



Expediente N°: E/02688/2013

### **RESOLUCIÓN DE ARCHIVO DE ACTUACIONES**

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **CABLEUROPA, S.A.U.(ONO)** en virtud de denuncia presentada ante la misma por D. **A.A.A.** y en base a los siguientes

#### **HECHOS**

**PRIMERO:** Con fecha 6 de mayo de 2013 se dictó Resolución por el Director de la Agencia Española de Protección de Datos acordando estimar el recurso de reposición de referencia RR/00238/2013 interpuesto por D. **A.A.A.** (en adelante en denunciante) en base a los siguientes hechos:

En fecha 30 de julio de 2012, tras una llamada telefónica a la compañía CABLEUROPA, S.A.U.. (en adelante ONO), esta entidad ha modificado la encriptación de la red WIFI del denunciante, el cual manifiesta que la persona que realiza la llamada ha utilizado sus datos personales, entre ellos, el número de DNI para identificarse ante ONO sin su consentimiento. En esa misma fecha, el denunciante contacta nuevamente con la compañía la cual vuelve a reencriptar la red WIFI esta vez a solicitud del titular.

Por este motivo, el denunciante solicita a ONO grabación de la primera llamada y la compañía se ha negado a proporcionársela.

Adjunto a la denuncia se ha aportado, entre otros, los siguientes documentos:

Fotocopia de un fax de fecha 30/07/2012 remitido por el denunciante a ONO solicitando la grabación de la primera llamada.

Fotocopia de un fax de fecha 01/09/2012 remitido por el denunciante a ONO solicitando la grabación de la primera llamada y aportando el número de teléfono desde el cual se realizó la llamada ( **C.C.C.**).

Escrito de contestación de ONO, de fecha 5/09/2012 remitido al denunciante donde la informan que *"su conversación no fue grabada en aquel momento ya que las grabaciones se realizan de forma aleatoria...Por este motivo no resulta posible acceder a lo solicitado"*.

Listado de llamadas, donde constan las llamadas de fecha 30/07/2012.

**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:

Tal y como consta en el Acta de Inspección E/2688/2013-/I/1 realizada en fecha 9 de julio de 2013:

1. Para instalar en los domicilios de los clientes (cliente residencial), ONO utiliza dos tipos de aparatos que proporciona acceso a Internet (Modem),:

- 1.1. CABLEMODEM ENCRIPTADO DE FÁBRICA (CB), el cual necesita contraseña y ésta viene en una pegatina de fábrica en el propio aparato. Esta contraseña puede ser modificada por el cliente.

El aparato, además, tiene un botón denominado RESET que, al pulsarlo, restablece los valores de fábrica, es decir restablece la contraseña que había por defecto y que está en la pegatina debajo del CB.

Cualquier persona con acceso físico al aparato puede modificar la contraseña utilizando el botón RESET e introduciendo una nueva.

- 1.2. CABLEMODEM NO ENCRIPTADO. Por defecto no tiene contraseña pero puede encriptarse utilizando el manual del fabricante o con la ayuda de scripts de encriptación que se encuentran publicados en [www.ono.es](http://www.ono.es). Para realizar la encriptación es necesario que un PC esté conectado por cable al modem. También este aparato tiene la tecla RESET que permite desencriptarlo y volver a la situación de origen, sin contraseña,

En ambos casos, ONO no cambia nunca la contraseña simplemente ayuda explicando el modo de poder realizar el cambio. También en el manual del aparato se explica los pasos a seguir para modificar una contraseña.

2. El procedimiento de identificación de un cliente que solicita el cambio de contraseña comienza por la recepción de la llamada del cliente por una máquina "IVR" que permite redirigir llamadas. Dicha máquina identifica el número de teléfono desde el que el cliente llama:

- 2.1. En caso de que el número de teléfono coincida con el registrado en la "ficha" del cliente y el cliente no tiene además otros domicilios, al agente que atiende la llamada se le abre una pantalla que dice "CLIENTE IDENTIFICADO" y se le muestra automáticamente la ficha del cliente al operador. Si el cliente tiene más de una ficha a su nombre y con el mismo DNI se solicita la dirección como dato adicional de comprobación.

- 2.2. Si el cliente llama desde un número desconocido, distinto al asignado a su domicilio, la IVR le solicita su DNI y el cliente debe marcarlo. Después al operador que atiende la llamada se le abre una pantalla que dice "CLIENTE AUTENTICADO" y la ficha del cliente.

- 2.3. Sí la máquina IVR no llega a identificar al cliente, el operador tendrá que solicitarle su DNI y cualquier otro dato que le identifique.

A este respecto se ha acreditado que, en los Sistemas de ONO se encuentran los datos del denunciante como titular de la línea **C.C.C.**. Este número de línea telefónica ha sido aportado por el denunciante como línea telefónica desde la que se realizó la llamada para la modificación de la contraseña del módem ubicado en su domicilio. Asimismo se ha verificado que consta como modem "CABLEMODEM WIFI EPR..." el cual, según ONO corresponde con el tipo de modem CABLEMODEM ENCRIPADO DE FÁBRICA (CB).

3. Respecto de las grabaciones de las llamadas telefónicas recibidas en el Servicio de Atención al Cliente, ONO manifiesta que son grabaciones de control de calidad, por ello se graban un número determinado de llamadas de forma aleatoria y se destruyen como máximo a los tres meses
4. En el Sistema de Información de ONO donde se registran los contactos mantenidos con los clientes, se ha verificado:

- 4.1. la existencia de dos contactos en fecha 30/07/2012, uno de ellos a las 17:35 y el otro a las 21:26 en relación con la modificación de la contraseña del wifi del cliente. En el primero de ellos consta la siguiente anotación: "*se encripta router*". En el segundo figura "*Se encripta a petición del titular*".

A este respecto, ONO manifiesta que aunque los operadores del Servicio de Atención al cliente registran como anotación "*se encripta router*" y "*se encripta a petición del titular*", lo que realmente se facilita es información al cliente sobre el procedimiento de modificación de la contraseña del router. Desde ONO no se puede modificar la contraseña del router ya que hay que realizarla directamente en el aparato.

- 4.2. Con fecha 31/07/2012, figura registrada la recepción de un fax en el que el cliente solicita la grabación de la llamada realizada el 30/07/2012 a las 17:35 y se le indica el procedimiento para solicitarla.
- 4.3. Con fecha 16/08/2012, figura registrada una petición del cliente solicitando la grabación de la llamada realizada el 30/07/2012 y figura la siguiente anotación "*No cumple los requisitos por no conocer el número de telef. desde donde se realizó la llamada*"
- 4.4. Con fecha 27/08/2012, figura registrada una petición del cliente solicitando la grabación de la llamada realizada el 30/07/2012 y donde se indica que la llamada se realizó desde el número **C.C.C.**.
- 4.5. Con fecha 01/09/2012, figura registrada la entrada de un fax una petición del cliente solicitando la grabación de la llamada realizada el 30/07/2012 y donde se indica que la llamada se realizó desde el número **C.C.C.**. Asimismo consta, con fecha 07/09/2012 una anotación donde se indica que no se ha podido localizar telefónicamente al cliente y que se informará por carta.

A este respecto, ONO ha aportado copia del escrito de fecha 5 de septiembre de 2012 donde se informa que la conversación no ha sido grabada. Este escrito coincide con el aportado por el denunciante.

- 4.6. Con fecha 12/12/2012 figura registrada la entrada de un escrito de la OMIC de la Comunidad de Madrid donde el cliente solicita la grabación de la llamada. Así mismo consta, en la contestación, que la reclamación ya se había realizado y contestado al cliente y que las llamadas *“se efectúan para la mejora de nuestro servicio y que se eliminan en un plazo no superior a tres meses cuando se cumple la finalidad de la grabación”*.

A este respecto, ONO ha aportado copia del escrito de contestación remitido a la OMIC de fecha 2 de enero de 2013.

- 4.7. Con fecha 11/06/2013 figura registrada una entrada de escrito de la SETSI donde el cliente solicita la grabación de la llamada.

A este respecto, ONO manifiesta que todavía no se ha emitido contestación a ese Organismo, no obstante, manifiesta que la contestación será similar a la aportada a la OMIC.

## **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**

El artículo 6.1 y 2 de la LOD dispone que:

*“1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”.*

*“2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado”.*

El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, Fundamento Jurídico 7

primer párrafo, “(...) consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)”.

El artículo 6 de la LOPD consagra el principio del consentimiento o autodeterminación, piedra angular en la construcción del derecho fundamental a la protección de datos que alude a la necesidad de contar con el consentimiento del afectado para que puedan tratarse sus datos personales. Conforme al citado precepto el tratamiento de datos sin consentimiento de su titular o sin otra habilitación amparada en la Ley constituye una vulneración de este derecho, pues sólo el consentimiento, con las excepciones contempladas en la ley, legitima el tratamiento de los datos personales.

Por tanto, el tratamiento de datos de carácter personal tiene que contar con el consentimiento del afectado o, en su defecto, debe acreditarse que los datos provienen de fuentes accesibles al público, que existe una Ley que ampara ese tratamiento o una relación contractual o negocial entre el titular de los datos y el responsable del tratamiento que sea necesaria para el mantenimiento del contrato.

### III

En el supuesto que nos ocupa, el denunciante pone de manifiesto que CABLEEUROPA S.A. ha realizado un tratamiento de sus datos sin su consentimiento, puesto que realiza un acceso no autorizado a su red wifi en el que cambia su usuario y contraseña sin su consentimiento

No obstante, de la inspección practicada por esta Agencia en las dependencias de la entidad denunciada, se pudo comprobar que la contraseña de los clientes no puede cambiarla la entidad denunciada, sino que únicamente se puede modificar desde el domicilio de los mismos, a través de una llamada en la que se le informa de cómo hacerlo pero sin proceder a modificarla, únicamente se le da la información. Si dicha llamada se realiza desde la línea contratada con ONO, como ocurre en el presente caso, la entidad lo identifica a través de un ordenador y se le da dicha información.

En el presente caso, se puede acreditar que se produjo una llamada desde el domicilio del denunciante, tal y como consta en el sistema de información de ONO, sistema donde se registran los contactos mantenidos con los clientes. A través de esta

llamada la entidad denunciada aporta información sobre el procedimiento de modificación de la contraseña del router, sin que, tal y como afirma el denunciante, pudiera modificar tal contraseña en la medida en que tal cambio ha de realizarse directamente desde el aparato.

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, resultando clara la plena virtualidad de los principios de presunción de inocencia. La presunción de inocencia debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, pues 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 130.1 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 *“Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aún a título de simple inobservancia.”*

Conforme señala el Tribunal Supremo (STS 26/10/98) el derecho a la 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.”*

La Sentencia del Tribunal Constitucional de 20/02/1989 indica que *“Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando,*

*concorre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate.”*

En definitiva, aquellos principios impiden imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo acreditativa de los hechos que motivan dicha imputación o la intervención en los mismos del presunto infractor, aplicando el principio “*in dubio pro reo*” en caso de duda respecto de un hecho concreto y determinante, y que obliga en todo caso a resolver dicha duda del modo más favorable al interesado.

Por ello, dada la ausencia de elementos de cargo que permitan imputar a **CABLEUROPA, S.A.U.** la presunta infracción de lo previsto en el artículo 6 de la LOPD procede acordar el archivo de las actuaciones practicadas.

#### IV

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 a **CABLEUROPA, 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 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.

