Expediente Nº: E/00279/2015

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 la denuncia presentada por D. ***A.A.A.*** y en consideración a los siguientes

HECHOS

PRIMERO: Con fecha 12/09/2014, tuvo entrada en esta Agencia un escrito de D. ***A.A.A.*** (en lo sucesivo, el denunciante) en el que manifiesta que existen brechas de seguridad en los ficheros de la operadora **ORANGE ESPAGNE, S.A.U**. (en lo sucesivo, ORANGE o la denunciada) y relata que en la actualidad es titular de una línea con esa compañía (número ******TEL.1***), que al acceder a la página web de la operadora para comprobar su factura, utilizando para ello su usuario y contraseña, el sistema le dio acceso como cliente del número ******TEL.2*** que está asociado a un tercero (***B.B.B.***), permitiéndole conocer los datos del tercero –nombre y apellidos, NIF, domicilio, cuenta bancaria y el número de otra línea telefónica de la que es titular - y ofreciéndole la posibilidad de modificarlos.

Acompaña a la denuncia una impresión de pantalla correspondiente al *"área de clientes", "mi factura*", de la página web de ORANGE, que contiene una relación de once facturas en formato PDF cuyas fechas de emisión están comprendidas entre el 01/10/2013 y el 01/08/2014; la copia de una factura de ORANGE a nombre de ***B.B.B.***., en la que consta su dirección postal, número de NIF, datos identificativos de la cuenta bancaria en la Caja de Ahorros de Vigo, Orense y Pontevedra parcialmente anonimizados y la relación de llamadas realizadas desde los números ******TEL.2*** y ******TEL.3.***

SEGUNDO: Tras la recepción de la denuncia, la Subdirección General de Inspección de Datos realizó actuaciones encaminadas al esclarecimiento de los hechos teniendo conocimiento de los siguientes extremos que constan en el Informe de Actuaciones Previas de Inspección que se reproduce

<<ANTECEDENTES

Con fecha de 12 de septiembre de 2014 tiene entrada en esta Agencia un escrito de ***A.A.A.*** *en el que declara lo siguiente:*

En la actualidad mantengo contratada la línea ******TEL.1*** *con Orange tras haber dado de baja otras tres por diversos motivos.*

Que al hacer uso del acceso para clientes en la correspondiente página web del

*operador utilizando para ello su usuario *****TEL.1** y clave *****CLAVE.1**, el sistema le da acceso como cliente del número *****TEL.2** a nombre de un tal **B.B.B.** permitiéndole visualizar datos de la referencia línea así como de la línea *****TEL.3** con la posibilidad de conocer y cambiar datos personales y servicios asociados: tipo de contratos, cuentas bancarias números, visualizar información como fecha y duración de todas sus llamadas histórico de facturación ...etc.*

Que ha intentado remitir correo a la dirección que de la empresa figura en la factura, envíos que no han sido posibles ya que sistemáticamente rechaza cualquier comunicado a esta dirección remitiendo a un apartado de correo que hace imposible la entrega fehaciente de cualquier comunicado, lo cual contraviene la obligación de identificación por parte de mencionada compañía generando indefensión en las reclamaciones.

Junto a la denuncia aporta la siguiente documentación:

- *Copia del DNI ***DNI.1 de A.A.A.*
- *Copias de pantallas relativas a la aplicación de clientes de ORANGE en las que se aprecia el número de teléfono ***TEL.2, un listado de 12 facturas en formato PDF comprendidas entre el 1/10/2013 y el 1/8/2014 y el contenido de la correspondiente a 1/8/2014 en la que se aprecia que dicha factura se emite a nombre de B.B.B. con NIF: ***NIF.1 y domicilio en la calle (C/.....1) (Madrid). La factura incluye el detalle de llamadas efectuadas desde los números ***TEL.3, ***TEL.2.*

ACTUACIONES PREVIAS

1. *En fecha de 8/5/2015 se realiza una inspección a la entidad **ORANGE ESPAGNE SAU** en la que se averigua lo siguiente:*
   - *1.1. Los inspectores solicitan y obtienen acceso a los sistemas informáticos de ORANGE al objeto de realizar las siguientes comprobaciones:*
   - *1.2. Durante la inspección se accede a la aplicación que gestiona los cuentas y productos contratados por los clientes realizándose las siguientes búsquedas:*
     - *1.2.1. Por el DNI por el número *****DNI.1** obteniéndose que corresponde al cliente de nombre **A.A.A.** que es titular de dos contratos:*
       - *1.2.1.1. Un contrato antiguo con dos líneas asociadas que fueron dadas de baja el 2/8/2005 por impago.*
       - *1.2.1.2. Un contrato con cuatro servicios:*
         - *1.2.1.2.1. Línea *****TEL.4** con fecha de alta 7/4/14 y fecha de baja 22/8/2014*
         - *1.2.1.2.2. Línea *****TEL.5** con fecha de alta 7/7/14 y fecha de baja 22/8/2014*
         - *1.2.1.2.3. Servicio GPRS sin voz.*
         - *1.2.1.2.4. Línea *****TEL.6** con fecha de alta 8/7/14 y activa al día de la fecha.*
     - *1.2.2. Por el número *****TEL.2** obteniéndose que corresponde al cliente de nombre **B.B.B.** con DNI *****NIF.1** titular de dicho número dado de alta en*

ORANGE el 25/7/2012 y en activo al día de la fecha. Los representantes de ORANGE manifiestan que a la vista del resultado de la consulta dicho número ha estado siempre asociado a ***B.B.B.*** *en ORANGE.*

1.3. Se accede también a la aplicación de contactos con los clientes y se realiza una consulta por el DNI ******DNI.1*** *verificándose que* ***A.A.A.*** *no ha realizado ninguna reclamación en ORANGE relacionada con los hechos denunciados en la Agencia.*

1.4. Se accede a la aplicación web y se realizan las siguientes consultas:

1.4.1. Se accede por el número ******TEL.6*** *y clave* ******CLAVE.1*** *obteniéndose acceso a la los datos personales de* ***A.A.A..***

1.4.2. Se accede por el número ******TEL.2*** *y clave* ******CLAVE.1*** *obteniéndose un mensaje: "teléfono o contraseña son erróneos, por favor introdúcelo de número".*

1.5. Los inspectores muestran a los representantes de ORANGE copia de las pantallas aportadas por ***A.A.A.*** *en su acceso a la aplicación web para clientes de ORANGE y donde figuran datos relativos a* ***B.B.B. .***

1.6. Ante la información anterior, los representantes de ORANGE manifiestan que necesitarían tiempo para poder analizar a través de los ficheros log del sistema al objeto de investigar posibles incidencias que arrojaran luz sobre los hechos denunciados. Dado que el mencionado log correspondiente a agosto de 2014 se encuentran en copias de seguridad que es necesario recuperar, los inspectores requieren a los representantes de ORANGE para que el plazo de quince días remitan a la Agencia el resultado de dicha investigación.

1.7. En fecha de 27/5/2015 se recibe escrito de ORANGE SPAGNE, S.A.U. en el que manifiestan que una vez analizado el log de conexión al Área de Clientes se observa que las dos líneas presentan accesos comunes los días 15/7/2014 sobre las 7 horas, el día 8/8/2014 sobre las 9 horas y el día 11/8/2014 entorno a las 11:20, presentando también accesos diferentes los días 18, 19, 22, 25, 29 de julio, 8, 11 y 13 de agosto, 6, 18, 20 y 25 de septiembre para el número ******TEL.1*** *y 3, 4, 5, 8, 10, 11, 18, 20, 24 y 26 de septiembre para el número* ******TEL.2****.*

2. A la vista de la información recabada en ORANGE no se observa que los números ******TEL.1*** *y* ******TEL.2*** *guarden ninguna vinculación aparente, ya que no presentan en su histórico ningún titular común. A la luz del análisis de la información contenida en el registro de accesos no se desprende que se hayan vinculado ambas líneas de forma que el acceso a una lleve al acceso a la otra ya que el log de accesos refleja, en general, accesos distintos a una y a otra. No obstante, y respecto a los tres accesos coincidentes en el tiempo en ambos números los días 15/7/2014, 8/8/2014 y 11/8/2014, no hay evidencias que señalen que se haya producido una vinculación temporal de ambos números ya sea como consecuencia de un posible error en las base de datos o si se trata de tres accesos coincidentes en el tiempo, ya sea de forma premeditada por sus usuarios o no.>>*

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, 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." (El subrayado es de la AEPD)

Este precepto deben 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".*

La infracción de la obligación que el artículo 9 de la LOPD impone a los responsables de los ficheros y/o encargados de tratamiento se tipifica como infracción grave en el artículo 44.3.h) en los siguientes términos: "*Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

El Tribunal Constitucional ha resaltado la importancia de las medidas de seguridad 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.

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

"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".

El desarrollo reglamentario de la LOPD se llevó a cabo a través del 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 con arreglo a lo dispuesto en el Título VIII, con independencia de cuál sea su sistema de tratamiento. El RLOPD clasifica las medidas de seguridad que deben implantar los responsables de los ficheros y los encargados de los tratamientos en tres niveles: básico, medio y alto. Prevé que las medidas de seguridad de nivel básico se adopten en "*todos*" los ficheros o tratamientos de datos de carácter personal.

Entre las medidas de nivel básico el artículo 93 del RLOPD menciona la *"Identificación y autenticación"* y 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 personalizadas 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. (…)".

III

Las actuaciones de investigación que la AEPD llevó a cabo en la sede de ORANGE en fecha 08/05/2015 con la finalidad de constatar los hechos que se denuncian y comprobar si la operadora había incurrido en una infracción del deber de adoptar las medidas que garantizasen la seguridad de los datos personales tratados no permitieron obtener pruebas ni indicios razonables que confirmaran la realidad de lo manifestado en el escrito de denuncia.

Al acceder a los registros informáticos de la operadora los inspectores verificaron que, en esa fecha, existía una línea de teléfono (******TEL.1***) activa asociada al nombre, apellidos y NIF del denunciante. Que esa línea había pertenecido al denunciante desde la fecha de alta, el 25/07/2012. Y también que él había sido titular de otras dos líneas que se dieron de baja el 22/08/214.

Asimismo, desde la aplicación web de la operadora se comprobó que al acceder

por el número ***TEL.1 –del que es titular el denunciante - y por su clave (***CLAVE.1*) se visualizaban únicamente los datos del denunciante. Del mismo modo se constató que si se accedía con el número ***TEL.2* y la clave del denunciante el sistema informaba de que el teléfono o la contraseña eran erróneos.

Se comprobó también que al realizar una consulta en la aplicación de productos contratados y clientes utilizando el número ***TEL.2* éste se encontraba asociado a ***B.B.B.***. y a su NIF desde el 25/07/2012.

A mayor abundamiento, la consulta hecha por los Inspectores de la AEPD a la aplicación de "*contactos con los clientes*" utilizando el NIF del denunciante reveló que no constaba en ORANGE ninguna reclamación del denunciante relacionada con los hechos sobre los que versa su denuncia.

Por otra parte, es digno de destacar que la información ofrecida por ORANGE a la Inspección de la AEPD relativa a los log de conexión al área de clientes de su página web –a la vista de las impresiones de pantalla que el denunciante nos ha remitido- tampoco ha permitido verificar que el acceso a la citada página web se efectuara como el denunciante describe en su denuncia. Si bien ORANGE ha informado que los días 08/08/2014 y 08/011/2014 los MSISDN ***TEL.2* y ***TEL.1* se conectaron a su página web casi simultáneamente (el día 08/08 el primero a las 8:57:08 horas y el segundo a las 09:01:18 horas y el día 11/08 a las 11:18:23 horas y a las 11:23:17 horas, respectivamente) esta circunstancia carece de virtualidad a los efectos de poder derivar de ella un indicio de prueba de los hechos objeto de la denuncia..

En definitiva, las actuaciones de investigación previa no han permitido confirmar que si se accede a la página web de ORANGE en las mismas condiciones en las que el denunciante declaró haberlo hecho (introduciendo su número de teléfono y su clave) se produzca la anomalía que denuncia, esto es, que se visualicen los datos personales del tercero ***B.B.B..***

Debe subrayarse, además, que la documentación que el denunciante ha remitido a la AEPD con su escrito, entre la que destaca la copia de una factura emitida por ORANGE a nombre de ***B.B.B.*.** –número de factura ***FACTURA.1 de fecha 01/08/2014- en la que constan varios datos personales del tercero y la impresión de pantalla obtenida de www.orange.es con una relación de las últimas doce factura, no ofrece prueba alguna ni indicio del que pudiera inferirse que la visualización de los datos de ***B.B.B..*** a través de la página web de ORANGE fue el resultado de haber accedido a la página web con su número de teléfono y su clave (***CLAVE.1*).

Resulta por tanto que el único elemento en el que se sustenta la presunta vulneración por ORANGE de las medidas que garantizan la seguridad de los datos personales objeto de tratamiento es su declaración, insuficiente por sí sola para enervar el principio de presunción de inocencia.

Esto, porque como se ha explicado, ni las investigaciones de la AEPD han demostrado que al acceder a la página web de la entidad del modo en que el denunciante afirma haberlo hecho se produjera una "*brecha de seguridad*", ni la documentación facilitada por el denunciante ha ofrecido indicios razonables de que los hechos acontecieron tal y como los describe, pues no hay vinculación entre la

información que sobre el tercero, ***B.B.B..,*** nos ofrece y el cauce a través del cual dice haber accedido a estos datos.

Llegados a este punto 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 de la potestad sancionadora del Estado, en sus diversas manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

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 26/10/1998 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)."

De las reflexiones precedentes se concluye que 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.

Trasladando las anteriores consideraciones a los hechos que nos ocupan se concluye que, a la luz del principio de presunción de inocencia, no concurren razones que justifiquen la incoación de un expediente sancionador. **En consecuencia, procede acordar el archivo de las actuaciones de investigación previa practicadas.**

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 **ORANGE ESPAGNE, S.A.U.** y a D. ***A.A.A.***.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción introducida 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 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