Procedimiento Nº: A/00087/2013

RESOLUCIÓN: R/02327/2013

En el procedimiento A/00087/2013, instruido por la Agencia Española de Protección de Datos a la entidad ASOCIACIÓN UNIFICADA DE MILITARES ESPAÑOLES, vista la denuncia presentada por D. ***C.C.C.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 20 de junio de 2012, tuvo entrada en la Agencia Española de Protección de Datos un escrito de D. ***C.C.C.*** (en lo sucesivo el denunciante) en el que manifiesta que, al realizar una búsqueda a través de Google utilizando su número de DNI, entre los resultados aparece una referencia a "***B.B.B.***" que corresponde a un documento en formato "pdf" contenido en el Boletín Oficial de Defensa, de fecha DD1 de MM1 de AA1, en el que figuran los datos personales del denunciante junto con su relación profesional con el Ministerio de Defensa.
Asimismo, manifiesta que a través de esta URL ***B.B.B.***, modificando el campo de fecha (***FECHA.1) se accede al contenido completo de cada uno de los Boletines de Defensa que se publican.
El denunciante manifiesta que el Boletín Oficial de Defensa solamente es accesible para el personal del Ministerio de Defensa a través de la intranet del Organismo y que, sin embargo, a través de la web *¡Error! Referencia de hipervínculo no válida.* se accede al contenido completo de los boletines, en los que figuran los datos personales de militares.

El denunciante aporta impresión de la búsqueda realizada mediante el buscador Google en fecha 19/06/2012.

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

1. En fecha 21 de junio de 2012, desde la Inspección de Datos se verificó que modificando el parámetro de fecha en la URL indicada por el denunciante ***A.A.A.*** se obtiene el Boletín Oficial del Ministerio de Defensa completo de fecha DD de MM de AA. Los datos personales que figuran corresponden a: DNI, nombre y apellidos, fecha de antigüedad, situación, destino y localidad del destino.
2. Con fecha 26 de octubre de 2012, utilizando el número de DNI del denunciante en el buscador Google se obtiene una referencia a la URL ***B.B.B.*** y el siguiente literal "*No hay disponible una descripción de este resultado debido al archivo robots.txt de este sitio*". No obstante, se permite el acceso al documento pdf que contiene el Boletín Oficial del Ministerio de Defensa".
3. Con esta misma fecha, se comprueba que modificando el dato de fecha en la URL ***B.B.B.*** se accede al contenido completo de los boletines publicados en las fechas utilizadas para la búsqueda.
4. La titularidad del sitio web *¡Error! Referencia de hipervínculo no válida.* corresponde a la Asociación Unificada de Militares Españoles (en lo sucesivo AUME), tal y como consta en la

propia web.

En Acta de Inspección realizada en la entidad AUME en fecha 30 de octubre de 2012 consta lo siguiente:

5. La AUME es una entidad sin ánimo de lucro y con personalidad jurídica propia. Tiene como finalidad principal "*la satisfacción de los intereses sociales, económicos y profesionales de sus afiliados y la realización de actividades sociales que favorezcan la eficacia en el ejercicio de la profesión y a la deontología profesional de sus miembros*". Todos los afiliados tienen que ser militares españoles.
   AUME utiliza los dominios: ***F.F.F.*** y ***B.B.B.***.
6. Para el cumplimiento de sus objetivos y con objeto de facilitar el acceso a la información que se publica en el Boletín Oficial del Ministerio de Defensa, ponen en la web *¡Error! Referencia de hipervínculo no válida.* el contenido completo de los Boletines. AUME manifiesta que los Boletines son de acceso público, ya que el Ministerio de Defensa permite la adquisición de los mismos mediante una suscripción. En los propios Boletines se informa del precio de la suscripción, así como la dirección, teléfono, fax o correo electrónico donde se puede solicitar.
   Durante más de un año, AUME estuvo suscrita al Ministerio de Defensa para la obtención de los Boletines que publicaba posteriormente en su web. Actualmente los obtienen de la web *¡Error! Referencia de hipervínculo no válida.*.
   En la Inspección realizada se ha verificado la existencia de publicaciones de diferentes Boletines Oficiales del Ministerio de Defensa en la propia web de este Ministerio, en la dirección http://www.defensa.gob.es. No obstante, en esta web no se ha obtenido constancia de la existencia de la publicación de los Boletines Oficiales del Ministerio de Defensa de fechas DD de MM de AA y DD1 de MM1 de AA1.
   Asimismo, se comprueba que en el sitio web *¡Error! Referencia de hipervínculo no válida.* se oferta la descarga gratuita de los boletines oficiales del Ministerio de Defensa, para lo cual hay que registrarse como usuario. En dicha web figura que el Boletín Oficial de Defensa es una fuente de acceso público ya que según el artículo 3 de la LOPD "*tienen consideración de fuentes de acceso público […] y las listas de personas pertenecientes a grupos de profesionales que contenga únicamente los datos de nombre, título, profesión, actividad, grado académicos, dirección e indicación de su pertenencia al grupo. Asimismo, tiene carácter de fuentes de acceso público, los Diarios y Boletines y los medios de comunicación social*".
7. El acceso a la web *¡Error! Referencia de hipervínculo no válida.* obliga a la identificación y autenticación de los usuarios, por ello es necesario haberse registrado antes en el Sistema. Un usuario de la web no necesariamente es asociado a la AUME.
8. Respecto al motivo por el cual los datos de los Boletines son indexados por Google, lo que permite que dichos boletines sean de acceso público, AUME manifiesta que
   > En septiembre de 2012 aproximadamente, una persona contactó con AUME informando de que buscando en Google su nombre y apellidos junto con la palabra "*redmil*" aparecía una referencia a sus datos personales publicados en los boletines Oficiales del Ministerio de Defensa.
   >
   > Una vez comprobado que el buscador Google indexaba la información contenida en la web *¡Error! Referencia de hipervínculo no válida.*, pusieron en funcionamiento el protocolo estándar de exclusión robots.txt para que no rastree ese contenido.

   A este respecto desde la Inspección de Datos se había comprobado que, con fecha 26 de octubre de 2012, en el buscador Google y en la referencia ***B.B.B.*** constaba el literal "*No hay disponible una descripción de este resultado debido al archivo robots.txt de este sitio*".
   Asimismo, en la Inspección se verificó que, a través de Google, utilizando como argumento de búsqueda el DNI del denunciante, se encuentra una referencia al sitio web *¡Error! Referencia de hipervínculo no válida.* en la que figura la siguiente información "*No hay*

disponible una descripción de este resultado debido al archivo robots.txt de este sitio", no obstante, al señalar con un clik se accede directamente al Boletín Oficial del Ministerio de Defensa de DD1 de MM1 de AA1 en el que figuran los datos personales del denunciante.
También se ha verificado que la URL generada, en la cual consta la fecha del boletín, permite la modificación de dicha fecha, accediendo a otro Boletín. En la Inspección se realiza una modificación de la fecha a 25/11/2011 obteniéndose el Boletín Oficial del Ministerio de Defensa de dicha fecha.

9. En el transcurso de la Inspección, AUME ha deshabilitado el acceso a los Boletines Oficiales del Ministerio de Defensa publicados en la web *¡Error! Referencia de hipervínculo no válida.*, y manifiestan que hasta que no haya una resolución de la Agencia, el acceso a los boletines estará deshabilitado.
A este respecto, los inspectores realizan nuevamente una búsqueda, a través de Google, del DNI del denunciante verificando que la página no está disponible.
Asimismo, con fechas 14 de noviembre de 2012 y 8 de abril de 2013, desde la Inspección de Datos se realizan nuevamente una búsqueda, a través de Google, con el DNI del denunciante como criterio, verificando que la página no está disponible.

TERCERO: Con fecha 20/05/2013, el Director de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), acordó someter a la entidad AUME a trámite de audiencia previa al apercibimiento, en relación con la denuncia por infracción del artículo 9 de la LOPD, en relación con los artículos 91 y 93 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la citada Ley Orgánica, tipificada como grave en el artículo 44.3.h) de la misma norma.

Con tal motivo, se concedió a la entidad AUME plazo para formular alegaciones, recibiéndose escrito en el que dicha Asociación niega haber mantenido ficheros sin las debidas condiciones de seguridad y que, en cuanto tuvo conocimiento de la situación descrita, se adoptaron las medidas necesarias para evitar la continuidad de la situación negativa detectada, de modo que la acción de mantener no se llegó a producir. Entiende, por ello, que no se cumple el tipo establecido y tampoco se han señalado las condiciones de seguridad específicas infringidas.

HECHOS PROBADOS

1. AUME es una entidad sin ánimo de lucro y con personalidad jurídica propia. Tiene como finalidad principal "*la satisfacción de los intereses sociales, económicos y profesionales de sus afiliados y la realización de actividades sociales que favorezcan la eficacia en el ejercicio de la profesión y a la deontología profesional de sus miembros*". Todos los asociados son militares españoles.

2. La entidad AUME es titular del sitio web ***¡Error! Referencia de hipervínculo no válida.***. El acceso a esta web obliga a la identificación y autenticación de los usuarios previamente registrados. Un usuario de la web no necesariamente es asociado a la AUME.

3. Con fecha 19/06/2012, mediante una búsqueda a través de Google utilizando como criterio su número de DNI, el denunciante obtuvo una referencia a la URL "***B.B.B.***" que corresponde al Boletín Oficial de Defensa de 30/11/2011 en formato pdf, en el que figuran los datos personales del denunciante junto con su relación profesional con el Ministerio de Defensa.

4. La entidad AUME ha manifestado que en septiembre de 2012 manifiesta que en septiembre de 2012 pusieron en funcionamiento el protocolo estándar de exclusión robots.txt para impedir que los buscadores de internet rastreen el contenido de la web B.B.B..

5. Con fecha 26/10/2012, los Servicios de Inspección de la AEPD comprobaron que utilizando el número de DNI del denunciante en el buscador Google se obtenía una referencia a la URL ***B.B.B.*** y el siguiente literal "*No hay disponible una descripción de este resultado debido al archivo robots.txt de este sitio*". No obstante, se permitía el acceso al documento pdf que contiene el Boletín Oficial del Ministerio de Defensa.

6. Con fecha 26/10/2012, los Servicios de Inspección de la AEPD comprobaron que modificando el dato de fecha en la URL ***B.B.B.*** se accedía al contenido completo de los boletines publicados en las fechas utilizadas para la búsqueda.

7. Durante la Inspección realizada en fecha 30/10/2012, AUME deshabilitó el acceso a los Boletines Oficiales del Ministerio de Defensa publicados en la web ***¡Error! Referencia de hipervínculo no válida.***.

8. Con fechas 14/11/2012 y 08/04/2013, los Servicios de Inspección de la AEPD realizaron nuevamente una búsqueda, a través de Google, con el DNI del denunciante como criterio, verificando que la página B.B.B. no estaba disponible.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37.g) en relación con el artículo 36 de la LOPD.

II

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

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

III

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

El Art. 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"Seguridad de los datos:
Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

El Art 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:
1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

La LOPD, traspuso al ordenamiento interno el contenido de la Directiva 95/46. En el artículo 9 de la citada LOPD se dispone lo siguiente:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten la alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".

El trascrito artículo 9 de la LOPD establece el *"principio de seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado"* por parte de terceros.

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de *"fichero"* y *"tratamiento"* contenidas en la LOPD.

En lo que respecta al concepto de "*fichero*" el artículo 3.b) de la LOPD lo define como *"todo conjunto organizado de datos de carácter personal",* con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la *"comunicación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Asimismo, el artículo 3.a) de dicha Ley añade que se entenderá por datos de carácter personal *"cualquier información concerniente a personas físicas identificadas o identificables".* En este mismo sentido se pronuncia el artículo 2 a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que

respecta al tratamiento de datos profesionales y a la libre circulación de estos datos, que dispone *"toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".*

Para completar el sistema de protección en lo que a la seguridad afecta, el artículo 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros *"...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso, –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. Dichas medidas, deben salvaguardar la confidencialidad y seguridad de los datos de carácter personal, según el nivel que corresponda adoptar en atención a la naturaleza de la información que contiene el sistema de información de que se trate, tal como se especifica en el art. 80 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD. El artículo 81.1 del citado Reglamento señala que *"Todos los ficheros o tratamiento de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico"*.

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

El artículo 91 del citado Reglamento, aplicable a todos los ficheros y tratamientos automatizados, establece:

"Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y

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

Este artículo desarrolla las previsiones que deberá establecer el responsable del fichero para garantizar que los usuarios con acceso a datos personales o recursos, por haber sido previamente autorizados, sólo puedan acceder a tales datos y recursos. Para ello es necesario que se implanten mecanismos de control para evitar que un usuario pueda acceder a datos o funcionalidades que no se correspondan con el tipo de acceso autorizado para el mismo, en función del perfil de usuario asignado.

"Artículo 93. Identificación y autenticación.

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

El artículo 5.2.b) del citado Reglamento define la autenticación como el procedimiento de comprobación de la identidad de un usuario; y el mismo artículo, letra h), se refiere a la identificación como el procedimiento de reconocimiento de la identidad de un usuario. Corresponde al responsable del fichero o tratamiento comprobar la existencia de la autorización exigida en el citado artículo 91, con un proceso de verificación de la identidad de la persona (autenticación) implantando un mecanismo que permita acceder a datos o recursos en función de la identificación ya autenticada. Cada identidad personal deberá estar asociada con un perfil de seguridad, roles y permisos concedidos por el responsable del fichero o tratamiento.

En definitiva, la entidad AUME 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.

En este caso, consta que la entidad AUME es responsable del sitio web B.B.B. y que utiliza esta página para el cumplimiento de sus fines, restringiendo el acceso a la información que se inserta en la misma únicamente a usuarios que previamente se hayan registrado en su sistema como usuarios autenticados. Entre la información que difunde a estos usuarios autenticados figura el Boletín Oficial del Ministerio de Defensa.

Sin embargo, a partir de la denuncia que ha dado lugar a las actuaciones, se comprobó que la entidad AUME no había limitado el acceso al contenido de los boletines oficiales del Ministerio de Defensa por terceros no registrados como usuarios de la web, resultando que cualquier usuario que conociera la dirección web, en la que únicamente hacía falta modificar el número de boletín, podía acceder a los distintos documentos. Además, tampoco se había limitado el rastreo por los motores de búsqueda ocasionando la indexación por Google.

Así, al realizar una búsqueda en Google con el nombre del denunciante como criterio, resultaron accesibles los datos personales del mismo contenidos en el Boletín Oficial del Ministerio de Defensa de fecha 30/11/2011, que se encontraba disponible sin restricción en la URL "***B.B.B.***". Asimismo, consta que modificando el campo de fecha en dicha dirección se accedía al contenido completo de cada uno de los boletines publicados.

Por tanto, los hechos expuestos, en relación con el acceso por parte de terceros a datos personales del denunciante a través del sitio web B.B.B., cuya titularidad corresponde a AUME, que además pudieron ser indexados por buscadores de Internet, considerando las deficiencias de seguridad indicadas, suponen la comisión por parte de dicha entidad de una infracción del artículo 9.1 de la LOPD. Tales hechos se producen por un error en el sistema de información diseñado por la propia entidad. Dicho fallo posibilitó que los datos personales contenidos en Boletines Oficiales del Ministerio de Defensa publicados en la web ***¡Error! Referencia de hipervínculo no válida.*** permanecieran abiertos a cualquier persona y no exclusivamente a los usuarios registrados, según pretendía AUME.

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

Tales hechos quedaron acreditados por la documentación aportada por el denunciante, que incluía el detalle sobre el resultado de la búsqueda realizada a través de Google, y por las constataciones realizadas por los Servicios de Inspección de la Agencia Española de Protección de Datos, que constan detalladas en los Hechos Probados; y han sido reconocidos por la propia entidad imputada.

IV

En esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deben impedir, de forma efectiva, el acceso a la información por parte de terceros. Esta necesidad de especial diligencia en la custodia de la información por el responsable ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: *"Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor".*

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

de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone *"sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."*

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

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

V

La entidad AUME ha señalado que los boletines del Ministerio de Defensa son de acceso público. Sin embargo, según consta en la Orden núm. 74/2010, de 21 de diciembre, de ordenación del Boletín Oficial del Ministerio de Defensa, su difusión se lleva a cabo de forma restringida a través de la Intranet del Ministerio y por correo electrónico previa suscripción, correspondiendo a la Subdirección General de Publicaciones gestionar la base de datos y el envío de los correos (artículos 11 y 13).

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".

Los hechos expuestos, en relación con la puesta a disposición de terceros del Boletín Oficial de Defensa a través de la web de la entidad AUME, considerando las deficiencias de seguridad indicadas en los antecedentes y por haberse permitido la indexación por buscadores de internet, vulneran el *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, por lo que se considera que AUME ha incurrido en la infracción grave descrita.

VII

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

"*Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que*

concurran los siguientes presupuestos:

a) que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento".

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

"4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

a) El carácter continuado de la infracción.

b) El volumen de los tratamientos efectuados.

c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

d) El volumen de negocio o actividad del infractor.

e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

f) El grado de intencionalidad.

g) La reincidencia por comisión de infracciones de la misma naturaleza.

h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.

i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente".

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

Por otra parte, los Servicios de Inspección comprobaron que por parte de AUME se deshabilitó el acceso a los Boletines insertados en su web, hasta la resolución de las actuaciones, y que pusieron en funcionamiento el protocolo estándar de exclusión robots.txt para evitar la indexación de los contenidos por los buscadores de Internet.

Por tanto, se entiende que AUME ha adoptado las medidas correctoras adecuadas, siempre que exija el registro como usuario autenticado para acceder al contenido insertado en la web.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- APERCIBIR (**A/00087/2013**) a la entidad ASOCIACIÓN UNIFICADA DE MILITARES ESPAÑOLES con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con la denuncia por la infracción del artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de esta acto, según lo previsto en el artículo 46.1 del referido texto legal.

2.- NOTIFICAR el presente Acuerdo a la entidad ASOCIACIÓN UNIFICADA DE MILITARES ESPAÑOLES.

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

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