Expediente Nº: E/01327/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **TRAVELCONCEPT, S.L.U. (LOGITRAVEL)** en virtud de denuncia presentada por D. ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: En fecha de 16/02/2018 tiene entrada un escrito de D. ***A.A.A.*** (el denunciante en lo sucesivo) en el que pone de manifiesto los siguientes hechos:

Al comprar un billete de avión a través de LOGITRAVEL.COM accede a los datos de un tercero y, tras ponerse en contacto con la compañía por dicha circunstancia y por que los billetes que adquirió no se los enviaban, la entidad manifiesta que ha habido un "cruce de datos". Puesto en contacto con el tercero manifiesta que éste también ha accedido a sus datos y que los billetes del denunciante los tiene esta persona.

Y, entre otra, anexa la siguiente documentación:

> *Capturas de pantalla de la reserva realizada y del acceso a los datos del tercero con fotografía nombre y apellidos, teléfono dirección de correo, Comunicación a la Brigada de Investigación Tecnológica de la Comisaría General de Policía Judicial de que ha interpuesto denuncia ante la Comisaría del Cuerpo Nacional de Policía y comunicaciones con la entidad.*

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:

Mediante escrito de 13/03/2018 se solicita información a TRAVELCONCEPT, S.L.U (LOGITRAVEL) respecto de lo sucedido, así como las medidas que han adoptado, y se recibe escrito en fecha de 28/03/2018 en el que manifiestan, en síntesis, lo siguiente:

1. En fecha de 1/02/2018 a las 12:16h el tercero (el usuario en adelante) realizó una reserva con localizador ***LOC.1. Y le pasó al denunciante el enlace a su reserva, que contenía su código de sesión.
2. El mismo día, el denunciante hizo su reserva (localizador ***LOC.2) utilizando ese enlace. Lo que provocó la captura de la sesión del usuario con el resultado de que la reserva del billete del denunciante quedó registrado en la cuenta del usuario, resultando este último titular de las dos reservas.
3. Todo ello se desprende de los registros de los sistemas y de la llamada que el usuario realizó al call center el mismo día a las 15:07h con el contenido que se

puede leer en el registro de la incidencia que se adjunta, donde se reconoce expresamente que han hecho dos reservas y que se han pasado el link para reservar mismo vuelo y misma hora. Asimismo reconocen que son amigos.

4. El mismo día en que se tiene conocimiento de la incidencia, empiezan a realizarse las gestiones y averiguaciones oportunas para diagnosticar y solventar dicha situación, que queda resuelta técnicamente el día 2/02/2018, al cambiar el mecanismo por el cual se manda la sesión a la pantalla de pago.

5. Se comprueba que solamente afecta al apartado de la web relacionado con la línea de negocio de aéreo y en un punto solamente: cuando esta monta el link para pasar a la página de pago está pasando un parámetro de inicio de sesión, esta circunstancia produce que si se copia la URL y se comparte, se están pasando todos los datos mientras la sesión no ha caducado.

6. El día 2/02/2018 a las 8:00 se realiza una instalación con el siguiente cambio:

   -retirado el código de sesión del link en el salto a la página de pago.

Cuando el cliente accede a la página de pago desde la página previa se envían una serie de parámetro para poder recuperar la información que permita muestra la página al cliente con los productos seleccionados. Entre estos se encuentra el código de sesión del cliente. Este dato se estaba enviando en la URL por formato GET de tal forma que era visible, y se hizo un cambio para pasar este parámetro por formato POST, de tal manera que quedaba oculto, impidiendo así su copia.

El cambio principal es que antes cuando una persona enviaba la URL a otra, ésta podía ver la misma información que la primera, en cambio ahora la segunda persona no verá nada pues le saltará un error.

7. Aportan la descripción de las medidas de seguridad de los datos de los clientes, y de los procedimientos de acceso de los usuarios de la organización.

8. Las medidas de acceso para usuarios/clientes registrados en la web es mediante usuario y contraseña, y en el momento de pulsar el botón “iniciar sesión” se manda la información a un controlador interno que verifica si los datos son correctos. Si no lo son devuelve un error.

9. Aportan copia de las reclamaciones recibidas respecto de los hechos denunciados: Email emitido por el denunciante el 1/02/2018; denuncia presentada ante la policía en la misma fecha; email remitido por el denunciante el 13/02/2018 y contestación de la entidad mediante email de 16/02/2018.

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

Teniendo en cuenta el momento en el que se produjeron los hechos, la entidad denunciada estaba obligada al cumplimiento de lo dispuesto en el artículo 9 de la LOPD, que dispone:

"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".

El citado 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 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"*.

Es necesario analizar también las previsiones que el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el R.D. 1720/2007, de 21 de diciembre, prevé para garantizar que no se produzcan accesos no autorizados a los ficheros.

El artículo 81.1 de este Reglamento establece que "*Todos los ficheros o tratamientos 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.

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.

El citado Reglamento regula:

"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."

Asimismo el artículo 32.1.b) del Reglamento (UE) 679/2016 del Parlamento Europeo y del Consejo, de 27 abril, de protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, vigente cuando se produjeron los hechos aunque aplicable a partir del 25 de mayo de 2018, dispone: "*Seguridad del tratamiento. 1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento"

Así, la entidad TRAVELCONCEPT, S.L.U., como responsable del fichero de datos personales de sus clientes, está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y, entre ellas, las medidas dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros.

En el caso presente el denunciante ha comunicado que al comprar un billete de avión a través de LOGITRAVEL.COM accede a los datos de un tercero y, tras ponerse en contacto con la compañía por dicha circunstancia y porque los billetes que adquirió no se los enviaban, la entidad manifiesta que ha habido un "cruce de datos".

La entidad denunciada ha informado que el mismo día en que se tiene conocimiento de la incidencia, empiezan a realizarse las gestiones y averiguaciones oportunas para diagnosticar y solventar dicha situación, que queda resuelta técnicamente el día 2/02/2018, al cambiar el mecanismo por el cual se manda la sesión a la pantalla de pago.

Aportan la descripción de las medidas de seguridad de los datos de los clientes, y de los procedimientos de acceso de los usuarios de la organización.

El acceso para usuarios/clientes registrados en la web es mediante usuario y contraseña, y en el momento de pulsar el botón “iniciar sesión” se manda la información a un controlador interno que verifica si los datos son correctos. Si no lo son devuelve un error.

En conclusión, según las actuaciones previas realizadas por los servicios de inspección de esta Agencia, se constata que la entidad denunciada ha adoptado las medidas de seguridad adecuadas que garanticen la seguridad de los datos de carácter personal y, que impidan el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros

III

En todo caso, debe señalarse que, si bien estamos ante una incidencia en las medidas de seguridad de los datos personales de sus clientes debido a un acceso no autorizado por parte de terceros, la entidad denunciada al tener noticia de los hechos aquí expuestos ha comunicado a la Agencia que ha procedido a realizar las gestiones y averiguaciones oportunas para diagnosticar y solventar esta incidencia.

Pues bien, en atención a las citadas circunstancias se considera necesario subrayar que la Audiencia Nacional, en su Sentencia de 29 de noviembre de 2013, (Rec. 455/2011), Fundamento de Derecho Sexto, a propósito de la naturaleza jurídica de esta figura, 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- cuyo objeto es la imposición de medidas correctoras, la SAN citada concluye que cuando las medidas correctoras pertinentes ya hubieran sido adoptadas, lo procedente en Derecho será acordar el Archivo de las actuaciones.

En el presente caso y teniendo en cuenta las circunstancias del mismo, este organismo está facultado para, en lugar de iniciar la apertura de un procedimiento sancionador, apercibir al denunciado a fin de que adopte las oportunas medidas correctoras.

Sin embargo, atendiendo a los principios de intervención mínima y proporcionalidad que informan la capacidad de actuación de esta Agencia y teniendo en cuenta que las medidas correctoras que procedería imponer fueron ya adoptadas por iniciativa propia, en armonía con el pronunciamiento de la Audiencia Nacional recogido en la SAN de 29/11/2013 (Rec. 455/2011) debe acordarse el **Archivo** de las actuaciones de investigación practicadas.

IV

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:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a TRAVELCONCEPT, S.L.U. (LOGITRAVEL) 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 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