Expediente Nº: E/03731/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante SOCIEDAD CONJUNTA PARA LA EMISIÓN Y GESTIÓN DE MEDIOS DE PAGO, E.F.C., S.A. en virtud de denuncia presentada por don ***B.B.B.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 28 de junio de 2016 tiene entrada en esta Agencia un escrito de don ***A.A.A.*** en el que pone de manifiesto una posible quiebra de seguridad en el área de clientes del sitio web www.iberiacards.com, que permitiría a un cliente debidamente identificado y autenticado tener acceso a los extractos de movimientos de otros clientes, con solo modificar, a través del navegador, el código de cliente que figura claramente visible en la dirección web de acceso (URL).

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 6 de julio por la Inspección de Datos se verifican los hechos denunciados utilizando para ello las credenciales de un inspector que también es usuario del citado sitio web. No se halla constancia de que entre los extractos accedidos de otros clientes figuren datos que permitan identificar a los clientes afectados.
2. En fecha 22 de julio tiene entrada en la Agencia un escrito de SOCIEDAD CONJUNTA PARA LA EMISIÓN Y GESTIÓN DE MEDIOS DE PAGO, E.F.C., S.A., en respuesta al requerimiento de la Inspección. La financiera considera que no se ha producido ninguna vulneración en la confidencialidad de los datos personales de sus clientes, por cuanto, si bien era posible visualizar los movimientos realizados con una Tarjeta que no era la del cliente previamente autenticado, dichos movimientos no se mostraban en pantalla acompañados del nombre y demás datos personales del titular de la Tarjeta con la que se hicieron. Esto quiere decir, que si bien un cliente, alterando el normal uso de la web, podía acceder a movimientos de otras Tarjetas, en ningún caso la información mostrada identificaba a la persona que los realizó. También precisa que el uso malintencionado de la web en ningún caso permitía el acceso al área privada de otro cliente, sino simplemente a visualizar en pantalla los movimientos de otra Tarjeta y ello cuando se daban una serie de coincidencias. La financiera entiende que los datos personales de los clientes de Iberia Cards no han estado comprometidos en ningún momento, sin perjuicio de que efectivamente se podía acceder a movimientos de Tarjetas de una manera aleatoria, circunstancia ya corregida.
3. La financiera ha declarado que la incidencia se originó como consecuencia del rediseño de la web privada de Iberia Cards, que se puso en producción el 18 de febrero de 2016. Según expone, no se produce de forma automática, por deficiencias o errores informáticos en la Web privada, sino que para originarse deben existir acciones encaminadas a generarla y, para ello, el denunciante debe disponer de conocimiento técnico, que no se corresponde con el propio de un usuario normal.

4. En el escrito se exponen las correcciones aplicadas, aportándose documentación acreditativa al respecto.

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

El artículo 9 de la LOPD establece:

"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 Título VIII del Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, se detallan los requisitos de seguridad que han de reunir los ficheros y tratamientos de datos de carácter personal, en función de la tipología de los datos involucrados.

No obstante, en el artículo 2.1 de la LOPD se establece 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".* Es en el artículo 3.a) de la LOPD donde se define dato personal*: "Cualquier información concerniente a personas físicas identificadas o identificables".*

El artículo 5.1.o) del Reglamento define como persona identificable a *"toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados".*

En el presente caso no se ha hallado constancia de que, debido a la incidencia descrita, los datos eventualmente accedidos por terceros no autorizados pudieran ser atribuidos a personas identificadas o identificables.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

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

2. **NOTIFICAR** la presente Resolución a SOCIEDAD CONJUNTA PARA LA EMISIÓN Y GESTIÓN DE MEDIOS DE PAGO, E.F.C., S.A. y a don ***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 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 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