Expediente Nº: E/07252/2012

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos en virtud de denuncia presentada por don ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 6 de noviembre de 2012, tiene entrada en esta Agencia un escrito de don ***A.A.A.*** en el que denuncia un fallo de seguridad en la tienda online de mobiliario http://www.conforama.es que ocasiona que resulten públicamente accesibles sus datos y los de otros clientes.

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. En fecha 7 de noviembre de 2012, desde la Inspección de Datos, se verificó que, tal y como exponía el denunciante, sus datos (nombre y apellidos, número de teléfono, dirección de correo electrónico y dirección postal) eran públicamente accesibles a través de una dirección web construida añadiendo el número de su pedido al literal http://www.conforama..... Asimismo se verificó que al sustituir el número de pedido por otros números se accedía a los datos de otros clientes que habían realizado los respectivos pedidos.

2. Durante la inspección realizada en fecha 11 de marzo de 2013 en el establecimiento de CONFORAMA ESPAÑA, S.A. (en adelante CONFORAMA) se tuvo conocimiento de que esta compañía tiene registrados, entre otros, los dominios *conforama.es* y *confoonline.es* a través de los cuales se accede a la tienda online de la compañía.

3. Según consta en Acta de inspección, CONFORAMA tiene suscrito un contrato de prestación de servicios con la empresa de nacionalidad portuguesa LMRL-MARKETING E COMUNICAÇAO, Lda. (en adelante LMRL), para el desarrollo y mantenimiento informático de sus páginas web, lo que conlleva, tal y como consta en el contrato, el acceso y tratamiento por parte de la empresa portuguesa a los datos de carácter personal de los que CONFORAMA es responsable. En el apartado 3c del contrato se prevé que la empresa portuguesa "*Adoptará, a tenor de lo dispuesto en el art. 9 de la LOPD, las medidas organizativas y técnicas pertinentes para garantizar la seguridad e integridad de los datos de carácter personal a los que tenga acceso, evitando su alteración, perdida, tratamiento o acceso no autorizado. En este sentido [LMRL] manifiesta expresamente que dispone de las medidas de seguridad correspondientes establecidas por el R.D. 1720/2007, de 21 de diciembre, en función del nivel de seguridad aplicable a los datos a los que habrá de acceder para la prestación del servicio a Conforama, tal y como se describe en el Anexo II*". En este anexo se aclara que LMRL "*implantará las medidas de seguridad de nivel BÁSICO, que es el nivel de seguridad que Conforama ha declarado en el fichero CLIECONF002 inscrito ante la Agencia Española de Protección de Datos*".

4. Según consta en Acta, la tienda online de CONFORAMA se puso en funcionamiento el 31 de octubre de 2012. Al ser detectada en esta misma fecha la incidencia que

permitía que los datos de los pedidos realizados fueran accesibles sin restricciones al añadir a la dirección web http://www.conforama..... el número de pedido correspondiente, CONFORAMA la notificó por correo electrónico a la compañía portuguesa encargada del tratamiento, LMRL, a las 18:45. La empresa portuguesa remitió un mensaje electrónico a CONFORAMA a las 19:07 de ese mismo día, informando de que la incidencia había sido solucionada.

5. No obstante, al tener conocimiento durante la Inspección de que en fecha 7 de noviembre de 2012 la Agencia había verificado que aún eran públicamente accesibles los datos de los clientes, CONFORAMA solicitó aclaración a LRML el mismo día de la inspección, recibiendo confirmación de que en realidad la incidencia fue finalmente corregida a lo largo del mes de noviembre.

6. Durante la inspección realizada en el mes de marzo de 2013 se verificó que desde la dirección http://www.confoonline.....1 se trasladaba el control a http://www.confoonline.....2, donde se solicitaba la identificación y autenticación de usuario. Además se verificó que si el proceso de identificación fallaba se devolvía un mensaje de error y no se permitía el acceso a datos.

7. En fecha 24 de julio de 2013 por la Inspección de Datos, se ha verificado que las direcciones IP asociadas a los servidores que alojan los sitios web relacionados con los dominios *conforama.es* y *confoonline.es* se ubican geográficamente en Lisboa, Portugal, estando asignado su uso al operador NFSI TELECOM, Lda.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) establece, en el artículo 2.1, su ámbito de aplicación: "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". Asimismo prevé: "*Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:*

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito."

El artículo 9 de la LOPD prevé, por su parte:

"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 su 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."

En el apartado 1.a) del artículo 3 del Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, se establece que se regirá por este texto legal todo tratamiento de datos de carácter personal, en particular:

"*Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.*

Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento."

Es preciso asimismo tener en consideración las previsiones que la Directiva 95/46/CE realiza en su artículo 17 al respecto de la seguridad de los tratamientos de datos de carácter personal. El apartado 3 de este artículo establece:

"La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste."

Se ha constatado por la Inspección de Datos que la compañía LRML, a la que CONFORAMA había encargado el desarrollo y mantenimiento de la tienda online, no implementó medidas de seguridad suficientes para asegurar la confidencialidad de los datos de los clientes, en contra del compromiso adquirido contractualmente. No obstante, el encargado del tratamiento no tiene su establecimiento en España, no resultándole aplicable a LRML el régimen sancionador previsto en el artículo 45 de la LOPD.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución a CONFORAMA ESPAÑA, S.A. y a don ***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.

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 este acto, según lo previsto en el artículo 46.1 del referido texto legal.

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