

Expediente N°: E/06757/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la(s) entidad(es) **ORANGE ESPAGNE S.A.U.** en virtud de denuncia presentada por Don **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 30 de agosto de 2013 tiene entrada en esta Agencia un escrito de **A.A.A.** en el que declara que el 19 de agosto de 2013 ha recibido una llamada de **Vodafone (ORANGE)** para consultar si ha recibido los móviles que ha solicitado en un domicilio de Murcia.

Al preguntar al operador le comunican que el 3 de agosto se ha cambiado su domicilio a uno en Murcia, el 5 de agosto se solicita un cambio de tarifa y un móvil nuevo, el 7 de agosto se solicita otro cambio de tarifa y otro móvil.

El afectado indica que es un fraude y que no ha solicitado nada. Abre una incidencia en la entidad y le comunican que la solicitud del día 5 se canceló por no tener la conformidad del cliente y la del día 7 ha sido devuelta por domicilio desconocido.

El día 21 de agosto recibe un mensaje de Orange indicando que la portabilidad será efectiva al día siguiente.

Se pone en contacto con la entidad y solicita la anulación de la portabilidad posteriormente desde Orange le confirman que se ha anulado tanto la portabilidad como la entrega de un terminal.

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:

Sobre el sistema de información de **ORANGE** se han realizado las siguientes verificaciones:

1.1. Se realiza una consulta sobre el fichero de clientes en relación a los datos asociados al DNI *****DNI.1** L obteniéndose información relativa a **A.A.A.**. El domicilio que figura en el sistema es **(C/.....1) Lleida.**

1.2. Se accede a las reclamaciones presentadas por este cliente, verificándose que en fecha 01/10/2013 se recibe un correo electrónico de la OMIC de Barcelona en la que solicita información sobre un alta fraudulenta.

En las actuaciones realizadas por la entidad se verifica que no se ha realizado el alta de ninguna línea a nombre del reclamante.

Se responde a la OMIC en fecha 31/10/2013.

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 de la LOPD, determina:

“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 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.

El tratamiento de datos sin consentimiento 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, (F.J. 7 primer párrafo) señala que:

“...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. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y, el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que rectifique o los cancele”.

Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y tratamiento de sus datos personales y a saber de los mismos.

III

En el presente caso, se procede a examinar la reclamación de fecha de entrada en esta AEPD—**30/08/13**—en dónde el epigrafiado pone de manifiesto los siguientes “hechos” en orden a su adecuación a la LOPD:

“Suplantando mi identidad han modificado mi domicilio en el contrato el día 03/08/13 y después han solicitado un terminal móvil nuevo de alta gama para entregar en Murcia (...)”—folio nº 1--.

Los hechos descritos pueden suponer una presunta vulneración del contenido del art. 6.1 LOPD anteriormente citado.

En fecha 28/05/13 se personan en la Entidad denunciada—**Orange**—Inspectores de esta AEPD debidamente autorizados por el Director de la Agencia, quedando plasmada su actuación investigadora en el acta de inspección **EI/06757/2013**.

*“En las actuaciones realizadas por la Entidad se verifica que **no se ha realizado el alta de ninguna línea** a nombre del reclamante”.*

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 su Sentencia 76/1990, de 26/04, 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.

La presunción de inocencia rige sin excepciones en el Ordenamiento sancionador y ha de ser respetada en la imposición de cualquier sanción, ya sea penal o **administrativa** (TCo 13/1981), pues el ejercicio del derecho sancionador en cualquiera de sus manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

Conforme a este principio, no puede imponerse sanción alguna en razón de la culpabilidad del imputado si no existe una **actividad probatoria de cargo**, que en la apreciación de las autoridades u órganos llamados a resolver, destruya esta presunción (TCo Auto 3-12-81).

La Audiencia Nacional—SAN 06/07/12—ha manifestado que: *“Si bien la presunta suplantación de identidad no ha podido ser esclarecida, de lo que no cabe duda a juicio de la Sala, es de que Canal Satélite Digital obró con una diligencia normalmente exigible en una operación de servicios como los contratados. Y además el correspondiente contrato tuvo que ser firmado por alguien que, si no era tal denunciante, al menos si conocía su nombre y apellidos, su domicilio, su teléfono móvil y su número de DNI. Abonándose además, puntualmente y durante ocho meses, tales consumos televisivos.”*

De acuerdo con lo argumentado, cabe concluir que nos encontramos ante un presunto **fraude** realizado por un tercero de mala fe que utiliza los datos del afectado con la finalidad de obtener terminales de teléfono de manera ilegal, sin que se haya producido la contratación de servicio/s alguno con los datos de carácter personal del afectado; por lo que no se ha producido tratamiento alguno de sus datos sin su consentimiento.

En este caso, la Entidad denunciada—**Orange**—ha desplegado la diligencia mínima exigible en estos casos al no disponer del consentimiento del titular de la línea, siendo víctima al igual que el afectado de un presunto fraude de un tercero de mala fe que excluye el elemento subjetivo de la culpabilidad necesario para la imposición de una sanción administrativa.

La reciente Sentencia de 24 de enero de 2014 -recurso nº. 540/2012 -, en un supuesto similar al que nos ocupa, y en que igualmente la parte recurrente era la misma: << ... ningún reproche puede hacerse a la actuación de France Telecom en este ámbito sancionador al haber adoptado las cautelas precisas para asegurarse de la identidad de la persona de quien recababa los datos personales en relación con la contratación de las citadas líneas telefónicas, sin que existan elementos suficientes en el presente procedimiento para poder determinar si se trata de un supuesto en que un mismo número de DNI ha podido ser asignado erróneamente a dos personas distintas, o de un posible supuesto de **fraude**.

En cualquiera de los casos, bien por falta de tipicidad o de culpabilidad, no puede tenerse por acreditada o imputarse a France Telecom la vulneración del principio del consentimiento ni tampoco, y en correlación, la del principio de calidad de datos>>.

La actuación anteriormente descrita está incardinada en el tipo penal regulado en el art. 248 y ss CP—**delito de estafa**—careciendo esta AEPD de competencia material al respecto, siendo el Juez de Instrucción del lugar de comisión del hecho delictivo el

que tiene competencia para entrar a conocer del fondo del asunto.

Por todo lo expuesto se ordena el **ARCHIVO** del presente procedimiento frente a la Entidad denunciada.

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 la Entidad **ORANGE ESPAGNE S.A.U.** y a Don **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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos