Procedimiento Nº: A/00060/2015

RESOLUCIÓN: R/01966/2015

En el procedimiento A/00060/2015, instruido por la Agencia Española de Protección de Datos a la entidad PLANET SWAPSEE, S.L., vista la denuncia presentada por D. ***A.A.A.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 22/01/2015, tuvo entrada en esta Agencia un escrito de D. ***A.A.A.*** (en lo sucesivo el denunciante), en el que denuncia a la entidad PLANET SWAPSEE, S.L. (en lo sucesivo PLANET SWAPSEE) señalando que el curriculum vitae (CV) que remitió a la plataforma de empleo online http://swapsee.com figura publicado en Internet, en su integridad y sin restricciones. Añade que pudo acceder a dicho documento a través de un enlace obtenido como resultado mediante el buscador Google, utilizando como criterio de búsqueda su nombre y apellidos.

Aporta los resultados de una búsqueda realizada con Google en fecha 19/01/2015, entre los que figura el enlace objeto de la denuncia, con el detalle de la URL que permite accede al CV del denunciante. En este enlace, además de la URL, se ofrece la indicación siguiente:

" A.A.A.. …….".

SEGUNDO: A la vista de los hechos denunciados, la Subdirección General de Inspección de Datos de esta Agencia, en fechas 27/01 y 06/02/2015, comprobó que el CV del denunciante con sus datos personales resultaba accesible al buscar en Google con su nombre y apellidos, en la carpeta ***B.B.B.***. Asimismo, se comprobó que el citado buscador indexó otros documentos almacenados en la misma carpeta, entre ellos varios CV, un certificado académico y una carta de presentación con datos personales relativos a otras personas.

Se incorpora a las actuaciones copia de los CV accedidos por la Agencia (seis CV), incluido el del denunciante, con detalle de sus datos identificativos, formación académica y experiencia profesional de los afectados.

Asimismo, se incorpora copia de la "Política de Privacidad" insertada en la web www.swapsee.com, en la que se indica, entre otras informaciones, lo siguiente:

"Swapsee utiliza los datos personales únicamente con finalidades administrativas. Además, parte de esta información se utilizará para la creación de un perfil público que quedará accesible a otros usuarios. El usuario es consciente y consiente por tanto el uso de sus datos personales con dicho fin, de acuerdo con el artículo 5 y 11 de la Ley 15/1999, de 13 de Diciembre Ley de Protección de Datos 1999...".

Y en el documento *"Condiciones del sitio web de Swapsee"* se indica:

"1. Definiciones
A los efectos de estos Términos y Condiciones Generales, este artículo define el significado de los siguientes términos y expresiones:

. Swapsee: la sociedad constituida bajo las leyes de España, Planet Swapsee, SL
. Condiciones Generales: estos términos y condiciones
. Website: the website bajo el dominio swapsee.com y/o otros websites propiedad o que sean administrados por Planet Swapsee, SL y bajo un dominio español, incluidas las herramientas incluidas en este website
. Usuario: persona que está registrada como miembro del website
. Editor: un usuario que publica un anuncio para un trabajo o una habilidad para todos o algunos usuarios o para un usuario específico.
. Trabajo: cualquier servicio, independientemente de su naturaleza jurídica solicitado por un editor y/o sujeto a un contrato de usuario
. Habilidad: cualquier habilidad o servicio, independientemente de su naturaleza jurídica, ofrecido por un editor y/o sujeto a un contrato de usuario
. Contrato de usuario: Un contrato celebrado entre los usuarios en relación a uno o varios trabajos
. Intercambio: el hecho de pagar un trabaja a través de la realización de otro a cambio…

4. Trabajos y habilidades: Contratos de usuario

1. Los contratos de usuario están suscritos por los usuarios y tienen como objeto la prestación de un determinado trabajo a cambio de dinero u otro trabajo (intercambio)
2. En caso de que se acuerde un precio en dinero, el contrato de usuario se materializa a través de:

1. la publicación de un trabajo por un usuario para todos o algunos usuarios o para un usuario específico,
2. la oferta de otro usuario en relación a ese trabajo
3. la consecuente aceptación de la oferta por parte del editor.

3. En caso de que se acuerde un intercambio, el contrato de usuario se materializa a través de:

1. la publicación de un trabajo por un usuario para todos o algunos usuarios o para un usuario específico,
2. la oferta de otro usuario de realizar un trabajo a cambio de otro,
3. la aceptación del trabajo propuesto a cambio del originalmente publicado…".

5. Subscripciones y Pagos

1. Los usuarios pagan a Swapsee por el uso de la página web en determinados momentos del proceso. Estos precios pueden variar y los detalles están disponibles en el website...".

8. Responsabilidad

1. Swapsee no es responsable del contenido de los mensajes publicados por los usuarios en el website, el no cumplimiento de los contratos de usuario, los daños causados por el incumplimiento de los contratos de usuario o del no cumplimiento de los impuestos u otro tipo de obligaciones legales por parte de los usuarios…".

TERCERO: Con fecha 23/03/2015, 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 PLANET SWAPSEE 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 LOPD,

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

Después de dos intentos de notificación por el Servicio de Correos, el citado acuerdo de apertura fue notificado mediante el procedimiento previsto en los artículos 59 y siguientes de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, concediéndose a PLANET SWAPSEE plazo para formular alegaciones, que transcurrió sin que en esta Agencia se haya recibido escrito alguno.

CUARTO: Con fecha 17/07/2015, la Subdirección General de Inspección de Datos comprobó que el CV del denunciante con sus datos personales permanecía accesible al buscar en Google con su nombre y apellidos, en la misma carpeta ***B.B.B.***, al igual que el resto de CV mencionados en el Antecedente Segundo.

HECHOS PROBADOS

1. La entidad PLANET SWAPSEE es titular del sitio web "www.swapsee.com".

2. El sitio web "www.swapsee.com" está diseñado como una plataforma para que los usuarios registrados inserten mensajes en la web ofreciendo sus servicios, de la naturaleza que sean, o contraten los de otros usuarios. Para ello, los interesados pueden facilitar información personal y profesional, incluido el CV, parte de la cual se puede utilizar *"para la creación de un perfil público que quedará accesible a otros usuarios"*, según se informa en la "Política de Privacidad" accesible a través de la citada web. Según las *"Condiciones del sitio web de Swapsee"*, se entiendo por *"Usuario"* cualquier *"persona que está registrada como miembro del website".*

3. El denunciante se registró como usuario de la web "www.swapsee.com" e incorporó su CV a la misma.

4. Con fecha 22/01/2015, se recibe en la AEPD un escrito del denunciante en el que informa que mediante el buscador de Internet Google, con su nombre y apellidos como criterio de la búsqueda, en fecha 19/01/2015, obtuvo como resultado un enlace a la web www.swapsee.com que daba acceso al CV que incorporó al registrarse como usuario de dicha web. En dicho enlace, además de la URL, se ofrecía la indicación siguiente:

" A.A.A.".

5. En fechas 27/01 y 06/02/2015, la Subdirección General de Inspección de Datos comprobó que el CV del denunciante, con sus datos personales, resultaba accesible al buscar en Google con su nombre y apellidos, en la carpeta ***B.B.B.***. Asimismo, se comprobó que el citado buscador indexó otros documentos almacenados en la misma carpeta, entre ellos varios CV (seis), un certificado académico y una carta de presentación, con datos personales relativos a otras personas (datos identificativos, formación académica y experiencia profesional de los afectados).

6. Con fecha 17/07/2015, la Subdirección General de Inspección de Datos comprobó que el CV del denunciante con sus datos personales permanecía accesible al buscar en Google con su nombre y apellidos, en la misma carpeta ***B.B.B.***, al igual que el resto de CV mencionados en el Hecho Probado Quinto..

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 artículo 18.4 de la Constitución Española establece en que: *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*", consagrándose así el derecho a la protección de datos como un derecho autónomo, incluso del propio derecho a la intimidad, tal y como ha indicado la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

El artículo 1 de la LOPD dispone: *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*

En cuanto al ámbito de aplicación de la citada norma, el artículo 2.1 de la misma señala que *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"*; definiéndose el concepto de dato de carácter personal en el artículo 3.a) de la citada LOPD como *"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 24/10/1995, 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 (en lo sucesivo la Directiva), según el cual se entiende por dato personal *"toda información sobre una persona física identificada o identificable; 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"*.

En el presente caso, ha quedado acreditado que el fichero accedido, atendiendo a su contenido (datos personales identificativos de los afectados y datos curriculares, con detalle de su formación y experiencia profesional), se encuentra incluido dentro del ámbito de aplicación establecido en la LOPD y sus normas de desarrollo.

III

El Titulo VII sobre *Infracciones y sanciones*, en 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."

El artículo. 3 de la LOPD establece las definiciones de responsable de fichero o

tratamiento y de encargado de tratamiento:

"d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".
"g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".

IV

Se imputa a la entidad PLANET SWAPSEE 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.

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 PLANET SWAPSEE, relativos a los usuarios de su web "www.swapsee.com", correspondiendo adoptar las de nivel básico en atención al tipo de información que contiene, tal como se especifica en los artículos 80 y siguientes 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, 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.

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 PLANET SWAPSEE está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas 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. En este caso, sin embargo, la citada entidad incumplió esta obligación, al haber quedado acreditada la posibilidad de acceder, sin restricción alguna, a los datos personales relativos a usuarios de su web contenidos en la carpeta ***B.B.B.***, que incluye los datos curriculares de varias personas que registraron sus datos personales a través de la web www.swapsee.com, con detalle de los datos personales identificativos, formación académica y experiencia profesional.

En concreto, consta en los Hechos Probados que el mencionado sitio web se configura como una plataforma en la que los usuarios pueden anunciarse ofreciendo sus servicios, y permite a los mismos registrarse como usuarios e incorporar sus CV y establecer un perfil público con algunos de esos datos accesibles, que queda accesible a otros usuarios. En esta plataforma los usuarios registrados pueden insertar mensajes en la web ofreciendo sus servicios, de la naturaleza que sean, o contratar los de otros usuarios.

Sin embargo, en relación con el denunciante y otras cinco personas, se comprobó el acceso por parte de terceros, sin restricción alguna, a datos personales y documentos curriculares de estos usuarios inscritos a través de la citada web, al haberse permitido su recopilación e indexación por buscadores de internet, que pudieron acceder a los documentos de las características señaladas que permanecían almacenados en la carpeta correspondiente al no haberse definido restricciones de acceso sobre los mismos. Los CV aportados por los afectados, incluido el denunciante, resultan accesibles a través de la web "www.swapsee.com" utilizando el buscador Google, según el detalle que consta en los hechos probados, siendo PLANET SWAPSEE, responsable del sitio web www.swapsee.com, la responsable de no haber definido restricciones de acceso para impedir que la información fuese indexada por buscadores de Internet.

En concreto, consta que, con fechas 27/01, 06/02 y 17/07/2015, a través de una búsqueda en Internet utilizando como criterio el nombre y apellidos del denunciante, se obtuvo como resultado un enlace al sitio web www.swapsee.com a través del cual se accedía al curriculum vitae incorporado por el mismo a dicha web, así como los del resto de afectados mediante una búsqueda de CV vinculado a sitio web.

Se trata de deficiencias apreciadas en el sistema de información diseñado por la propia entidad PLANET SWAPSEE, que quedaron acreditadas por la documentación aportada por el denunciante y por las comprobaciones realizadas por la Subdirección General de Inspección de Datos.

Así, los datos personales de los usuarios de la web "www.swapsee.com", resultaron accesibles por parte de 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 PLANET SWAPSEE ha incurrido en la infracción grave descrita. PLANET SWAPSEE es responsable de la infracción señalada, habiendo quedado justificada, al menos, una falta de la diligencia debida en los hechos constatados plenamente imputable a la misma.

Así lo ha declarado la Audiencia Nacional en un supuesto similar, examinado en la Sentencia de fecha 24/09/2010, en cuyo Fundamento de Derecho Séptimo se indica lo siguiente:

"A pesar de dichas alegaciones de la demanda y de conformidad con la normativa y la doctrina de esta Sala que se han expuesto en el fundamento jurídico anterior, consideramos que la infracción del deber de seguridad impuesta a XXX a tenor del artículo 9 de la LOPD, ha de ser

confirmada por la misma.
Y ello dado que dicha entidad actora, como encargada del tratamiento de los datos personales de la compañía de seguros, estaba obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas en la normativa de aplicación, respecto de los ficheros informáticos de aquella y, entre ellas, las dirigidas a impedir el acceso no autorizado de terceros a los datos de los solicitantes de seguros "on line", que eran los que se contenían en el fichero "clientes" de tal compañía de seguros, que, como se ha indicado, requerían medidas de seguridad de nivel alto.
Ha quedado acreditado, por el contrario, que XXX incumplió esta obligación, al posibilitar el acceso a datos de personas físicas sin que existiera un procedimiento de cifrado o cualquier otro que garantizara que la información obtenida en dichos accesos no podía ser identificada o manipulada por terceros, como pudo comprobar la Inspección de Datos, a través de la Web…
Consideramos, por todo ello, que XXX infringió lo dispuesto en el artículo 9 de la LOPD…".

La entidad PLANET SWAPSEE informó a los usuarios que se establecería un perfil público con parte de la información facilitada y únicamente a disposición de otros usuarios, y no la publicación de toda la información a disposición de terceros, sin restricción alguna. Por tanto, ha de entenderse que los afectados que registraron sus datos a través de la web de la citada entidad no consintieron que tales datos se pusieran a disposición de cualquier tercero.

Este acceso por terceros a los datos personales reseñados supone la comisión, por parte de PLANET SWAPSEE, 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.

V

En este caso, se concluye que PLANET SWAPSEE no había adoptado las medidas técnicas y organizativas apropiadas, habiéndose acreditado la existencia de una relación entre el acceso y la inexistencia o ineficacia de las medidas.

En todo caso, 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 la misma Sentencia citada en el Fundamento de Derecho anterior, así como en su Sentencia de 11/12/2008 (recurso 36/08), en la que indica lo siguiente: *"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).

Por otra parte, ha de señalarse que es la entidad PLANET SWAPSEE la responsable del fichero y, por tanto, la obligada última a garantizar la seguridad de los datos, asegurando la efectividad de las medidas adoptadas.

VI

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 PLANET SWAPSEE ha incurrido en la infracción grave descrita.

V

De acuerdo con lo expuesto, se iniciaron actuaciones contra la entidad PLANET SWAPSEE por la presunta vulneración del *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, que se tipifica como infracción grave en el artículo 44.3.h) de la LOPD: *"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"*.

Por otra parte, se tuvo en cuenta que la citada entidad PLANET SWAPSEE no ha sido sancionada o apercibida con anterioridad.

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".

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 por la incidencia denunciada.

Por otra parte, considerando que la información que ha motivado las actuaciones continúa accesible, procede requerir a la entidad PLANET SWAPSEE la adopción de nuevas medidas que

impidan que en el futuro pueda producirse de nuevo una infracción de lo dispuesto en el artículo 9 de la LOPD, estableciendo medidas correctoras adecuadas para impedir el acceso indiscriminado a los datos personales registrados en sus sistemas de información y en los equipos de su responsabilidad, evitando que resulten accesibles por parte de terceros, con el alcance expresado en los Fundamentos de Derecho anteriores. Deberá solicitar a Google la eliminación de las direcciones ***B.B.B.*** de la cache de los motores de búsqueda y adoptar las medidas pertinentes para impedir la indexación de la web por motores de búsqueda.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- APERCIBIR (**A/00060/2015**) a la entidad PLANET SWAPSEE, S.L. 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, respectivamente, y de conformidad con lo establecido en los artículos 36 y 37.a), f) y n) de la LOPD, que atribuye la competencia **al Director de la Agencia Española de Protección de Datos.**

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.- REQUERIR a PLANET SWAPSEE, S.L., de acuerdo con lo establecido en el apartado 6 del artículo 45 de la Ley 15/1999, para que en el plazo de un mes desde este acto de notificación:

2.1.- <u>CUMPLA</u> lo previsto en el artículo **9** de la LOPD. En concreto se insta al denunciado a adoptar, de manera efectiva, las medidas técnicas y organizativas que garanticen la seguridad de los datos personales, que impidan el acceso indiscriminado y sin restricciones por parte de terceros a los datos personales registrados en sus sistemas de información y en los equipos de su responsabilidad, y sin el consentimiento de los afectados, evitando que resulten accesibles por parte de terceros, con el alcance expresado. Deberá solicitar a Google la eliminación de las direcciones ***B.B.B.*** de la cache de los motores de búsqueda y adoptar las medidas pertinentes para impedir la indexación de la web por motores de búsqueda.

2.2.- <u>INFORME</u> a la Agencia Española de Protección de Datos del cumplimiento de lo requerido en el apartado anterior, aportando aquellos documentos en los que se ponga de manifiesto dicho cumplimiento.

Se le advierte que en caso de no atender el citado requerimiento, para cuya comprobación se abre el expediente de investigación **E/04738/2015**, podría incurrir en una infracción del artículo 37.1.f) de la LOPD, que señala que "*son funciones de la Agencia de Protección de Datos: f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la*

adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.", tipificada como grave en el artículo 44.3.i) de dicha norma, que considera como tal, *"No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma",* pudiendo ser sancionada con multa de **40.001 € a 300.000 €,** de acuerdo con el artículo 45.2 de la citada Ley Orgánica.

3.- NOTIFICAR el presente Acuerdo a la entidad PLANET SWAPSEE, S.L. y 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