Expediente Nº: E/06584/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

Examinado el escrito presentado por **VODAFONE ESPAÑA. S.A.U.** relativo a la ejecución del requerimiento de la resolución de archivo de actuaciones de referencia E/07413/2013 dictada por el Director de la Agencia Española de Protección de Datos en el procedimiento, y en virtud de los siguientes

ANTECEDENTES DE HECHO

PRIMERO: Con fecha 07/11/2013, tuvo entrada en la Agencia Española de Protección de Datos (AEPD) un escrito de Dña. ***A.A.A.*** (en lo sucesivo la denunciante) en el que expone que cuando se llama al número de atención al cliente de VODAFONE ESPAÑA, S.A.U., (en lo sucesivo, VODAFONE) y se accede a los servicios de respuesta vocal es posible cambiar la información de la cuenta bancaria, acceder a los servicios contratados y modificarlos sin que exista "*ningún tipo de control de seguridad que permita asegurar que la persona que intenta tener acceso a la información es el titular de la misma"*, lo que considera contrario a la normativa de protección de datos.

Aporta la grabación de tres llamadas telefónicas dirigidas al Servicio de Atención al Cliente (SAC) de VODAFONE en fechas 03/07/2013 y 04/07/213, sin que se tenga conocimiento de la fecha de la tercera de ellas. Aporta también copia de los contratos de las líneas ******TEL.1*** (de fecha 26/03/2013), ******TEL.2*** (de fecha 27/02/2013) y ******TEL.3*** (de 26/02/2013) celebrados con VODAFONE.

SEGUNDO: Tras la realización de actuaciones previas de inspección para determinar la existencia de vulneración de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (en lo sucesivo LOPD), en fecha 30/10/2014 el Director de la Agencia Española de Protección de Datos (AEPD) dictó Resolución de archivo de actuaciones E/07413/2013, en la que acordó:

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

***2. REQUERIR** a VODAFONE ESPAÑA, S.A.U. para que refuerce su política de seguridad e informe, dentro del mes siguiente a la notificación de esta resolución, del cumplimiento de lo requerido. "*

El fundamento de derecho III de dicha resolución contenía las siguientes consideraciones:

"…

*De las consideraciones precedentes se **concluye que no existe en los hechos que se someten a nuestra consideración vulneración del deber de secreto,** pues la información relativa al importe de la deuda pendiente y a los números de teléfono de la*

denunciante se proporcionó a quienes habían cumplido las medidas de seguridad establecidas, a lo que se añade que la infracción del deber de secreto es una infracción de resultado, lo que exige que haya existido revelación de una información a quien la desconocía, circunstancias que no parecen concurrir en quien pertenece al círculo próximo de la afectada y conoce los datos necesarios para pasar la política de seguridad establecida para la autenticación del usuario.

Por otra parte, las grabaciones aportadas demuestran que VODAFONE aplicó en el presente caso las medidas de seguridad que tiene implementadas.

Se advierte también que la aplicación diligente de medidas de seguridad no es óbice para que puedan llegar a producirse situaciones irregulares, como cuando un tercero conoce los datos personales de un cliente y los utiliza ilegítimamente, de tal forma que consigue pasar la política de seguridad del responsable del fichero.

No obstante las consideraciones precedentes estimamos que VODAFONE ***debe reforzar su política de seguridad*** *incrementando el rigor que actualmente tienen las medidas implementadas de manera que* ***no puedan acceder a información o a realizar gestiones vinculadas al servicio contratado aquellas personas que, pese a haber superado los controles exigidos para la autenticación del usuario, no se identifiquen como titular de la línea o como su representante.***

Por tanto, ***se requiere*** *a esta entidad para que en el plazo de* ***un mes*** *desde la notificación de la presente resolución* ***rectifique*** *su política de seguridad en el sentido indicado* ***e informe a la AEPD*** *del cumplimiento de lo requerido, debiendo aportar a tal fin prueba documental de las nuevas medidas de seguridad adoptadas. Al efecto de comprobar el cumplimiento de lo requerido se abre el expediente E/ 06584/2014."*

TERCERO: En el marco de las Actuaciones Previas de Investigación E/06584/2014, acordadas por el Director de la AEPD a los efectos de constatar el cumplimiento de las medidas requeridas en la resolución de archivo de actuaciones E/07413/2013, VODAFONE remitió a la AEPD escrito referido a la política de seguridad de datos en el servicio de atención al cliente del que se concluye lo siguiente:

1. Existen dos niveles de seguridad según el objeto de la llamada, y si la persona es o no cliente y es un tercero, en cuyo caso asimismo se distingue si dispone del terminal del titular, o bien de sus datos.

2. Existen una serie de acciones para las cuales **no es necesario pasar ninguna política de seguridad por cuanto no se facilitan datos personales:**

- información de la línea (plan de precios, permanencia, penalización y programa de puntos, estado de activación, información general de la factura).
- activación y desactivación de servicios sin coste.
- reclamaciones relacionadas con el servicio,
- envío de duplicados de facturas (siempre a la dirección de facturación)
- confirmar el número de tarjetas SIM
- aplicar restricciones a la línea por robo o pérdida.

3. Existe una serie de acciones para las cuales **es necesario pasar la política de seguridad consistente en facilitar el DNI y/o palabra clave que una vez superada y efectuada la acción se envía un SMS de confirmación al cliente):**

- Activar, desactivar o modificar tarifas, productos y servicios con coste (se envía SMS de confirmación)
- Modificaciones en controles de consumo (se envía SMS de confirmación)
- Información de PIN y PUK
- Activar/modificar claves, reseteo de contraseña de mi VF y clase contestador
- Confirmación de datos personales del cliente (no se facilita información sobre nombre, DNI, domiciliación bancaria, dirección de facturación)
- Modificación de datos personales del cliente:(domiciliación bancaria se envía SMS de conformación), dirección de facturación, cambio de vía de pago, correo electrónico, teléfono de contacto)
- Envío de factura a distinta dirección , fax o correo electrónico que aparece en sistemas
- Canje de puntos (se envía SMS de confirmación)
- Cambio de número
- Eliminar cualquier restricción (se envía SMS de confirmación)
- Modificación datos de la factura: método de pago, ciclo de facturación, formateo factura
- Información y gestión de abonos con/sin reembolso
- Desactivar y aplicar restricciones de SMS, Premium, Pagos VF.
- Aplicar restricciones: servicios especiales, roaming, GPRS, WAP, MMS y llamadas en general (se envía SMS de confirmación)

4. Existe una acción para la cual **es necesario pasar la política de seguridad (facilitar el DNI y/o palabra clave y antigua dirección):**

- Modificar la dirección de facturación o dirección de envío del pedido terminal.

5. Reforzamiento de las medidas de seguridad consistentes en que ningún agente facilitará a ningún cliente números de teléfono completos de tal modo que si un cliente llama para pedir esa información el agente sólo puede dar los tres primeros números y el último.

CUARTO: En el presente supuesto, del examen de las medidas adoptadas por VODAFONE se constata la existencia de medidas de seguridad implementadas en el servicio de atención al cliente en la medida que, para acceder al fichero de clientes y facilitar información personal se exige al usuario sus datos personales (DNI y nombre y apellidos) así como palabra clave, en caso de que hubiera sido activada por el titular de los datos personales con lo que es éste el que en última instancia decide proteger el acceso a sus datos personales con un nivel reforzado de seguridad. Asimismo se acredita la existencia de una medida de refuerzo en al acceso a los datos consistente en el envío de SMS de confirmación en caso de determinadas acciones solicitadas por el usuario del citado servicio de atención al cliente que implican modificación de datos personales o un coste económico para el titular de los datos.

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 LOPD.

II

El artículo 9 de la LOPD bajo la rúbrica "*Seguridad de los datos*" 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."

Este precepto debe integrarse con la definición de "*datos de carácter personal"* y de *"tratamiento de datos*" que ofrece la LOPD en sus artículos 3, a) y 3, c), respectivamente: "*cualquier información concerniente a personas físicas identificadas o identificables*"; *"operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

A propósito de esta obligación impuesta por el artículo 9 de la LOPD es también necesario citar el artículo 93 de su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre, (RLOPD) relativo a la "*Identificación y autenticación*" que dispone:

"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"

A su vez el artículo 5.2, apartados b), c) y p), del RLOPD aclara que se entiende por "*Autenticación*" el "*procedimiento de comprobación de la identidad de un usuario" ;* por "*contraseña"* la *"información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario*"; y por *"Usuario" "el sujeto o proceso autorizado para acceder a datos o recursos".*

La importancia que tienen las medidas de seguridad en relación con el derecho

fundamental de protección de datos ha sido destacada por el Tribunal Constitucional, que ha indicado (por todas, SSTC 143/1994 y 197/2003) que un sistema normativo que autorice la recogida de datos, incluso con fines legítimos, y no contemple las garantías adecuadas frente a un uso potencialmente invasor de la vida privada del ciudadano a través de su tratamiento técnico vulneraría el derecho a la intimidad del mismo modo que lo harían las intromisiones directas en el contenido nuclear de ésta.

La Directiva 95/46 CE, del Parlamento Europeo y del Consejo, que se traspuso a nuestro ordenamiento jurídico por la LOPD establece en su artículo 17, bajo la rúbrica "seguridad del tratamiento" lo siguiente:

"1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar 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 autorizado, 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".

III

En supuesto presente, del examen de las medidas adoptadas por VODAFONE señaladas en el antecedente de hecho tercero, se constata que las medidas de seguridad implementadas en el acceso al fichero de clientes mediante el servicio de atención al cliente, reúnen los requisitos requeridos por la AEPD.

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 **VODAFONE ESPAÑA S.A.U.,** y 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 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 lo sucesivo LJCA), 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