Procedimiento Nº: A/00112/2014

RESOLUCIÓN: R/01788/2014

En el procedimiento A/00112/2014, instruido por la Agencia Española de Protección de Datos a la entidad EDITORIAL MAD, S.L., vista la denuncia presentada por DÑA. ***A.A.A.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 27/06/2013, tuvo entrada en esta Agencia Española de Protección de Datos un escrito de Dña. ***A.A.A.*** (en lo sucesivo la denunciante) en el que se pone de manifiesto los siguientes hechos:

El día 26/06/2013, la denunciante realizó un pedido a través de la web www.mad.es, perteneciente a la entidad EDITORIAL MAD, S.L. (en lo sucesivo EDITORIAL MAD) Para finalizar la compra, previamente hay que verificar los datos personales y del pedido. En este momento el sitio web ofreció los datos de un tercero en lugar de los datos de la denunciante.

Con su denuncia aportó impresión de pantalla del acceso a la web en el que figuran datos de un tercero.

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 :

. Con fecha 18 de noviembre de 2013 se solicitó información a EDITORIAL MAD y de la respuesta recibida se desprende:

1. El procedimiento para la realización de un pedido en la web www.mad.es es el siguiente:

   Los usuarios seleccionan los artículos que desean comprar y acceden a la cesta para validar la compra.

   Tras validar la compra, el Sistema le muestra una pantalla en la que se solicita la dirección de correo electrónico y la contraseña, en el caso de que sean usuarios ya registrados, o la dirección de correo electrónico, en caso de ser nuevos usuarios.

   En caso de ser un usuario ya registrado, el Sistema muestra en un formulario los datos personales del mismo, con posibilidad de modificarlos.

   En caso de ser un usuario nuevo, el Sistema muestra un formulario en el que se solicitan al mismo sus datos personales.

   Por último, se muestra al cliente un resumen de la compra con los datos de: facturación, envío (en caso de ser necesario) y un detalle de la compra.

   Tras validar la información, se solicita el pago de la compra mediante el TPV, si se seleccionó el pago con tarjeta, o informándole de los siguientes pasos, en caso de ser compra contra reembolso.

El criterio para la identificación del usuario es la dirección de correo electrónico y como

autenticación la contraseña que el usuario proporciona en el proceso de alta.

Desde la Inspección de Datos, con fecha 29/04/2014, se accedió a la web www.mad.es y se verificó que para realizar un pedido por un nuevo usuario, el Sistema solicita la dirección de correo electrónico y posteriormente es necesario cumplimentar un formulario con los datos de: nombre y apellidos, NIF, dirección postal, teléfono, dirección de correo electrónico y contraseña, todos ellos obligatorios. Opcionalmente se puede cumplimentar la dirección de envío.

2. Respecto del motivo por el cual la denunciante ha tenido acceso a los datos de un tercero, EDITORIAL MAD manifestó que, tras recibir el requerimiento de la Agencia Española de Protección de Datos, notificaron la incidencia al equipo técnico de la compañía que determinó el siguiente diagnóstico:

   > El problema de seguridad fue localizado en el paso cuarto del proceso de compra y ocurría cuando dos usuarios navegan como nuevos usuarios y accedían a un recurso compartido que les asigna el identificador de cliente, quedando asignado este identificador para ambos usuarios, y por tanto accediendo ambos a la misma pantalla durante el paso cuarto del proceso de compra.
   >
   > La ocurrencia de este hecho se produce cuando acceden a dicho recurso compartido en escasos milisegundos, de ahí la dificultad en las labores de diagnóstico. Es una incidencia con un muy bajo porcentaje de ocurrencia.

   Como acción correctora se ha procedido, de forma urgente, a controlar el acceso al recurso compartido a través de un control por semáforo, deteniendo el acceso a este recurso compartido, mientras está siendo usado por otro usuario.

   EDITORIAL MAD manifestó que tanto la gestión del alojamiento del sitio web, como la gestión de los aplicativos de comercio electrónico son responsabilidad de la compañía.

3. EDITORIAL MAD ha aportado impresión del Registro de Incidencia en el que figura que, con fecha 20/11/2013, se notifica la incidencia de seguridad y con fecha 25/11/2013 consta que se actualiza "*el software de compra, mediante un parche corrector, para controlar el acceso al recurso compartido a través de un control por semáforo, deteniendo el acceso a este recurso compartido, mientras está siendo usado ya por otro hilo de ejecución*".

4. EDITORIAL MAD manifestó que la denunciante no ha contactado con la entidad para comunicar la incidencia

TERCERO: Con fecha 22/05/2014, 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 EDITORIAL MAD 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 EDITORIAL MAD plazo para formular alegaciones, que transcurre sin que se haya recibido escrito alguno.

HECHOS PROBADOS

1. EDITORIAL MAD es responsable del sitio web www.mad.es.

2. Con fecha 26/06/2013, la denunciante accedió al sitio web www.mad.es para adquirir unos libros. Durante el proceso de validación de la compra que la denunciante pretendía realizar, al requerir la confirmación de los datos del cliente y del pedido, el sistema ofreció los datos personales de un tercero en lugar de los correspondientes a la denunciante, con detalle de los relativos a nombre, apellidos, DNI, dirección del cliente y dirección de envío, producto adquirido y precio.

3. En su respuesta al requerimiento de información que le fue realizado por los Servicios de Inspección de la AEPD, la entidad EDITORIAL MAD admitió la incidencia reseñada en el Hecho Probado Segundo, informado que el problema de seguridad fue localizado en el paso cuarto del proceso de compra y ocurría cuando dos usuarios navegan como nuevos usuarios y accedían a un recurso compartido que les asigna el identificador de cliente, quedando asignado este identificador para ambos usuarios, y por tanto accediendo ambos a la misma pantalla durante el paso cuarto del proceso de compra.

4. En el Registro de Incidencias de la entidad EDITORIAL MAD consta anotada la incidencia reseñada en el Hecho Probado Segundo, con indicación de las medidas correctoras implementadas en fecha 25/11/2013. Consta que se actualiza *"el software de compra, mediante un parche corrector, para controlar el acceso al recurso compartido a través de un control por semáforo, deteniendo el acceso a este recurso compartido, mientras está siendo usado ya por otro hilo de ejecución"*.

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

La entidad EDITORIAL MAD está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales registrados en sus ficheros, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a tales datos.

En este caso, el acceso por parte de clientes del sitio web www.mad.es a datos personales de otros clientes contenidos en la base de datos de EDITORIAL MAD, pertenecientes también a usuarios del citado sitio web, podría supone la comisión, por parte de dicha entidad, de una infracción del artículo 9.1 de la LOPD, al haberse constatado que tales hechos se producen por un error en el sistema de información diseñado por la propia entidad, según ha reconocido la misma.

Dicho fallo posibilitó que la denunciante, al realizar una compra a través del mencionado sitio web, durante el proceso de validación de datos y del pedido, accediera a la información relativa a otro cliente y a su pedido, con detalle de datos personales relativos a nombre, apellidos, DNI, dirección del cliente y dirección de envío, producto adquirido y precio.

De acuerdo con lo expuesto, se iniciaron actuaciones contra la entidad EDITORIAL MAD por la presunta vulneración del *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, según el cual "*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*", en relación con lo dispuesto en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, concretamente en los artículos 91 y 93, que establecen lo siguiente:

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".

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".

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".*

Por otra parte, se tuvo en cuenta que la citada entidad EDITORIAL MAD no ha sido sancionada o apercibida con anterioridad por esta Agencia.

En consecuencia, de conformidad con lo establecido en el artículo 45.6 de la LOPD, se acordó someter a la entidad EDITORIAL MAD a trámite de audiencia previa al apercibimiento, en relación con la denuncia por infracción del artículo 9 de la LOPD.

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

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

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

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

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

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado artículo 45.6 de la LOPD, por lo que procedería apercibir a EDITORIAL MAD.

No obstante, los Servicios de Inspección de la AEPD han comprobado que dicha entidad ha adoptado medidas para evitar que los datos personales de los usuarios de la web puedan ser accedidos por otros clientes, habiendo actualizado *"el software de compra, mediante un parche corrector, para controlar el acceso al recurso compartido a través de un control por semáforo, deteniendo el acceso a este recurso compartido, mientras está siendo usado ya por otro hilo de ejecución"*.

En consecuencia, deben estimarse adoptadas ya las medidas correctoras pertinentes en el presente caso, por lo que debe procederse a resolver el archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la entidad denunciada, en aplicación de lo establecido en el artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- ARCHIVAR el procedimiento **A/00112/2014** seguido contra la entidad EDITORIAL MAD, 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.

2.- NOTIFICAR el presente Acuerdo a EDITORIAL MAD, S.L.

3.- NOTIFICAR el presente Acuerdo a DÑA. ***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 esta 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