Expediente Nº: E/02887/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **VODAFONE ESPAÑA S.A.U.,** en virtud de denuncia presentada por D. ***A.A.A.*** y en consideración a los siguientes

HECHOS

PRIMERO: Con fecha 22 de marzo de 2013, tuvo entrada en esta Agencia un escrito de D. ***A.A.A.*** (en lo sucesivo, el denunciante) en el que manifiesta que es cliente de VODAFONE ESPAÑA, S.A.U., (en lo sucesivo, VODAFONE o la denunciada) y que el 19 de marzo de 2013 recibió en su móvil, número ******TEL.1***, dos sms de su operadora: el primero informándole del número de *"su nueva clave de autorizado*" y el segundo de que habían ejecutado su petición de "*modificación de la dirección de facturación*". Puesto que el denunciante nunca solicitó estos cambios se puso en contacto con la denunciada que le informó de la existencia de una llamada telefónica solicitándolos y , según dice, que "*para realizar dichos cambios la llamada tenía que ser efectuada desde la propia línea".*

SEGUNDO: Tras la recepción de la denuncia, la Subdirección General de Inspección de Datos procedió a efectuar actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos que se reflejan en el Informe de Actuaciones Previas de Inspección que reproducimos:

<<ANTECEDENTES

Con fecha de 22 de marzo de 2013 tiene entrada en esta Agencia un escrito de ***A.A.A.*** *en el que declara:*

> *<<Soy cliente de VODAFONE y titular de la línea* ******TEL.1****. El día* ***19-03-2013*** *a las 17:43 recibí un SMS procedente de VODAFONE indicándome: "VF informa: su nueva clave de autorizado es* ******CLAVE.1****. Puede modificarla en cualquier momento en el área de clientes en vodafone.es/empresas." Y seguidamente otro SMS indicándome: "Su petición relacionada con la modificación de la dirección de facturación ha sido realizada". Inmediatamente me puse en contacto con la compañía y me informaron que habían llamado y realizado dichos cambios. Cuál fue mi asombro cuando en ningún momento había realizado llamada alguna para realizarlos. Me aseguraban que para realizar dichos cambios la llamada tenía que ser efectuada desde la propia línea. Tras pedirles explicaciones me informaron que lo pondrían en comunicación de un superior porque era un tema grave por ser datos personales, seguidamente me pidieron excusas por los problemas causados. Mi sorpresa aumentaría al día siguiente 20-03-2013 a las*

*08:47 cuando Recibo una llamada desde el Nº ***TEL.3 perteneciente a VODAFONE pidiéndome confirmación del pedido realizado el día anterior en mi nombre por un importe de 521+IVA (Nº PEDIDO *****NÚMERO.1**). Después de varias llamadas pidiendo explicaciones me informan que el mismo se ha realizado desde el número *****TEL.2** y con la dirección de envío **(C/.....1) Zaragoza** a la atención de **A.A.A.**.>>*

Aporta el denunciante copia de la siguiente documentación:

- *Dos mensajes SMS de fecha 19/3/2013 (17:43 h.) emitidos desde el número 22167. En el primero de ellos consta:*

  *<<VF informa: su nueva clave de autorizado es *****CLAVE.1**. Puede modificarla en cualquier momento en el área de clientes en vodafone.es/empresas.>>*

  Y en el segundo:

  <<Su petición relacionada con la modificación de dirección de facturación ha sido realizada.>>

- *Impresión de pantalla del área de Clientes de Mi VODAFONE en el que constan los detalles del pedido* ***NÚMERO.1 *de fecha 19/3/2013, en estado finalizado. Consta que se trata de la compra de un iPhone 5 con contrato de permanencia de 24 meses por importe de 521 € y 400 puntos.*
- *Hoja de reclamaciones presentada el 20/3/2013 ante la OMIC del Ayuntamiento de Chiclana de la Frontera por los mismos hechos.*
- *Denuncia presentada en fecha 20/3/2013 en el cuartel de la Guardia Civil de Chiclana de la Frontera por los mismos hechos.*

ACTUACIONES PREVIAS

1 En fecha 24/2/2013 se realizó visita de inspección a VODAFONE durante la cual los inspectores de la Agencia solicitaron al representante de la entidad que les permitiese el acceso a sus sistemas de información en donde se realizaron las siguientes comprobaciones:

a. *Se realiza una consulta relativa al pedido de fecha 19/3/2013 y número* ***NÚMERO.1 *comprobándose que está asociado al cliente D. **A.A.A.**, con NIF *****CLAVE.141Y** y con domicilio en Chiclana de la Frontera. El pedido consiste en un terminal telefónico iPhone 5, por importe de 521 € y 400 puntos. Como número de contacto consta el teléfono *****TEL.2** y como domicilio de entrega **(C/.....1)** Zaragoza.*

b. *Se realiza una consulta en el sistema de pagos, verificándose que a D. **A.A.A.**, con NIF *****CLAVE.141Y** se le anotó el importe del terminal por 521€ en fecha 19/3/2013, con pago aplazado en 24 mensualidades, realizándose una posterior cancelación por el mismo importe, en fecha 27/5/2013.*

c. *Se realiza una consulta en el histórico de puntos de D. **A.A.A.**, observándose que en fecha 19/3/2013 le fueron descontados 400 puntos, que fueron posteriormente reintegrados, en fecha 30/4/2013.*

d. *Se accede al sistema de gestión de contactos con los clientes, en donde se observa que existen cuatro casos abiertos a nombre de D.* ***A.A.A..***

- *Caso de fecha 20/3/2013, en el que consta una petición de cancelación del pedido* ***NÚMERO.1 *por posible fraude.*

- *Caso de fecha 21/3/2013 consta que se ha enviado un terminal a la dirección en* ***(C/.....1) Zaragoza*** *cuando el cliente vive en Chiclana de la Frontera (Cádiz). Se procede a abrir caso de fraude. En una nota de la misma fecha consta que el caso ha sido calificado como fraude, cerrándose el caso.*

- *Caso de fecha 27/3/2013, el cliente informa que le han pasado la política de seguridad, haciéndose pasar por él, le han cambiado la clave de seguridad y la dirección de facturación, además de haber realizado un pedido a su nombre por 521 €. Este caso presenta numerosas notas, figurando entre ellas una reclamación a través de la OMIC.*

- *Caso de fecha 26/4/2013, en el que el cliente expone nuevamente la queja, informando que todavía está a la espera de respuesta.*

e. *Se accede al sistema de interacciones con el cliente, realizándose una consulta de las interacciones realizadas por D.* ***A.A.A.****, encontrándose que existen numerosas interacciones. Se procede a un filtrado de las interacciones ocurridas entre el 19/3/2013 y el 30/4/2014, encontrándose que:*

- *En fecha 19/3/2013 se recibió una llamada en VODAFONE por la que se realizó el reinicio (reseteo) de la clave del cliente así como el cambio de dirección de facturación.*

- *En la misma fecha se le manda al cliente un mensaje con el texto informativo de la nueva clave.*

- *En la misma fecha, se informa al cliente que la dirección de facturación ha sido cambiada.*

- *En la misma fecha, el cliente informa a VODAFONE que ha recibido un SMS al producirse un cambio en la clave de seguridad, cambio que no ha solicitado. El operador pasa política de seguridad al cliente, verificando que es el propio titular, y vuelve a modificar la clave.*

- *Seguidamente aparece la anotación del pedido* ***NÚMERO.1 *de compra de un terminal telefónico: según el operador, el cliente desea solicitar un nuevo terminal, el operador le indica el iPhone 5 y se lo manda.*

- *En la siguiente interacción, de fecha 20/3/2013, aparece que el cliente, tras pasar la política de seguridad, indica que no ha solicitado*

ningún terminal, el operador ve interacción del departamento de bajas con el ofrecimiento del mismo.

*f. Se realiza una consulta respecto al titular de la línea número *****TEL.2**, facilitada como contacto en la adquisición fraudulenta del terminal telefónico, encontrándose que se encuentra a nombre de una persona domiciliada en **(C/.....1)** Zaragoza. No se recaba copia de dicha consulta, a tratarse de una persona distinta del denunciante.*

2 Los representantes de VODAFONE realizan las siguientes manifestaciones en respuesta a las cuestiones planteadas por los inspectores:

*a. La persona que suplantó al denunciante disponía de información suficiente del mismo para poder realizar la suplantación, de forma que pasó las políticas de seguridad de la entidad. Según la política de seguridad se requiere facilitar o bien una contraseña o bien el conjunto de datos compuesto **por nombre y apellidos, NIF, entidad bancaria de domiciliación de pagos y dirección de facturación.***

b. El departamento de fraude de VODAFONE detectó y clasificó diligentemente el caso como fraude, de forma que le fueron reintegrados al denunciante los puntos así como se le realizó el abono del importe adeudado.

c. Entiende la entidad que el denunciante no ha sufrido menoscabo alguno de sus derechos, siendo la propia VODAFONE la entidad perjudicada en el caso.

d. Aportan copia de un documento en el que se recogen las políticas de seguridad de la entidad.

3 Solicitada a VODAFONE que aportase la grabación de la conversación en la que se produjo la suplantación de la identidad del denunciante, en la que se realizó el cambio de dirección de facturación y en la que se realizó el pedido del terminal telefónico iPhone 5, dicha grabación no ha sido aportada en el plazo concedido.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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

La LOPD se ocupa en su artículo 9 de la "*Seguridad de los datos*" y 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".

La Directiva 95/46/CE, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos cuya trasposición al ordenamiento interno español se llevó a cabo a través de la LOPD, establece en su artículo 17.1:

"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".

En el mismo sentido, el artículo 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, señala: *"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."*

En definitiva, el artículo 9 de la LOPD recoge el "*principio de seguridad de los datos*" que impone a los responsables de los ficheros y a los encargados de tratamiento la obligación de adoptar las medidas de índole técnica y organizativa que eviten la alteración, pérdida, tratamiento o acceso no autorizado a los datos que obran en sus ficheros.

El Tribunal Constitucional ha destacado la importancia de estas medidas protectoras al declarar (SSTC 143/1994 y 197/2003) que un sistema normativo que autorizase la recogida de datos, incluso con fines legítimos y de contenido aparentemente neutro, pero no incluyese garantías frente a un uso potencialmente invasor de la vida privada del ciudadano a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta.

Para poder delimitar cuáles son los accesos que la LOPD pretende evitar al exigir que se adopten determinadas medidas de seguridad es preciso examinar las definiciones de "*fichero*" y "*tratamiento*" contenidas en la Ley Orgánica 15/1999.

El artículo 3.a) de la LOPD define los ficheros como "*todo conjunto organizado de datos de carácter personal*" con independencia de la modalidad de acceso al mismo. La letra c) del artículo 3 considera tratamiento de datos cualquier operación o procedimiento técnico que permita –por lo que atañe al presente expediente-, la "*conservación*", "*consulta*", o "*modificación*" de los datos personales, tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.

El desarrollo reglamentario de la LOPD se llevó a cabo por el Real Decreto 1720/2007, de 21 de diciembre, (en lo sucesivo RLOPD), cuyo Título VIII se ocupa "*De las medidas de seguridad en el tratamiento de datos de carácter personal*".

El artículo 79 del RLOPD impone a los responsables de los ficheros y a los encargados de tratamiento la obligación de implantar medidas de seguridad en los términos previstos en su Título VIII. Estas medidas se clasifican en tres niveles: básico, medio y alto. Y añade que las medidas de seguridad de nivel básico deben adoptarse en "*todos*" los ficheros o tratamientos de datos de carácter personal.

De estas medidas de nivel básico se ocupan los artículos 89 a 93 del RLOPD (sección 1ª del capítulo III del Título VIII). El artículo 93 del RLOPD dispone en relación a la "*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."

II

Corresponde examinar en el asunto que nos ocupa si VODAFONE incumplió el artículo 9 de la LOPD en relación con el artículo 93.1 del RLOPD; esto es, si los mecanismos que la entidad denunciada tiene implementados fueron los correctos para garantizar la autenticación de los usuarios que accedieron a sus sistemas y si estos fueron efectivamente aplicados.

La política de seguridad adoptada por VODAFONE con este fin, de la que se ha tenido conocimiento con ocasión de la inspección practicada en su sede, contempla mecanismos diferentes según cuál sea la acción que el usuario quiere realizar.

Así, cuando el cliente pretende dar de alta o modificar ("*resetear*") su clave de seguridad el protocolo establecido exige cumplir dos condiciones: Por una parte, facilitar la clave o los siguientes tres datos (lo que denomina la entidad *"política larga"*): NIF o CIF, el nombre de la entidad bancaria en la que se gestionan los pagos con VODAFONE y la dirección de facturación. Y por otra parte *"hay que verificar que el cliente llame desde un teléfono de la empresa"*.

Si la acción que el cliente desea llevar a cabo es la "*modificación de sus datos*", hipótesis en la que se incluye el cambio de los datos de facturación al que se refiere el denunciante, la política de seguridad establecida consiste en recabar del usuario bien la clave o bien, si no se dispone de clave, los tres datos a los que la entidad se refiere con el nombre de "*política larga*".

En el presente caso las medidas de seguridad adoptadas se han demostrado suficientes para entender cumplidas las obligaciones que los artículos 9 de la LOPD y 93

del RLOPD imponen a los responsables de los ficheros.

Así, a tenor de lo manifestado por el denunciante, con cada una de las modificaciones de sus datos personales registradas en los ficheros de VODAFONE la denunciada le envió un sms. Cuando se produjo el primer cambio –el relativo a la clave de seguridad- se comunicó al denunciante -vía sms- la nueva clave.

Estos hechos evidencian que las medidas de seguridad implementadas funcionaron en la práctica y que son acordes con las normas jurídicas citadas. A mayor abundamiento debemos subrayar que con ocasión de la inspección practicada en la sede de VODAFONE se comprobó que el día 20 de marzo de 2013 la denunciada había ordenado la cancelación del pedido hecho por quien, todo indica, suplantó la identidad del denunciante y gestionó los cambios en sus datos personales. Esto es, solo un día después de que el denunciante, alertado por los sms, se pusiera en contacto telefónico con la denunciada. Igualmente se ha acreditado que el 30 de abril de 2013 VODAFONE reintegró al denunciante los puntos cliente que le había descontado y que bastó una única llamada del denunciante para que la operadora detectara la situación irregular y la calificara de posible fraude.

La aplicación diligente de unas medidas de seguridad adecuadas no es óbice para que se produzcan situaciones irregulares, como ocurre cuando un tercero conoce los datos personales de un cliente y los utiliza ilegítimamente logrando con ello pasar la política de seguridad del responsable del fichero. En tal hipótesis, contrarrestada además por el envío de un sms de aviso al cliente, no sería admisible exigir responsabilidad sancionadora por vulneración del artículo 9 de la LOPD, infracción tipificada en el artículo 44.3.h), pues esto supondría en la práctica una exigencia de responsabilidad objetiva proscrita en nuestro ordenamiento jurídico (Sentencia del Tribunal Constitucional 76/1990/ y artículo 130 de la Ley 30/1992).

Las consideraciones precedentes evidencian que los mecanismos de seguridad implementados por VODAFONE funcionaron en la práctica correctamente, por lo que corresponde ordenar el archivo de estas actuaciones.

Por lo tanto, de conformidad con lo señalado,

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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **VODAFONE ESPAÑA S.A.U.,** y a D.***A.A.A.***.

De acuerdo 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 este 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