

Expediente Nº: E/03485/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fecha 20 de marzo de 2014, tuvo entrada en esta Agencia escrito de denuncia de Dña. **A.A.A.** (en lo sucesivo la denunciante) en el que manifestaba que ORANGE ESPAGNE S.A.U. (en lo sucesivo ORANGE) había incluido sus datos personales en ficheros de información de solvencia patrimonial y crédito, cuando ella no había contratado con esta entidad.

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:

Con fecha 25 de junio de 2014, se solicitó a EQUIFAX IBERICA, SL información relativa a la denunciante y de la respuesta recibida con fecha 30 de julio de 2014, se desprende lo siguiente:

1. Respecto del fichero ASNEF:

Consta un registro asociado a la denunciante, por un importe de 169,75€, con fecha de alta 10 de septiembre de 2010, informado por la entidad ORANGE

2. Respecto del fichero de NOTIFICACIONES:

Consta una notificación asociada a la inclusión de los datos de la denunciante en el fichero ASNEF por la citada deuda, con fecha 10 de septiembre de 2010, por la entidad ORANGE., el domicilio de notificación es (C/.....1) (**HUELVA**)

3. Respecto del fichero de BAJAS:

No consta información asociada a ORANGE.

4. Respecto al expediente asociado al denunciante:

Consta un expediente de solicitud de acceso de fecha 24 de enero de 2012 y la contestación al mismo de fecha 27 de enero de 2012.

Así mismo, consta otro expediente de solicitud de acceso de fecha 6 de febrero de 2014 y la contestación de fecha 19 de febrero de 2014.

Con fecha 31 de julio de 2014, ORANGE ha remitido a esta Agencia la siguiente

información en relación con los hechos denunciados:

1. Aportan copia impresa de los datos que constan en sus ficheros relativos a la denunciante, donde figuran su nombre y apellidos, D.N.I. y domicilio en la (C/.....1) (**Huelva**).
2. Dichos datos constan como titular de un contrato post-pago, en el que figuran las líneas:
 - a. *****TEL.1**, dada de alta por portabilidad con fecha 20 de mayo de 2010 y en baja por impago con fecha 25 de noviembre de 2010.
 - b. *****TEL.2**, dada de alta por portabilidad con fecha 20 de mayo de 2010 y de baja por impago con fecha 25 de noviembre de 2010.
3. Aportan copia de las facturas emitidas por importes de 2,47€, 166,68€ y 423,60€, que fue rectificadas mediante factura de 25 de noviembre de 2011 quedando un importe de 0,60€, todas las facturas resultaron impagadas.
4. No les consta ninguna comunicación ni contacto con la cliente, excepto la solicitud de acceso de fecha 20 de febrero de 2012 y la contestación a la misma de fecha 15 de marzo de 2012, cuya copia adjuntan.
5. Aportan copia de los contratos correspondientes a las dos líneas, en los que figuran la firma del cliente, así como del D.N.I. recabado en la contratación, en el que consta el nombre y apellidos de la denunciante y el mismo número, sin embargo el nombre de los padres y la fecha y lugar de nacimiento son diferentes del que aportó la denunciante en su denuncia, así como el nombre de los padres, la fotografía y la fecha de expedición.
6. La contratación se realizó en un Punto de Venta del canal de distribución de la compañía: ONUFONE S.L. con domicilio en *****LOCALIDAD.1 (Huelva)**.
7. Los datos de la denunciante fueron incluidos en ficheros de solvencia y no se ha solicitado su exclusión al resultar la deuda cierta y exigible, además no constan en sus sistemas reclamaciones de la denunciante.

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, el tratamiento de datos realizado por la entidad denunciada fue llevado a cabo empleando una diligencia razonable. En este sentido ha de tenerse que cuenta que ORANGE ha presentado durante la fase de actuaciones previas de inspección copia de los contratos suscritos para dar de alta las líneas que generaron la deuda que motivó la posterior inclusión en ficheros de información de solvencia patrimonial y crédito. Junto con los contratos, se aportó igualmente copia del DNI presentado en el momento de la contratación para proceder al citado alta.

Por lo tanto, se ha de analizar el grado de culpabilidad existente en el presente caso. La jurisprudencia ha venido exigiendo a aquellas entidades que asuman en su devenir, un constante tratamiento de datos de clientes y terceros, que en la gestión de los mismos, acrediten el cumplimiento de un adecuado nivel de diligencia, debido a las cada vez mayor casuística en cuanto al fraude en la utilización de los datos personales. En este sentido se manifiesta, entre otras, la sentencia de la Audiencia Nacional de 29/04/2010 al establecer que *“La cuestión no es dilucidar si la recurrente trató los datos de carácter personal de la denunciante sin su consentimiento, como si empleó o no una diligencia razonable a la hora de tratar de identificar a la persona con la que suscribió el contrato.”*

A mayor abundamiento, y por lo que a la posible contratación fraudulenta de un servicio por suplantación de identidad se refiere, señalaba la Audiencia Nacional en su Sentencia de 6 de julio de 2012 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.”*

Habría que añadir que la posible falsificación de la documentación aportada para realizar la contratación o la presunta suplantación de identidad son cuestiones que deben sustanciarse en el ámbito jurisdiccional pertinente.

De acuerdo con estos criterios se puede entender que ORANGE empleó una razonable diligencia en el proceso de contratación de las líneas afectadas, ya que adoptó las medidas necesarias para identificar a la persona que realizaba la contratación.

Finalmente, parece que, hasta la fecha, ORANGE no ha excluido los datos de la denunciante del fichero ASNEF ya que no tiene ninguna constancia del supuesto fraude. Por tanto, Dña. **A.A.A.** podrá interponer denuncia donde se ponga de manifiesto la utilización fraudulenta de sus datos personales para dar de alta las líneas que generaron

la deuda imputada y adjuntarla a la reclamación que presente ante ORANGE. Posteriormente podrá ejercitar su derecho de cancelación ante la entidad utilizando los modelos que figuran en el siguiente enlace: <https://www.agpd.es>.

En conclusión, tras analizar los hechos denunciados y las actuaciones de investigación llevadas a cabo por esta Agencia, no se han acreditado elementos probatorios que permitan atribuir a ORANGE ESPAGNE SAU una vulneración de la normativa vigente en materia de protección de datos.

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 ORANGE ESPAGNE S.A.U. y a 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