Expediente Nº: E/01915/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **FEDERACIÓ BALEAR DE MUNTANYISME I ESCALADA** en virtud de denuncia presentada por ***B.B.B.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 7 de marzo de 2017, tuvo entrada en esta Agencia escrito de D. ***B.B.B.*** (en lo sucesivo el denunciante) en el que denuncia los siguientes hechos:

En la web de la Federació Balear de Muntanyisme i escalada (http://www.fbmweb.com/), concretamente en la página para darse de alta (http://www.fbmweb.com/federat/) si se introducía el DNI de un federado, salían sus datos personales. En su caso, en fecha 13/11/2016 pudo acceder a todos sus datos (captura adjunta) después de introducir su DNI.

Manifiesta que estos mismos hechos han sido denunciados en la página web ***WEB.1 página en la que confeccionaron un listado de datos obtenidos a través de este procedimiento.
Aportan una impresión de pantalla de la citada página web en la que constan sus datos personales, entre los de otras personas.

Y, entre otra, anexa la siguiente documentación:
Impresión de pantalla del formulario de alta de la página web www.fbmweb.com conteniendo los datos personales del denunciante: nombre, apellidos, fecha de nacimiento, dirección postal, nacionalidad, teléfono y correo electrónico.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. Con fecha 14 de marzo de 2017 la Inspección de Datos accede a la página web ***WEB.1 obteniendo como resultado una página en la que invitan a denunciar las "*chapuzas*" de seguridad en la dirección de correo ***C.C.C.***@mail.com. No constan datos de carácter personal.
2. Con fecha 19 de mayo de 2017 la Inspección de Datos ha comprobado que a través de la página web www.fbmweb.com se accede al formulario de alta para miembro de la Federación Balear de Montañismo y escalada. Tras introducir en

el campo DNI el número de DNI del denunciante y pulsar el botón de alta, **no se obtiene ningún dato de carácter personal.**

3. Con fecha 3 de julio de 2017 la Inspección de Datos accede a la página web ***WEB.1/fbm y ***WEB.1 obteniendo como resultado el mensaje "NOT FOUND" (no encontrada).

4. Con fecha 19 de mayo de 2017 se solicita información a ***FEDERACIÓ BALEAR DE MUNTANYISME I ESCALADA***, teniendo entrada con fecha 22 de junio de 2017 escrito de su representante en el que manifiesta lo siguiente:

    1. Los datos personales que constan en la impresión de pantalla aportada por el denunciante junto al escrito de denuncia son los datos que constan en los ficheros de ***FEDERACIÓ BALEAR DE MUNTANYISME I ESCALADA*** que se corresponden con la ficha de federado.

    2. En relación al hecho de poder acceder a los datos de cualquier federado con su DNI, indican que esa entidad en fecha 14 de noviembre de 2016 sufrió un acceso fraudulento al servidor. Personas desconocidas entraron al servidor donde se encuentra alojada la página web www.fbmweb.com/federat que contenía los datos personales de todos los afiliados los cuales han sido publicados en la url ***WEB.1.

        El servidor fue bloqueado por el informático de la Federación y procedieron a interponer una denuncia el mismo día ante la Policía Nacional. Aportan copia de la denuncia interpuesta el día por el titular de la Federación

5. Con fecha 23 de octubre de 2017, la Inspección de Datos solicita a ***FEDERACIÓ BALEAR DE MUNTANYISME I ESCALADA*** mediante escrito, copia de la documentación que a continuación se relaciona, siendo la notificación electrónica puesta a disposición de la entidad produciéndose un rechazo automático trascurridos los 10 dias :

    1 Copia de la documentación que acredite las medidas de segundad implementadas en el ' servidor en el momento en que tuvo lugar el acceso no autorizado.

    2 Especificación detallada de las causas que han hecho posible la incidencia incluyendo información respecto de las condiciones que se dieron para que se hayan producido los hechos.

    3 Número de afiliados afectados por la incidencia.

    4 Descripción detallada de las acciones tomadas con objeto de minimizar los efectos adversos indicando fecha y hora de las medidas adoptadas.

    5 Descripción detallada de las acciones realizadas para la resolución final de la incidencia, incluyendo fecha y hora de las medidas.

    6 Copia impresa del Registro de Incidencias tal y como se estipula en el

Reglamento de Protección de Datos de Carácter Personal (Real Decreto 1720/2007, de 21 de diciembre.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

Establece el artículo 9 de la LOPD (…) "*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.

Por su parte, el artículo 3.a) de dicha Ley añade que se entenderá por datos de carácter personal "*cualquier información concerniente a personas físicas identificadas o identificable*s".

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.

III

Los artículos 91 y 93 del RDLOPD, 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 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.

IV

En el presente caso, tal como se hace constar en los antecedentes de la presente resolución, tras la realización de las actuaciones previas de investigación, no se ha podido verificar la existencia de datos de carácter personal en las páginas web que son objeto de denuncia.

Asimismo debe indicarse que la entidad denunciada no ha sido sancionada ni apercibida con anterioridad, por lo que de haberse acreditado la comisión de la

infracción podría aplicarse el procedimiento de apercibimiento previsto en el artículo 45.6 de la LOPD. Todo ello sin perjuicio de que, ni en ese caso hubiera procedido una resolución de apercibimiento con requerimiento de medidas correctoras, pues la incidencia había sido subsanada, procediendo igualmente el archivo de las actuaciones de acuerdo con la Sentencia de 29 de noviembre de 2013, (Rec. 455/2011), Fundamento de Derecho Sexto, pues no tendría sentido el citado requerimiento.

En definitiva, no existen elementos suficientes que permitan acreditar conducta alguna que pueda incluirse en las infracciones que recoge el Titulo VII de la LOPD.

Consecuencia de ello y de acuerdo al principio de presunción de inocencia previsto en los artículos 24 de la Constitución Española y 23.2 a) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la solución procedente en Derecho es el archivo de las actuaciones.

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO.- PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO.- NOTIFICAR la presente Resolución a **FEDERACIÓ BALEAR DE MUNTANYISME I ESCALADA** y ***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 Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora 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 este 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