con detalle de su primer apellido, domicilio y número de teléfono.

3. Con fecha el día 21/04/2015, el denunciante remitió un correo electrónico a la dirección "atencionalcliente@ A.A.A.-cawley.com" solicitando la eliminación de los datos accesibles con el buscador de Internet Google, que fue respondido el mismo día por HANSEN & CAWLEY en los siguientes términos:

"En primer lugar queremos pedirle disculpas por la situación producida. Un fallo de seguridad en nuestros sistemas ha hecho que Google publique dicha información. Somos una empresa de transporte y siempre hemos mantenido la confidencialidad de datos de los pedidos de nuestros clientes. Eximimos de toda culpa a la empresa en la usted realizó sus compras, ya que el fallo ha sido en nuestros sistemas. Hemos corregido el fallo, pero Google lo sigue manteniendo en sus resultados de búsqueda (en caché). ¿Sería tan amable de decirnos la url o la búsqueda que realiza para que aparezcan sus datos?".

4. Con fecha 22/04/2015, el denunciante formuló denuncia ante la AEPD por la divulgación de sus datos personales en Internet, en la carpeta ***" A.A.A."***, accesible a través del sitio Web http:// A.A.A.-cawley.es. En su denuncia señala que la solicitud formulada a HANSEN & CAWLEY para que sus datos personales accesible a través de Google fuesen eliminados había sido atendida en

el momento de la denuncia.

5. Con fecha 22/04/2015, por la Subdirección General de Protección de Datos se realiza una búsqueda en Internet similar a la señalada en la denuncia, no obteniendo ningún resultado.

6. HANSEN & CAWLEY ha manifestado en su escrito de alegaciones que la incidencia denunciada se produjo como consecuencia de un fallo en una actualización del sitio web, que provocó la eliminación de los ficheros que protegían varios accesos a las zonas privadas del mismo.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora 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 HANSEN & CAWLEY 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 HANSEN & CAWLEY.

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, 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.

En definitiva, la entidad HANSEN & CAWLEY 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 sus clientes.

En las actuaciones consta acreditada la posibilidad de que por parte de terceros se pudiera acceder, sin restricción alguna, a los datos personales del denunciante, al haberse permitido su recopilación e indexación por buscadores de internet, que pudieron acceder a sus datos personales relativos a primer apellido, domicilio y número de teléfono, en la URL ***A.A.A.***.

En concreto, consta que, con fecha 21/04/2015, a través de una búsqueda en Internet utilizando como criterio el primer apellido y teléfono del denunciante se obtuvo como resultado el enlace al sitio web A.A.A.-cawley.es reseñado.

Esta irregularidad, es decir, la posibilidad de acceder a la información por parte de terceros debido a un fallo de seguridad, ha sido reconocida por la propia entidad imputada y así lo ha recogido en su escrito de alegaciones, en el que señala que estuvo provocado por un fallo en una actualización del sitio web, que provocó la eliminación de los ficheros que protegían varios accesos a las zonas privadas del mismo.

Así, los datos personales de algunos clientes resultaron accesibles a terceros desde la misma web, siendo ello consecuencia de una insuficiente o ineficaz implementación de las medidas de seguridad detalladas. Dado que ha existido vulneración del *"principio de seguridad de los datos"*, se considera que HANSEN & CAWLEY ha incurrido en la infracción grave descrita.

III

Por otra parte, se tuvo en cuenta que HANSEN & CAWLEY 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 citada entidad 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. Junto a ello, se constata una cualificada disminución de la culpabilidad de la imputada teniendo en cuenta la ausencia de intencionalidad, la ausencia de beneficios, que no se han provocado perjuicios distintos a los derivados específicamente de la infracción, así como la inmediata respuesta de HANSEN & CAWLEY para subsanar la incidencia.

Todo ello, justifica que la AEPD **no haya acordado la apertura de un procedimiento sancionador y que opte por aplicar el artículo 45.6 de la LOPD.**

Ahora bien, es obligado hacer mención a la Sentencia de la Audiencia Nacional de 29/11/2013, (Rec. 455/2011), Fundamento de Derecho Sexto, que sobre el apercibimiento regulado en el artículo 45.6 de la LOPD y a propósito de su naturaleza jurídica advierte que "*no constituye una sanción"* y que se trata de "*medidas correctoras de cesación de la actividad constitutiva de la infracción"* que *sustituyen* a la sanción. La Sentencia entiende que el artículo 45.6 de la LOPD confiere a la AEPD una "*potestad"* diferente de la sancionadora cuyo ejercicio se condiciona a la concurrencia de las especiales circunstancias descritas en el precepto.

En congruencia con la naturaleza atribuida al apercibimiento como una alternativa a la sanción cuando, atendidas las circunstancias del caso, el sujeto de la infracción no es merecedor de aquella, y considerando que el objeto del apercibimiento es la imposición de medidas correctoras, la SAN citada concluye que cuando éstas ya hubieran sido adoptadas, lo procedente en Derecho es acordar el archivo de las actuaciones.

Como se ha señalado, en el asunto analizado, consta que se ha impedido la indexación de los datos personales del denunciante por buscadores de Internet y que se han adoptado medidas para evitar incidencias similares en el futuro. En concreto, HANSEN & CAWLEY sobre las siguientes:

- Denegar el acceso a determinadas carpetas del servidor por medio de los permisos de usuario del Sistema Operativo.
- Denegar el acceso a determinadas carpetas del servidor por medio del fichero de protección Web ".htaccess".
- Denegar el acceso a determinadas carpetas del servidor a los buscadores como Google, por medio del fichero "robots.txt".
- Denegar el acceso vía URL colocando un "index.html" que deniega el acceso en todas las carpetas que no forman parte de la parte pública de la web.

Por tanto, a la vista del pronunciamiento recogido en la SAN de 29/11/2013 (Rec. 455/2011) referente a los supuestos en los que **el denunciado ha adoptado las medidas correctoras oportunas,** de acuerdo con lo señalado **se debe proceder al archivo de las actuaciones.**

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- ARCHIVAR el procedimiento **A/00143/2015** seguido contra HANSEN & CAWLEY, S.A., con

arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con la denuncia por la infracción del artículo 9 de la LOPD.

2.- NOTIFICAR el presente Acuerdo a la entidad HANSEN & CAWLEY, S.A. y a D. ***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.

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