



Procedimiento Nº A/00383/2015

**RESOLUCIÓN: R/00341/2016**

En el procedimiento A/00383/2015, instruido por la Agencia Española de Protección de Datos a la entidad **VIROA TELECOMUNICACIONES SL**, vista la denuncia presentada y en base a los siguientes,

**ANTECEDENTES**

**PRIMERO:** Con fecha de 28/7/15 tienen entrada en esta Agencia Española de Protección de Datos oficio de la Policía Local del Ayuntamiento de Liria (Valencia) en relación a la localización en la vía pública de documentación con datos de carácter personal.

**SEGUNDO:** Se refieren los hechos a una localización, el día 24/7/15, en la **Urbanización XXXX** denunciándose lo siguiente:

*\* Durante el servicio de vigilancia se observó junto a unos contenedores un vertido de documentación de carácter sensible, documentos personales de DNI, entidades financieras, etc. Correspondientes a una empresa de telecomunicaciones "Viroa Telecomunicaciones S.L."*

Copia de la citada documentación se ha incorporado al expediente, así como reportaje fotográfico de la localización de la misma.

**TERCERO:** Se manifiesta en la denuncia que el presunto responsable es **Viroa Telecomunicaciones S.L.** con domicilio (C/....1) (**Valencia**).

**CUARTO:** Con fecha 14/12/15 se acordó someter a trámite de audiencia previa el presente procedimiento de apercibimiento A/00383/2015

Dicho acto fue notificado mediante publicación en el BOE de fecha 8/1/16.

**HECHOS PROBADOS**

1º Consta denuncia presentada por la Policía Local del Ayuntamiento de Liria (Valencia) en relación a la localización en la vía pública de documentación con datos de carácter personal.

2º Consta informe de la policía local manifestando que: *\*Durante el servicio de vigilancia se observó junto a unos contenedores un vertido de documentación de carácter sensible, documentos personales de DNI, entidades financieras, etc. Correspondientes a una empresa de telecomunicaciones "Viroa Telecomunicaciones S.L."*

3º La citada documentación se localizó el día 24/7/15 en la **Urbanización XXXX**. Copia de la citada documentación se ha incorporado al expediente, así como reportaje fotográfico de la localización de la misma.

4º No constan alegaciones al trámite de audiencia previa que fue notificado mediante publicación en el BOE de fecha 8/1/16

**FUNDAMENTOS DE DERECHO**

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 de la LOPD.

II

El art. 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

*“Seguridad de los datos:*

*Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.”*

El Art 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

*“Seguridad del tratamiento:*

*1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las 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 autorizados, 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”*

III

La LOPD en su artículo 1 dispone que *“la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”*.

El artículo 2.1 de la misma ley orgánica establece: *“1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados”*.

El artículo. 3 de la LOPD establece las definiciones de responsable de fichero o tratamiento, de encargado de tratamiento y de cesión de datos:

*“d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*

.....

*g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*

.....

*l) Cesión o comunicación de datos: toda revelación de datos realizada a la persona distinta del*

*interesado.”*

La vigente LOPD atribuye la condición de responsables de las infracciones a los responsables de los ficheros (art. 43), concepto que debe integrarse con la definición que de los mismos recoge el artículo 3.d), arriba citado, que incluye en el concepto de responsable tanto al que lo es del fichero como al del tratamiento de datos personales. En el presente caso, **VIROA TELECOMUNICACIONES** es responsable de los ficheros y tratamientos, derivados de su actividad laboral, y en conformidad con las definiciones legales está sujeto al régimen de responsabilidad recogido en el Título VII de la LOPD.

#### IV

El artículo 9 de la LOPD, dispone:

*“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 la 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.”*

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de “fichero” y “tratamiento” contenidas en la LOPD.

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso, –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

La documentación encontrada procedente de esa entidad entra en la consideración de documentación en soporte papel, contiene datos personales, debiéndosele aplicar las medidas de seguridad previstas reglamentaria a este tipo de ficheros y que han sido contempladas en

el documento de seguridad de la denunciada.

Los hechos, que traen causa en este procedimiento, derivan de la localización, en la **Urbanización XXXX, y junto a unos contenedores, de un vertido de documentación de carácter sensible, documentos personales de DNI, entidades financieras, etc. Correspondientes a una empresa de "Viroa Telecomunicaciones S.L."**

Ante estos hechos debe tenerse en cuenta lo establecido en el artículo 112 del RD 1720/07, de desarrollo de la LOPD, que dispone lo siguiente:

*"1.La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.*

*2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que evite el acceso a la información contenida en las mismas o a su recuperación posterior"*

Se establece en este artículo las medidas que se tendrán que aplicar en los procesos de copia o reproducción de documentos; haciendo mención especial a la necesidad de proceder a la destrucción de las copias, o reproducciones desechadas, de forma que se evite el acceso a la información contenida en las mismas o a su recuperación posterior. Debe señalarse que el incumplimiento de este tipo de previsión implica un riesgo muy importante en la divulgación no deseada de documentos con datos personales.

En conclusión, es de aplicación lo dispuesto en artículo 92.4, del citado Reglamento, que dispone que: *"Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de aquellas medidas dirigida a evitar el acceso a la información contenida en el mismo o su recuperación posterior"*. Esta previsión del artículo 92 es también de aplicación a los ficheros y tratamientos no automatizados, en virtud de la remisión que se hace desde el artículo 105.2.d.

En ese apartado cuarto se regulan las obligaciones que tendrán que aplicarse cuando vaya a desecharse cualquier documento o soporte que contenga datos personales; estableciéndose, aunque no se definen en concreto, las medidas que serán aquellas que eviten el acceso a la información contenida en los mismos, así como su posible recuperación posterior. En el presente caso la aparición de documentación, procedente de la entidad denunciada, abandonada en la vía pública permite deducir que ésta no observó la diligencia adecuada; puesto que tenía que haber aplicado las medidas que imposibilitaran la recuperación posterior de la misma, o detallado por escrito la documentación entregada, en el caso que se cediera a un tercero para su destrucción.

## V

El hecho constatado en el presente procedimiento relativo a la aparición de documentación procedente de la entidad denunciada, en la vía pública y accesible a terceros, supone una inobservancia del deber de adoptar las medidas de seguridad pertinentes por parte de la responsable del tratamiento

El artículo 44.3 h) califica como infracción grave: *"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"*. De acuerdo con los fundamentos anteriores, se deduce que por parte de la entidad denunciada se ha producido una vulneración de la de seguridad de los datos, que ha tenido como consecuencia que los datos personales, pudieran



ser vistos por un tercero, infracción que procede calificarla en el grado señalado.

La exigencia de la “culpabilidad” deriva de lo que señala el artículo 130 de la Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Publicas y del Procedimiento Administrativo Común – LRJPAC- cuando dice que: *“Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia”*.

Si bien en materia sancionadora rige el principio de culpabilidad, la expresión “simple inobservancia”, del art. 130.1 de la Ley 30/92, permite la sanción por inobservancia del deber de cuidado. Tal es la interpretación que ha establecido la Audiencia Nacional en la sentencia de 6/02/08. Existe una obligación de resultado, que no se ha cumplido, pues documentación con datos de carácter personal procedente de la entidad denunciada se encontró si destruir, de lo que se desprende una falta de negligencia del responsable del tratamiento, obligado a implementar las medidas de seguridad.

La necesidad de especial diligencia en la custodia de la documentación por parte del responsable y encargado del tratamiento ha sido puesta de relieve por la Audiencia Nacional, en diversas sentencias, en particular en la sentencia de 25/06/09, Rec. 237/2008, que manifiesta: *“Es doctrina reiterada en esta Sala, SSAN, sec. 1ª, de 25/1/06 (re. 227/2004), 28/06/06 (Re. 290/2004), que “No basta con la aplicación formal de las medidas de seguridad, pues resulta exigible que aquellas se instauren y pongan en práctica de manera efectiva... Se impone, en consecuencia, una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva la recurrente es, por disposición legal, una deudora de seguridad en materia de datos y puesto que es una deudora de seguridad en materia de datos es insuficiente, según se desprende la doctrina de la Sala que se acaba de exponer, con acreditar que se adoptaron una serie de medidas, pues dicha entidad también es responsable de que las mismas se cumplan y ejecuten con rigor”*

## VI

Debe precisarse que los hechos acreditados, por el contra, no suponen una vulneración del art. 10 de la LOPD que establece:

*“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”*.

Ahora bien la obligación impuesta por el artículo 10 debe entenderse como una obligación de resultado, donde lo relevante, tal como lo ha entendido la Audiencia Nacional entre otras en la sentencia de 18/06/09, es que se llegue a producir la divulgación de un secreto, no siendo relevante (a los efectos de la violación del deber de secreto), que exista o no una omisión de las medidas de seguridad. En el caso que nos ocupa aun cuando a entidad denunciada es responsable de la custodia de la documentación relativa a su actividad laboral, la documentación fue recuperada y retirada por la Policía Local pero no se puede considerar que fuera revelada a terceras personas vulnerando así el deber de secreto. Entendiéndose así que no se ha producido vulneración del artículo 10 por parte de la entidad denunciada.

## VII

En el presente caso según ha quedado expuesto se produjo la recuperación por la policía local



de documentación, con datos de carácter personal, de cuya seguridad en orden a la custodia, conservación o destrucción de la misma, era responsable la entidad **VIROA TELECOMUNICACIONES**. La recuperación de dicha documentación supone que la entidad denunciada no observó la diligencia adecuada, ya que tenía que haberse asegurado que la documentación fuera destruida totalmente imposibilitando su recuperación posterior

El hecho constatado en el presente procedimiento, relativo a la aparición de documentación procedente de la entidad denunciada accesible a terceros supone una inobservancia del deber de adoptar las medidas de seguridad pertinentes por parte de la responsable del tratamiento

El artículo 44.3 h) califica como infracción grave: *“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*

## VIII

De acuerdo con lo expuesto, se iniciaron actuaciones contra **VIROA TELECOMUNICACIONES** por la presunta vulneración del deber adoptar las medidas de seguridad contempladas en el RLOPD.

Por otra parte, se tuvo en cuenta que la entidad denunciada no ha sido sancionada o apercibida con anterioridad.

En consecuencia, de conformidad con lo establecido en el artículo 45.6 de la LOPD, se acordó someter a la citada entidad a trámite de audiencia previa al apercibimiento en relación con la denuncia por infracción del artículo 9 de la LOPD.

La disposición final quincuagésima sexta de la Ley 2/2011 de 4 de marzo de Economía Sostenible (BOE 5-3-2011) añadió un nuevo apartado 6 al artículo 45 de la Ley 15/1999 de Protección de Datos en lugar del existente hasta su promulgación del siguiente tenor:

*“Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:*

*A) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.*

*B) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.*

*Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento”.*

La Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común –que, al decir de su Exposición de Motivos (punto 14) recoge *“los principios básicos a que debe someterse el ejercicio de la potestad sancionadora de la Administración y los correspondientes derechos que de tales principios se derivan para los ciudadanos extraídos del Texto Constitucional y de la ya consolidada jurisprudencia sobre la materia”*- consagra el principio de aplicación retroactiva de la norma



más favorable estableciendo en el artículo 128.2 que “*las disposiciones sancionadoras producirán efecto retroactivo en cuanto favorezcan al presunto infractor*”.

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado apartado 6. Junto a ello se constata una cualificada disminución de la culpabilidad del imputado teniendo en cuenta que no consta vinculación relevante de la actividad del denunciado con la realización de tratamientos de datos de carácter personal, su volumen de negocio o actividad, el carácter puntual del hecho y no constan beneficios obtenidos como consecuencia de la comisión de la infracción.

## IX

La sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección Primera, recurso 455/2011, de 29/11/2013, analiza el apercibimiento como un acto de naturaleza no sancionadora, como se deduce del fundamento de derecho SEXTO:

*“Debe reconocerse que esta Sala y Sección en alguna ocasión ha calificado el apercibimiento impuesto por la AEPD, en aplicación del artículo examinado, como sanción (SAN de 7 de junio de 2012, rec. 285/2010), y en otros casos ha desestimado recursos contencioso-administrativos interpuestos contra resoluciones análogas a la recurrida en este procedimiento, sin reparar en la naturaleza no sancionadora de la medida expresada (SSAN de 20 de enero de 2013, rec. 577/2011, y de 20 de marzo de 2013, rec. 421/2011). No obstante, los concretos términos en que se ha suscitado la controversia en el presente recurso contencioso-administrativo conducen a esta Sala a las conclusiones expuestas, corrigiendo así la doctrina que hasta ahora venía presidiendo la aplicación del artículo 45.6 de la LOPD.”*

Además, la sentencia interpreta o liga apercibimiento o apercibir con el requerimiento de una actuación para subsanar la infracción, y si no existe tal requerimiento, por haber cumplido las medidas esperadas relacionadas con la infracción, no sería apercibimiento, sino archivo como se deduce del fundamento de derecho SEXTO:

*“Pues bien, en el caso que nos ocupa el supuesto concreto, de entre los expresados en el apartado quinto del artículo 45, acogido por la resolución administrativa recurrida para justificar la aplicación del artículo 45.6 de la LOPD es el primero, pues aprecia “una cualificada disminución de la culpabilidad del imputado teniendo en cuenta que no consta vinculación relevante de la actividad del denunciado con la realización de tratamientos de datos de carácter personal, su volumen de negocio o actividad y no constan beneficios obtenidos como consecuencia de la comisión de la infracción”, tal y como expresa su fundamento de derecho VII.*

*Por ello, concurriendo las circunstancias que permitían la aplicación del artículo 45.6 de la LOPD, procedía “apercibir” o requerir a la denunciada para que llevara a cabo las medidas correctoras que la Agencia Española de Protección de Datos considerase pertinentes, en sustitución de la sanción que de otro modo hubiera correspondido.*

*No obstante, dado que resultaba acreditado que la denunciada por iniciativa propia había adoptado ya una serie de medidas correctoras, que comunicó a la Agencia Española de Protección de Datos, y que esta había verificado que los datos del denunciante no eran ya localizables en la web del denunciado, la Agencia Española de Protección de Datos no consideró oportuno imponer a la denunciada la obligación de llevar a cabo otras medidas correctoras, por lo que no acordó requerimiento alguno en tal sentido a ésta.*

*Recuérdese que al tener conocimiento de la denuncia la entidad denunciada, procedió por*

*iniciativa propia a dirigirse a Google para que se eliminara la URL donde se reproducían la Revista y el artículo, a solicitar a sus colaboradores que suprimieran cualquier nombre de sus artículos o cualquier otra información susceptible de parecer dato personal y que revisaran las citas del área privada de la web para borrar cualquier otro dato sensible, y, por último, a revisar la configuración de los accesos para que los buscadores no tuvieran acceso a las Revistas.*

*En consecuencia, si la Agencia Española de Protección de Datos estimaba adoptadas ya las medidas correctoras pertinentes en el caso, como ocurrió, tal y como expresa la resolución recurrida, la actuación administrativa procedente en Derecho era al archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la entidad denunciada, pues así se deduce de la correcta interpretación del artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica.*

*Por el contrario, la resolución administrativa recurrida procedió a “apercibir” a la entidad PYB ENTERPRISES S.L., aunque sin imponerle la obligación de adoptar medida correctora alguna, lo que solo puede ser interpretado como la imposición de un “apercibimiento”, entendido bien como amonestación, es decir, como sanción, o bien como un mero requerimiento sin objeto. En el primer caso nos hallaríamos ante la imposición de una sanción no prevista en la LOPD, con manifiesta infracción de los principios de legalidad y tipicidad en materia sancionadora, previstos en los artículos 127 y 129 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en el segundo supuesto ante un acto de contenido imposible, nulo de pleno derecho, de conformidad con lo previsto en el artículo 62.1.c) de la misma Ley.”*

Al haberse recuperado la citada documentación, cumpliendo la finalidad del apercibimiento, procede el archivo del presente procedimiento, dada la naturaleza del mismo.

De acuerdo con lo señalado,

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

**SE ACUERDA:**

**1.- ARCHIVAR** el procedimiento **A/00383//2015** seguido contra a **VIROA TELECOMUNICACIONES** con arreglo a lo dispuesto en el artículo 45.6 de la LOPD, en relación con la denuncia por la infracción del artículo 10 de la citada ley.

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 esta acto, según lo previsto en el artículo 46.1 del referido texto legal.

**2.- NOTIFICAR** el presente Acuerdo a **VIROA TELECOMUNICACIONES** y a **AYUNTAMIENTO DE LLIRIA** (Policía Local)



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.

Mar España Martí  
Directora de la Agencia Española de Protección de Datos