Procedimiento Nº: A/00362/2015

RESOLUCIÓN: R/00250/2016

En el procedimiento A/00362/2015, instruido por la Agencia Española de Protección de Datos a la entidad INICIATIVAS DE COMERCIO ELECTRÓNICO, S.L., vista la denuncia presentada por D. ***A.A.A.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 12/12/2014, tuvo entrada en esta Agencia un escrito de D. ***A.A.A.*** (en lo sucesivo el denunciante), en el que declara lo siguiente:

<<…lo que me ha ocurrido cuando he accedido a mi bandeja de pedidos en el sitio de www.ciclotekstore.com
Lo que ha pasado es que en mi bandeja de pedidos había los pedidos de otras personas que no conozco, con todos los datos personales como son teléfonos, direcciones, nombres de personas, números de identificador tipo D.N.I, las cosas que compraron.
Algunas son incluso facturas de antes de que yo me registrara en esta web.
Me han bloqueado el acceso a mi perfil al sistema de Ciclotek. Cuando he contactado por teléfono para informar de la situación y pedir dónde están mis datos, me dicen que no lo saben.
Yo creo que esta es una situación grave y por eso llamé a Ciclotek y viendo que pasaban de todo (ni siquiera una llamada de confirmación) me han recomendado que lo ponga en conocimiento de la Agencia Española de Protección de Datos.
Y aquí tenéis todos los pantallazos que pude hacer antes de que me denegaran el acceso al sistema que ni siquiera me han enviado un mail para informarme de mi situación...>>.

Aporta copia de la siguiente documentación:

- Consulta al área de clientes de la web www.ciclotekstore.com, apartado de pedidos, en la que constan los pedidos números ******PEDIDO.1*** de fecha 11/12/2013, ******PEDIDO.2*** de fecha 14/02/2014, ******PEDIDO.3*** de fecha 18/08/2014 y ******PEDIDO.4*** de fecha 02/12/2014.
- Facturas de los pedidos números ******PEDIDO.4***, ******PEDIDO.2***, ******PEDIDO.3*** y ******PEDIDO.1***. En las mismas constan los datos de entrega, con detalle del nombre, DNI/NIF/NIE o número de identificación equivalente, dirección postal completa, teléfonos fijo, móvil y fax.

SEGUNDO: A la vista de los hechos denunciados, en fase previa de investigación, por los Servicios de Inspección de esta Agencia se llevaron a cabo las siguientes actuaciones:

1. En fecha 06/05/2015 se realizó visita de inspección a la entidad Globetek Universal, S.L. (en lo sucesivo GLOBETEK). Durante la misma, los representantes de la entidad realizaron las siguientes manifestaciones en respuesta a las cuestiones planteadas por los inspectores:

   a. Que en el momento de la inspección los administradores de la entidad no están en España y no se podrá tener acceso a toda la documentación, pues parte de ella está en sus manos.
   b. GLOBETEK dispone de una tienda on-line en la web, con varias direcciones

distintas, entre ellas www.ciclotekstore.com. El proveedor del servicio de dicha web es Iniciativas de Comercio Electrónico, S.L. (en lo sucesivo ICE). El mismo desde hace unos 5 años.

c. En la tienda on-line los usuarios se registran directamente, mediante una dirección de correo electrónico y una contraseña.
d. Los clientes introducen sus pedidos en la tienda, y una vez generado y pagado el pedido queda validado para su expedición. El cliente es informado automáticamente, mediante correo electrónico, de los cambios de estado del pedido, desde la recepción del mismo hasta su expedición.
e. Para la gestión de incidencias, existe un número de teléfono, anunciado en la web, una cuenta de correo electrónico tienda@....., que es gestionada por varias personas, y un sistema de tikets dedicado a las incidencias técnicas de los productos enviados, mediante el cual el propio usuario introduce en la tienda on-line las incidencias que observe. Este último sistema es el preferido por la entidad, y se intenta redirigir a los clientes hacia él, para que todo el seguimiento de las incidencias quede por escrito.
f. Solicitado el Documento de Seguridad y el Registro de Incidencias, informan que desconoce si existe dicho documento, en todo caso estará en poder de los administradores de la entidad.
g. Informan igualmente que desconoce si ha habido algún tipo de incidencia informática con la tienda electrónica.

2. Los inspectores de la Agencia accedieron a los sistemas de información de la entidad, realizando las siguientes consultas:

h. Se realiza una consulta al sistema contable sobre las facturas libradas por ICE durante 2014, comprobándose que constan doce facturas emitidas mensualmente por dicha entidad a GLOBETEK.

La factura aportada por la entidad recoge entre los conceptos "ComercioPlusM ciclotekstore.com". Visitada la web de ICE se comprueba que dicho producto es una tienda de comercio electrónico, en la que se puede realizar la gestión de clientes, proveedores, productos, pedidos, etc.

i. Se realiza una consulta respecto de pedido número ******PEDIDO.1***, comprobándose que dicho pedido fue realizado en fecha 11/12/2013 a las 23:53, constando como cancelado. En el detalle del pedido consta que la persona de contacto es ***B.B.B.***, del que constan NIE, dirección postal y número de teléfono móvil. Dicho pedido aparece asociado al cliente número ******CLIENTE.1*** del que no aparecen datos de facturación. El pedido fue realizado desde la dirección IP ******IP.1***.

Como dirección de entrega figura una dirección en ******LOCALIDAD.1*** (***Gerona***). Según la información de geoposicionamiento, la IP desde la que se hizo el pedido está ubicada en ******LOCALIDAD.2*** (***Barcelona***).

Se realiza una consulta respecto de pedido número ******PEDIDO.3*** comprobándose que dicho pedido fue realizado en fecha 18/08/2014 a las 00:52, constando como cerrado. En el detalle del pedido consta que la persona de contacto es ***C.C.C.***, del que constan dirección postal y números de teléfono fijo y móvil. Dicho pedido aparece asociado al cliente número ******CLIENTE.1*** del que no aparecen datos de facturación. El pedido fue realizado desde la dirección IP ******IP.2***.

Como dirección de entrega figura una dirección de ***Francia***. Según la información de geoposicionamiento, la IP origen del pedido está ubicada en ******LOCALIDAD.3*** (***Francia***).

Se realiza una consulta respecto de pedido número ******PEDIDO.2*** comprobándose que dicho pedido fue realizado en fecha 14/02/2014 a las 12:16, constando como cerrado. En

el detalle del pedido consta que la persona de contacto es ***D.D.D.***, del que constan NIF, dirección postal y números de teléfono fijo, fax y móvil. Dicho pedido aparece asociado al cliente número ******CLIENTE.1*** del que no aparecen datos de facturación. El pedido fue realizado desde la dirección IP ******IP.3***.

Como dirección de entrega figura una dirección de ***Portugal***. Según la información de geoposicionamiento, la dirección IP origen del pedido está ubicada en Portugal (el sistema no especifica ciudad concreta).

Se realiza una consulta respecto del pedido número ******PEDIDO.4*** comprobándose que dicho pedido fue realizado en fecha 02/12/2014 a las 14:05, constando como cancelado. En el detalle del pedido consta que la persona de contacto es ***A.A.A.***, del que constan NIF, dirección postal y número de teléfono móvil. Dicho pedido aparece asociado al cliente número ******CLIENTE.1***, que consta identificado como ***A.A.A.***. El pedido fue realizado desde la dirección IP ******IP.4***.

Como dirección de entrega del pedido figura un domicilio en ******LOCALIDAD.4*** (***Gerona***). Según la información de geoposicionamiento, la dirección IP origen del pedido está ubicada España (el sistema no aporta ciudad concreta).

j. Se realiza una consulta respecto al cliente ******CLIENTE.1*** verificándose que consta registrado con fecha 24/09/2013, con fecha de última modificación 03/12/2014 (16:51 horas) desde la dirección IP ******IP.5***.

Según la información de geoposicionamiento, dicha IP está ubicada en Fuzhou (China).

Se realiza una consulta a los pedidos de dicho cliente, encontrándose que figuran asociados a este cliente los pedidos números ******PEDIDO.1*** de fecha 11/12/2013, ******PEDIDO.2*** de fecha 14/02/2014, ******PEDIDO.3*** de fecha 18/08/2014 y ******PEDIDO.4*** de fecha 02/12/2014.

k. Se accede a la cuenta de correo electrónico tienda@....2 realizándose una búsqueda de los correos cruzados con la cuenta ***.....@hotmail.com*** encontrándose que hay un total de 14 correos electrónicos comprendidos entre el 01/08/2014 y el 03/12/2014.

Se encuentra que existe un correo electrónico remitido por GLOBETEK en fecha 01/08/2014 (12:44 h) en el que consta el correcto procesado de un pedido identificado con el número ******PEDIDO.5*** dirigido a D. ***A.A.A.***, cliente identificado con el código ******CLIENTE.2.***

Se encuentra un correo electrónico de fecha 03/12/2014 mediante el cual D. ***A.A.A.*** remite a GLOBETEK dos impresiones de pantalla en las que muestra que está teniendo acceso a los pedidos que no son suyos, y a los datos asociados a dichos pedidos.

l. Se realiza una consulta respecto del pedido número ******PEDIDO.5*** comprobándose que dicho pedido fue realizado en fecha 01/08/2014 a las 12:44, constando como cancelado. En el detalle del pedido consta que la persona de contacto es ***A.A.A.***, del que constan NIF, dirección postal y número de teléfono móvil. Dicho pedido aparece asociado al cliente número ******CLIENTE.2*** del que consta identificado como ***A.A.A.***. El pedido fue realizado desde la dirección IP ******IP.6***.

Consta en dicho pedido una dirección de entrega en ******LOCALIDAD.4*** (***Gerona***). Según la información de geoposicionamiento, la IP origen del pedido está ubicada en España (el sistema no da una población concreta).

m. Se realiza una consulta respecto al cliente ******CLIENTE.2*** verificándose que consta registrado con fecha 24/07/2014, con fecha de última modificación 03/12/2014 (17:04 horas) desde la dirección IP ******IP.7***.

Consta que dicho cliente tiene registrada una dirección en ******LOCALIDAD.4***. Según la información de geoposicionamiento, la IP de la última modificación está ubicada en España (el sistema no da una población concreta).

3. Se informa a los representantes de la entidad que el origen de la inspección ha sido una denuncia en la que un cliente de la misma informa haber tenido acceso a los datos de pedidos que no son suyos, en donde podía ver los datos personales asociados a dichos pedidos. Informan los representantes de la entidad que dicha incidencia fue resuelta mediante la desactivación del cliente, el traslado de la incidencia a ICE para su resolución, desconociendo el origen de la incidencia. No pueden aportar mayor información, debido a que fueron los administradores de la empresa los que llevaron el asunto.

4. Con posterioridad, GLOBETEK aporta copia de la siguiente información:

n. Copia del documento de seguridad.
o. Copia de la información recogida en el Registro de Incidencias respecto de la incidencia origen de esta inspección. En dicha incidencia se documenta: *<<El cliente nº* ******CLIENTE.2*** *indica que en su ficha de cliente accede a datos de pedidos que no le corresponden>>.*

Respecto de las causas se indica: *<<Desconocemos las causas, ya que este fichero no es gestionado por nosotros. Enviamos consulta técnica a Iniciativas de Comercio Electrónico (Proveedor de la tienda>>*
Entre las acciones correctivas se anota: *<<Desactivamos el registro* ******CLIENTE.2*** *y cambiamos las contraseñas, tal y como nos indican. No volvemos a registrar ninguna incidencia>>* (Este es el número de registro de usuario del denunciante).

p. Copia del contrato suscrito con ICE para la prestación del servicio de tienda de comercio electrónico. El contrato recoge expresamente: *<<12.2 ICE adopta las medidas técnicas y organizativas necesarias para garantizar la seguridad, integridad y confidencialidad de los mismos conforme a lo dispuesto en la Ley Orgánica 15/99 de 13 de diciembre, de Protección de Datos de Carácter Personal>>.*
q. Copia de todos los contactos habidos con ICE en relación con la incidencia. Según dichos contactos, en fecha 03/12/2014 GLOBETEK da una incidencia a ICE en la que informa:

<<nos refiere un cliente que tiene acceso a pedidos que él no ha hecho. Al investigar su pedido descubrimos una ficha de cliente con datos en blanco y correo electrónico y diversos pedidos asociados a distintos clientes.
Es todo muy extraño, el cliente "fantasma" (con pedidos a nombre de otros clientes) se ha dado de alta desde China, pero no entendemos qué está pasando.
¿Nos pueden ayudar?
Adjunto captura de pantalla con datos originales del cliente borrados>>

Por ICE se responde:
<<Si hay cambios que uno no ha hecho entonces tiene pinta que le han accedido a su base de datos de alguna manera, le recomiendo cambie todas sus contraseñas de acceso a la tienda, ftp y plesk, tenga en cuenta que una buena contraseña consta de al menos de 15 caracteres combinando números/letras mayúsculas y minúsculas. También revise en su alojamiento si ve algún fichero extraño que le hayan podido colar, si nos facilita datos de su ftp lo podemos mirar nosotros>>.

5. Mediante escrito de fecha 02/10/2015 se remitió solicitud de información a ICE en la dirección obrante en el contrato aportado por GLOBETEK, coincidente con la dirección que aparece en la web de ICE. La carta resultó devuelta por el servicio de Correos como “Desconocido”.

6. En fecha 20/10/2015 se da de alta en la web de ICE (www.comerciosonline.com) una incidencia mediante la que se solicita aporten dirección postal para el envío de una solicitud de

información. Dicha incidencia nunca fue contestada.
Mediante correos electrónicos de fecha 20 y 23/10/2015 se solicitó una dirección postal a fin de remitir nuevamente la solicitud de información. Los correos no fueron contestados.

7. Se solicitó información a Grupo Loading Systems S.L. referente a la dirección postal, teléfonos y correo electrónico de ICE. La dirección informada es coincidente con la recogida en el contrato aportado por GLOBETEK.
En fecha 06/11/2015 se realizó una llamada al número de teléfono de ICE aportado por Grupo Loading Systems S.L., identificándose una empresa distinta de ICE. Remitido correo electrónico a la dirección facilitada por dicha entidad, el sistema informa que la dirección de correo electrónico es incorrecta.

TERCERO: Con fecha 24/11/2015, la Directora 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 ICE a trámite de audiencia previa al apercibimiento por la presunta infracción del artículo 9 de dicha norma, 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.

Con tal motivo, se concedió a la entidad ICE plazo para formular alegaciones, que transcurrió sin que en esta Agencia se haya recibido escrito alguno.

HECHOS PROBADOS

1. La entidad GLOBETEK es titular del sitio web www.ciclotekstore.com. Se trata de una tienda on-line en la que los usuarios pueden registrarse para realizar pedidos, utilizando para ello una dirección de correo electrónico y una contraseña. Para la gestión de incidencias, existe un número de teléfono, la cuenta de correo electrónico tienda@..... y un sistema de tikets dedicado a las incidencias técnicas de los productos enviados.

2. El proveedor de servicios de la web www.ciclotekstore.com es la entidad Iniciativas de Comercio Electrónico, S.L., que proporciona a GLOBETEK el software de la tienda virtual, además del alojamiento de dominio, la ayuda y soporte ilimitado. Según consta en las Condiciones Generales de Contratación que rigen dicha prestación de servicio, Iniciativas de Comercio Electrónico, S.L. *"adopta las medidas técnicas y organizativas necesarias para garantizar la seguridad, integridad y confidencialidad de los mismos conforme a lo dispuesto en la Ley Orgánica 15/99 de 13 de diciembre, de Protección de Datos de Carácter Personal"* (Cláusula 12.2).

3. Con fecha 24/07/2014, el denunciante se registró como cliente de GLOBETEK a través de la web www.ciclotekstore.com. En los sistemas de información de esta entidad figura el denunciante con el número de cliente ******CLIENTE.2***, con detalle de sus datos personales relativos a nombre, apellidos, NIF, dirección postal y número de teléfono móvil. Asimismo, consta que con fecha 01/08/2014 realizó el pedido número ******PEDIDO.5*** (en la cuenta de correo electrónico tienda@....2 consta un correo electrónico remitido a la dirección del denunciante ***.....@hotmail.com***, de 01/08/2014, que da cuenta del correcto procesado del pedido identificado con el número ******PEDIDO.5***).

4. Por los Servicios de Inspección se accedió a la cuenta de correo electrónico tienda@....2,

constatando la existencia de un correo electrónico de fecha 03/12/2014 mediante el cual el denunciante remite a GLOBETEK dos impresiones de pantalla en las que muestra que está teniendo acceso a pedidos que no son suyos y a los datos asociados a dichos pedidos.

5. Con fecha 12/12/2014, la AEPD recibió un escrito del denunciante, en el que denunció que, a través del área de clientes habilitada en el sitio web www.ciclotekstore.com, pudo acceder a los pedidos de otros clientes de GLOBETEK y a los datos personales asociados a tales pedidos (teléfonos, direcciones, nombres, apellidos, números de identificador, D.N.I, artículos adquiridos), algunos anteriores a su registro en dicha web. En su denuncia indicó que informó sobre esta incidencia a GLOBETEK, que bloqueó su acceso al sistema.

El denunciante aportó impresión de pantalla correspondiente a los pedidos números ******PEDIDO.1***, de fecha 11/12/2013, ******PEDIDO.2***, de fecha 14/02/2014, ******PEDIDO.3***, de fecha 18/08/2014, y ******PEDIDO.4***, de fecha 02/12/2014, así como las facturas respectivas. En las mismas constan los datos de entrega, con detalle del nombre, DNI/NIF/NIE o número de identificación equivalente, dirección postal completa, teléfonos fijo, móvil y fax.

6. Por los Servicios de Inspección se accedió al sistema de información de GLOBETEK, comprobando que los datos personales del denunciante figuran asociados al cliente número ******CLIENTE.1***, al que corresponden los pedidos señalados con los números ******PEDIDO.1*** (en el detalle del pedido consta que la persona de contacto es un tercero y como domicilio de entrega una dirección de un municipio distinto al del denunciante)***; ***PEDIDO.3*** (la persona de contacto es ***C.C.C.*** y como dirección de entrega figura un domicilio de ***Francia***); ******PEDIDO.2*** (la persona de contacto es ***D.D.D.*** y como dirección de entrega figura una dirección de ***Portugal***); ******PEDIDO.4*** (la persona de contacto es el denunciante).
Se realizó una consulta sobre este cliente ******CLIENTE.1***, verificándose que consta registrado con fecha 24/09/2013 desde una IP ubicada en Fuzhou (China).

7. En el Registro de Incidencias de GLOBETEK consta una anotación con el siguiente texto: *"El cliente nº* ******CLIENTE.2*** *indica que en su ficha de cliente accede a datos de pedidos que no le corresponden".* Respecto de las causas se indica: *"Desconocemos las causas, ya que este fichero no es gestionado por nosotros. Enviamos consulta técnica a Iniciativas de Comercio Electrónico (Proveedor de la tienda".* Entre las acciones correctivas se anota: *"Desactivamos el registro* ******CLIENTE.2*** *y cambiamos las contraseñas, tal y como nos indican. No volvemos a registrar ninguna incidencia"*.

En relación con esta incidencia, con fecha 03/12/2014, GLOBETEK informó a Iniciativas de Comercio Electrónico, S.L.:
"Nos refiere un cliente que tiene acceso a pedidos que él no ha hecho. Al investigar su pedido descubrimos una ficha de cliente con datos en blanco y correo electrónico y diversos pedidos asociados a distintos clientes.
Es todo muy extraño, el cliente "fantasma" (con pedidos a nombre de otros clientes) se ha dado de alta desde China, pero no entendemos qué está pasando.
¿Nos pueden ayudar?
Adjunto captura de pantalla con datos originales del cliente borrados".

Por ICE se respondió:
"Si hay cambios que uno no ha hecho entonces tiene pinta que le han accedido a su base de datos de alguna manera, le recomiendo cambie todas sus contraseñas de acceso a la tienda, ftp y plesk, tenga en cuenta que una buena contraseña consta de al menos de 15 caracteres combinando números/letras mayúsculas y minúsculas. También revise en su alojamiento si ve algún fichero extraño que le hayan podido colar, si nos facilita datos de su ftp lo podemos mirar

nosotros".

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora 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*, 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 la definición de responsable de fichero o tratamiento y del encargado del 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".

III

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 de clientes de GLOBETEK relativos a teléfonos, direcciones, nombres, apellidos, números de identificador, D.N.I, artículos adquiridos), se encuentra incluido dentro del ámbito de aplicación establecido en la LOPD y sus normas de desarrollo.

IV

Se imputa a la entidad ICE 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.

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, 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 ICE.

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.

En definitiva, según las normas expuestas, y de acuerdo con las estipulaciones convenidas por ICE con la entidad GLOBETEK, a la que presta servicios como proveedor de la web www.ciclotekstore.com, según las cuales ICE se compromete a adoptar las medidas técnicas y organizativas para garantizar la seguridad de los datos, corresponde a esta última entidad impedir el acceso no autorizado por parte de terceros a los datos personales de los clientes de la tienda online registrados a través de dicha web. Sin embargo, ha quedado acreditado que la citada entidad incumplió esta obligación, al haberse constatado el acceso por parte del denunciante a través del área de clientes habilitada en la web citada, de la que es

usuario, a los pedidos de otros clientes y a los datos personales asociados a los mismos según los detalles reseñados en los Hechos Probados Quinto y Sexto.

Esta irregularidad, es decir, la posibilidad de que el denunciante pudiera acceder a la información de otros clientes debido a un fallo de seguridad ha sido reconocida por la propia entidad imputada y por GLOBETEK, según consta anotado en el Registro de Incidencias.

Así, los datos personales de algunos clientes de la tienda online resultaron accesibles por parte de terceros (el denunciante), 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 ICE, como encargada de la seguridad del sitio web www.ciclotekstore.com, ha incurrido en la infracción tipificada como 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"*.

V

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).

En definitiva, ha de señalarse que es la entidad ICE la obligada garantizar la seguridad de los datos, asegurando la efectividad de las medidas adoptadas.

VI

Por otra parte, se tuvo en cuenta que ICE no ha sido sancionada o apercibida con anterioridad por esta Agencia, así como el volumen de tratamientos afectados por la incidencia, la ausencia de beneficio y el grado de intencionalidad.

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".

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 imputada teniendo en cuenta el grado de intencionalidad, la ausencia de beneficios y el volumen de tratamientos afectados por la incidencia, así como la inmediata respuesta de ICE para subsanar la incidencia.

Todo ello, justifica que la AEPD no haya acordado la apertura de un procedimiento sancionador y que opte por aplicar el artículo 45.6 de la LOPD.

Ahora bien, es obligado hacer mención a la Sentencia de la Audiencia Nacional de 29/11/2013, (Rec. 455/2011), Fundamento de Derecho Sexto, que sobre el apercibimiento regulado en el artículo 45.6 de la LOPD y a propósito de su naturaleza jurídica advierte que "*no constituye una sanción"* y que se trata de "*medidas correctoras de cesación de la actividad constitutiva de la infracción"* que *sustituyen* a la sanción. La Sentencia entiende que el artículo 45.6 de la LOPD confiere a la AEPD una "*potestad"* diferente de la sancionadora cuyo ejercicio se condiciona a la concurrencia de las especiales circunstancias descritas en el precepto.

En congruencia con la naturaleza atribuida al apercibimiento como una alternativa a la sanción cuando, atendidas las circunstancias del caso, el sujeto de la infracción no es merecedor de aquella, y considerando que el objeto del apercibimiento es la imposición de medidas correctoras, la SAN citada concluye que cuando éstas ya hubieran sido adoptadas, lo procedente en Derecho es acordar el archivo de las actuaciones.

Como se ha señalado, en el asunto analizado, consta que se ha impedido el acceso por parte del denunciante a la información correspondiente a otros usuarios de la web www.ciclotekstore.com, habiendo desactivado el registro de usuario que dio lugar a la incidencia y modificado las contraseñas.

Por tanto, a la vista del pronunciamiento recogido en la SAN de 29/11/2013 (Rec. 455/2011) referente a los supuestos en los que el denunciado ha adoptado las medidas correctoras oportunas, de acuerdo con lo señalado se debe proceder al archivo de las actuaciones.

De acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1.- ARCHIVAR el procedimiento **A/00362/2015** seguido contra INICIATIVAS DE COMERCIO ELECTRÓNICO, 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 la entidad INICIATIVAS DE COMERCIO ELECTRÓNICO, 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.

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 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 esta 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