Expediente Nº: E/05302/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **ORANGE ESPAGNE, S.A.U.,** en virtud de seis denuncias presentadas en este organismo y en consideración a los siguientes

HECHOS

PRIMERO: Han tenido entrada en la Agencia Española de Protección de Datos un total de seis denuncias dirigidas contra **ORANGE ESPAGNE, S.A.U**. (en lo sucesivo ORANGE o la denunciada) que aluden a la presunta vulneración por esta operadora del deber de secreto y/o del deber de seguridad de los datos al haber permitido que un tercero accediera a la cuenta de uno de sus clientes, cambiara contraseña y datos y accediera a sus facturas teniendo conocimiento por esta vía tanto de los datos personales del titular de la línea telefónica como del teléfono de sus contactos.

El detalle de las denuncias recibidas es el siguiente:

1. De 26/07/2013, en la que el **denunciante 1** expone que desde febrero de 2013 está siendo acosado, insultado y amenazado a través sms enviados desde el teléfono de un tercero que, según dice, obtuvo su número al acceder al contrato que ***A.A.A.*** tiene suscrito con ORANGE y a su facturación.
2. De 05/07/2013, en la que la **denunciante 2, *A.A.A..,*** expone que desde agosto de 2012 está siendo amenazada, acosada e insultada por una señora que también ha suplantado su identidad y publicado en internet videos que la relacionan con hechos delictivos. Añade que "*le consta*" que esta persona ha accedido a su contrato de telefonía con ORANGE y a sus facturas y ha modificado las condiciones de contratación. Advierte que gracias a las facturas de ORANGE esta persona ha conocido sus datos personales (nombre, apellidos, DNI, domicilio) y ha contratado en su nombre líneas de teléfono e internet de prepago, realizado suscripciones a revistas y anuncios de prostitución.
3. De 05/07/2013, en la que el **denunciante 3** relata que desde agosto de 2012 está siendo acosado, insultado y amenazado por una persona que ha usurpado su identidad y de cuyo número de teléfono tuvo conocimiento al acceder al contrato de telefonía que ***A.A.A..*** tiene suscrito con ORANGE y a las facturas.
4. De 05/07/2013, en la que el **denunciante 4** manifiesta que desde agosto de 2012 está siendo amenazado, insultado y acosado por una señora que, además, ha usurpado su identidad. Afirma que esta señora ha accedido a sus contratos de telefonía con ORANGE para modificar las condiciones y perjudicarle.
5. De fecha 05/07/2013, en la que el **denunciante 5** expone que desde agosto de 2012 está siendo amenazado, acosado e insultado y que su número de teléfono lo obtuvo la autora de estas conductas al acceder a la facturación del contrato que ***A.A.A..*** tiene con ORANGE.

6. De fecha 10/07/2013, en la que el denunciante 6 expone que desde hace unos cuatro meses está siendo sometido a amenazas, acusaciones e insultos por vía telefónica. Que, presuntamente, la responsable es ***B.B.B.,*** que obtuvo información de sus dos números de teléfono al acceder a las facturas telefónicas de ***A.A.A.***., vía que también utilizó para acceder a todos los contactos telefónicos de ***A.A.A..***

En prueba de los hechos que denuncian todos los denunciantes aportan copia del documento denominado "*Correo*", de fecha 26/09/2012, dirigido al Departamento de Atención al Cliente de ORANGE en el que consta como remitente ***A.A.A..,*** figurando también su domicilio y DNI, en el que informa a la operadora de la situación existente y advierte que únicamente cuando se reciba una llamada desde la propia línea contratada podrá modificar las condiciones contratadas.

Además del citado escrito los denunciantes 6 y 2 aportan, respectivamente, los siguientes documentos:

Denunciante 6: Copia de su DNI y de dos denuncias presentadas contra ***B.B.B.*** en la Comisaría de Policía de fechas 17/06/2013 y 25/06/2013.

Denunciante 2: Copia del DNI; copia de un escrito sin fecha dirigido al *Departamento Bajas Orange* informando a la entidad que le remite los documentos para tramitar la baja del número de móvil; y copia de un correo electrónico de fecha 13/06/2013 cuyo asunto es "*trámite baja*".

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 que se recogen en el Informe de Actuaciones Previas que se reproduce:

<< ANTECEDENTES

En fechas comprendidas entre el 5 de julio y 9 de septiembre de 2013 se ha recibido en esta Agencia escritos de los denunciantes, cuya relación se adjunta a este Informe, en los que se pone que se pone de manifiesto los siguientes hechos:

Los denunciantes manifiestan que están recibiendo llamadas amenazadoras de un tercero que ha accedido a los datos personales y de facturación de ***A.A.A.***

A.A.A. *manifiesta, además, que la persona que realiza las llamadas amenazantes ha conseguido modificar la dirección de correo electrónico asociada a su línea (1) recibiendo sus facturas, realizando también otras modificaciones a pesar de tener contraseña para las modificaciones de datos, durante los meses de agosto de 2012 hasta enero de 2013. Asimismo, manifiesta que se están haciendo contrataciones fraudulentas de líneas prepago a su nombre sin exigir ninguna documentación que acredite la identidad. Ha dado de baja la línea en fecha 13 de mayo de 2013 desde la dirección de correo (2)*

A.A.A.. *ha aportado copia de un correo remitido al Departamento de Atención al Cliente en fecha 26 de septiembre de 2012 poniendo de manifiesto estos mismos hechos.*

ACTUACIONES PREVIAS DE INSPECCIÓN

Tal y como consta en el Acta de Inspección E/5302/2013/-I/1 realizada el 14 de mayo de 2014 en ORANGE:

1. *Se ha verificado que en los Sistemas de Información de ORANGE constan los datos de **A.A.A.**como titular de la línea (1) con fecha de activación 3/10/2011 y desactivado con fecha 13/05/2013. Como dirección de correo electrónico figura (3)*

   No constan líneas prepago asociadas a este cliente.

   Asimismo se ha verificado que la línea (1) no ha estado asociada a ningún otro cliente.

2. *Se ha verificado las siguiente modificaciones de datos realizadas al cliente **A.A.A.:***

   Con fecha 22/03/2012 se registra la dirección de correo (3)

   Con fecha 25/09/2012 se registra la contraseña (4) para la modificaciones de datos

   Con fecha 27/09/2012 a las 17:56 se modifica la contraseña quedando registrada (5) y a las 20:01 se vuelve a modificar a otra nueva contraseña quedando registrada (6).

   Con fecha 11/10/2012 se modifica el correo electrónico quedando registrada la dirección de correo (7)

   Con fecha 28/12/2012 se modifica la contraseña volviendo a quedar registrada (5).

   Con fecha 21/01/2013 se modifica la contraseña al valor (8) y la dirección de correo quedando registrado (3) Con fecha 09/02/2013 se modifica la dirección de correo quedando registrado (9) Con fecha 11/03/2013 se modifica la dirección de correo quedando registrado (7)

   Con fecha 09/04/2013 se modifica la dirección de correo quedando registrado (3)

   Con fecha 14/04/2013 se modifica la dirección de correo quedando registrado (7)

   Con fecha 18/04/2013 se modifica la dirección de correo quedando registrado (3).

3. *Se ha comprobado que asociada a la cliente **A.A.A.** constan diversas alertas:*

   Con fecha 25, 27 y 28 de septiembre y 25 de octubre de 2012, figuran registradas alertas para pedir la clave ya que hay un tercero que se hace pasar por la titular.

   Con fecha 21 de enero de 2013, figura registrada una alerta donde el cliente indica que no se modifiquen sus datos de correo electrónico si no se llama desde su número de teléfono y pedir la clave.

   Con fecha 19 de marzo de 2013, figura registrada una alerta indicando que hay un tercero que se hace pasar por la titular y solicita modificar las contraseñas sin conocer la última contraseña asignada.

4. *Se ha verificado que figuran diversas interacciones con la cliente **A.A.A.;***

   Con fecha 25/9/2012 consta "persona accede a datos de cliente. Se pone clave. Pedirla siempre".

   Con fecha 11/10/2012, el cliente solicita una modificación de la dirección de correo electrónico

   Con fecha 15/10/2012 a las 21:24 solicita envío de factura y consta que desconoce la clave. A las 21:31 consta que solicita el envío de la última factura y se realiza el envío.

   Con fecha 15/02/2013 consta que el cliente solicita envío de factura pero se solicita la clave y aporta una clave anterior y la dirección de correo no coincide.

   Con fecha 11/03/2013 consta que el cliente de la dirección de correo (7) solicita el envío de la factura y se le envía. En esa misma fecha y hora consta una modificación de la dirección de correo electrónico realizadas ambas por el mismo operador. A este respecto, ORANGE manifiesta que en la misma llamada se modifica la dirección de correo y se registra la solicitud y el envío de la factura.

   Con fecha 14/04/2013 consta que el cliente llama para el envío de factura y se registra OK.

5. *Respecto del fax aportado en la denuncia, no consta en la entidad dicha reclamación ni la recepción del mismo. A este respecto, ORANGE manifiesta que en el documento aportado por **A.A.A.** no figura el número de fax donde se ha remitido por lo que no se puede conocer si se remitió el fax a un número de la compañía.*

6. *ORANGE manifiesta que:*

   La entidad ha tomado todo tipo de medidas para evitar las modificaciones de datos no solicitadas por el verdadero titular, incluyendo un sistema de alarmas que obliga a que solo la persona que conozca la contraseña definida por el cliente, pueda solicitar modificaciones de datos.

   *En la compañía se ha realizado una inspección, en fecha 17 de enero de 2013, y con referencia E/2889/2013, como consecuencia de una denuncia por los mismos hechos en relación con otro cliente. En la Inspección se verificó que había diversas modificaciones en la dirección de correo electrónico del cliente y el dato que se aportaba en los cambios de dirección de correo era (7) que coincide con la mayor parte de las modificaciones en la dirección de correo electrónico de **A.A.A.** que se han verificado en las comprobaciones realizadas.*

   *En la Resolución de la Agencia de dicho procedimiento E/2889/2013 se especifica que la denunciante manifestó que la persona que suplantaba su identidad ante ORANGE es **B.B.B.***

   *A este respecto, uno de los denunciantes han indicado que la persona que realiza las llamadas amenazantes es **B.B.B.** tal y como ha denunciado ante la Dirección General de la Guardia Civil.>>*

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 establece en su artículo 9, *"Seguridad de los datos":*

"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 artículo 10 de la LOPD, "Deber de secreto", dispone:

"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

La obligación impuesta por el artículo 10 de la LOPD *tiene como finalidad evitar que, por parte de quienes están en contacto con los datos personales almacenados en ficheros, se realicen filtraciones de datos no consentidas por sus titulares.*

El Tribunal Superior de Justicia de Madrid en Sentencia de 19 de julio de 2001 afirma que *"El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)".*

En el mismo sentido se ha pronunciado la Audiencia Nacional, que en Sentencias de 14 de septiembre de 2001 y 29 de septiembre de 2004 ha afirmado que "*Este deber de sigilo resulta esencial en las sociedades actuales cada vez más*

complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la "intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE.

Este precepto contiene un <<*instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos*>> (STC 292/2000*).* Derecho fundamental a la protección de los datos que <<*persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino*>> *(STC 292/2000*), que impida que se produzcan situaciones atentatorias con la dignidad de la persona, <<*es decir, el poder de resguardar su vida privada de una publicidad no querida*>>.

III

En el supuesto que nos ocupa los denunciantes consideran que ORANGE ha permitido que un tercero (al que algunos denunciantes identifican como ***B.B.B.***) acceda a los datos de facturación de uno de los clientes de la operadora (la denunciante 2) y haciéndose pasar por ella cambie su contraseña y modifique sus datos recibiendo de este modo las facturas del servicio telefónico titularidad de la denunciante 2, hecho que le habría permitido obtener información de sus números de teléfono.

Las actuaciones de investigación practicadas por la Agencia en las dependencias de ORANGE han permitido comprobar que entre septiembre de 2012 y abril de 2013 se registraron varias modificaciones de los datos de su cliente (denunciante 2), como son las contraseñas de acceso y la dirección electrónica.

No obstante, se ha comprobado también que la operadora habilitó un procedimiento de autenticación especial; no solo porque activó una contraseña para el acceso a los datos de la cuenta de su cliente (denunciante 2) sino también porque registró hasta cinco alertas relacionadas con la protección de los datos de este cliente.

Debe traerse a colación el artículo 93 del Reglamento de desarrollo de la LOPD, aprobado por el R.D. 1720/2007 (RLOPD), conforme al cual "*El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios".* Y añade que "*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".*

El resultado de las investigaciones practicadas durante la Inspección confirman que ORANGE adoptó las medidas necesarias para garantizar la seguridad de los datos de su cliente (denunciante 2) y se atuvo a las obligaciones que le impone el artículo 93 del RLOPD.

En este orden de ideas debe tenerse en cuenta que en el ámbito administrativo sancionador son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, teniendo plena virtualidad el principio de presunción de inocencia, que debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetado en la imposición de cualesquiera sanciones. Esto, porque el ejercicio del *ius puniendi,* en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

En tal sentido el Tribunal Constitucional, en Sentencia 76/1990, considera que el derecho a la presunción de inocencia comporta "*que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio".*

De acuerdo con este planteamiento el artículo 137 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC), establece que *"1. Los procedimientos sancionadores respetarán la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario."*

Como ha precisado el Tribunal Supremo en STS de 26 de octubre de 1998 la vigencia del principio de presunción de inocencia *"no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo."*

Por su parte el Tribunal Constitucional en STC 24/1997 ha manifestado que *"los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que:*

a) La prueba indiciaria ha de partir de hechos plenamente probados.

b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras)."

En definitiva, el principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo que acredite los hechos que motivan la imputación o la intervención en los mismos del presunto infractor de manera que, en lo que concierne a la presunta infracción del deber de secreto del artículo 9 de la LOPD, dada la ausencia de evidencias o indicios razonables de su comisión por ORANGE procede acordar el archivo de las actuaciones de investigación practicadas.

En relación a la presunta infracción del deber de secreto que el artículo 10 de la LOPD impone al responsable del fichero, vulneración que los denunciantes atribuyen a ORANGE por haber permitido que un tercero accediera a los datos asociados a uno de sus clientes (la denunciante 2), tampoco obran en el expediente pruebas de que esta revelación hubiera llegado a producirse ni de la responsabilidad de la operadora denunciada en tales hechos

IV

A la vista de lo expuesto en los párrafos precedentes y habida cuenta de la falta de pruebas de las que se infiera la comisión de una infracción de los artículos 9 y /o 10 de la LOPD ni de la responsabilidad que en ellos pudiera haber tenido ORANGE, procede acordar el archivo de las presentes actuaciones.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. PROCEDER AL ARCHIVO de las presentes actuaciones.

2. NOTIFICAR la presente Resolución y el Anexo I a **ORANGE ESPAGNE S.A.U., y la presente resolución** así como **el Anexo** que a cada uno corresponda a los **denunciantes 1, 2, 3, 4, 5, y 6.**

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 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