



Procedimiento Nº: A/00160/2016

RESOLUCIÓN: R/01537/2016

En el procedimiento A/00160/2016, instruido por la Agencia Española de Protección de Datos a la entidad **UNOLEC CATALUNYA S.L.**, vista la denuncia presentada por **DIRECCION GENERAL DE LA POLICIA** y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 20/4/15 tiene entrada en esta Agencia un escrito de **DIRECCION GENERAL DE LA POLICIA** de la **Generalitat de Cataluña** en el que declara:

*<<A las 10 horas del día 10 de abril de 2015 se ha personado ante esta unidad instructora el vigilante de seguridad de RENFE PLAZA CATALUNYA con TIP****. Este vigilante se había encontrado un fajo de documentos con datos personales en el interior de la última papelera del andén de la estación de plaza de Cataluña dirección Jefe de aviadores. Toda la documentación corresponde a contratos la empresa EDP Energía. Como que los responsables de esta empresa no han tenido suficiente cuidado de los datos personales que les han estado confiados, hacemos remisión de toda esta documentación.... >>*

SEGUNDO: Examinada la documentación presentada, se encuentra que está compuesta por:

** Contratos de suministro de energía o servicios en los que constan datos personales del cliente, NIF, teléfonos, dirección del punto de suministro, dirección de facturación y código de cuenta bancaria. Algunos aparecen firmados y otros no. Consta como canal FVE, si bien no aparece el agente comercial.*

** En el lateral de los contratos aparecen identificadas las entidades:*

*-- Con CIF A***** correspondiente a HIDROCANTABRICO ENERGIA, SA, actual EDP ENERGIA S.A.*

*-- Con CIF A***** correspondiente a NATURGAS ENERGIA COMERCIALIZADORA, S.A., actual EDP COMERCIALIZADORA S.A.*

** Ordenes de Domiciliación de Adeudo Directo SEPA, en las que aparecen el nombre, DNI, dirección postal y código de cuenta bancaria. Algunos aparecen firmados.*

** Listado de 23 páginas y 40 filas por página, en los que aparece una relación de direcciones, con su calle, número piso y puerta, el código postal, el nombre completo de una persona así como el CUPS de la vivienda y un código. No aparece ninguna titulación del listado, cabecera ni pie de página. Se aprecia que todos los domicilios se corresponden con el código postal ***CP.1. Aparecen diversas marcas en bolígrafo, de significado desconocido.*

** Listado de cuatro páginas y 55 filas por página en los que aparece una relación de direcciones, con su calle, número piso y puerta, el código postal, dos nombres completos de una persona, (aunque muchas veces coinciden) así como el CUPS de la vivienda y un código. En la cabecera de página figura "(C/....1) 1" y al pie aparece "Gavà" y "****CP.1". Aparecen diversas marcas en bolígrafo, de significado desconocido.*

** Listado de cinco páginas y 41 filas por página, en los que aparece una relación de direcciones, con su calle, número piso y puerta, el código postal, dos nombres completos de personas (en muchos casos, coincidentes) así como dos CUPS de las viviendas y un código. En la cabecera*

de página figura "(C/....1) 2" y al pie aparece "****LOCALIDAD.1 ***CP.1". Aparecen diversas marcas en bolígrafo, de significado desconocido, y en algunas páginas se ha escrito a mano "FACTURADORA LOCAL EDP"

* Listado de cinco páginas y 41 filas por página, en los que aparece una relación de direcciones, con su calle, número piso y puerta, el código postal, dos nombres completos de personas (en muchos casos, coincidentes) así como dos CUPS de las viviendas y un código. En la cabecera de página figura "(C/....1) 3" y al pie aparece "****CP.2 ***LOCALIDAD.2".

TERCERO Por parte del Subdirector General de Inspección de Datos, en base al contenido de la denuncia, se procedió a la apertura de actuaciones previas con referencia E/03409/2015 y concluye la investigación con el informe siguiente de la Inspección de Datos:

<<<< 1. Solicitada información a EDP ENERGIA S.A. respecto de una serie de DNI que constan entre la información encontrada, la entidad informa:

* Que respecto de los DNI/NIE *****DNI.1, ***DNI.2, ***DNI.3, ***DNI.4** no consta ningún dato en el sistema/base de datos de clientes.

* Que sólo constan datos relativos al DNI *****DNI.5**. ...

* Que las labores comerciales entre los meses de marzo y abril de 2015 en las zonas de *****LOCALIDAD.1** c. postal *****CP.1** y *****LOCALIDAD.2** c. postal *****CP.2** se realizaron a través de las Fuerzas de Venta Externas UNOLEC y Redes de Impulso.

* Adjunta se remite copia de los contratos suscritos,

* - Que por lo que se refiere al flujo de datos, indicar lo siguiente:

Al iniciar una campaña comercial, se prepara un target de clientes potenciales (cuyos datos son obtenidos de la base de datos de puntos de suministro a que tienen acceso las empresas comercializadoras) y se remite el mismo a la Fuerza de Venta Externa - en adelante, FVE- que en cada campaña se considere oportuno, en base a los acuerdos de colaboración formalizados. Una vez recibido el target por parte de la FVE, los comerciales de la FVE visitan los distintos domicilios -direcciones de suministro- a fin de ofertar los servicios de EDP Comercializador.

2. Solicitada información a EDP COMERCIALIZADORA S.A. aporta idéntica respuesta.

3. Solicitada ampliación de información a EDP ENERGIA S.A. respecto de los datos asociados al DNI *****DNI.5** la entidad aporta copia del contrato, DNI, facturas y orden de adeudo directo. Informa la entidad que la contratación se realizó a través de **UNOLEC CATALUNYA S.L. >>>>**

CUARTO: Con fecha 5/5/16 la Directora de la Agencia Española de Protección de Datos acordó someter a trámite de audiencia previa el presente procedimiento de apercibimiento A/00162/2016

Dicho acto fue notificado mediante publicación en BOE de fecha 27/5/16

HECHOS PROBADOS

1º Consta denuncia presentada por la DIRECCION GENERAL DE LA POLICIA de la Generalitat de Cataluña relativa a la recuperación, con fecha 10/4/15, por parte de un vigilante de seguridad de RENFE de documentación con datos de carácter personal abandonados en una papelería

Se manifiesta que toda la documentación recuperada corresponde a contratos la empresa EDP

Energía.

2º Que la documentación recuperada contiene *Contratos de suministro de energía o servicios en los que constan datos personales del cliente, NIF, teléfonos, dirección del punto de suministro, dirección de facturación y código de cuenta bancaria. Algunos aparecen firmados y otros no. Consta como canal FVE, si bien no aparece el agente comercial.*

3º Consta manifestaciones de EDP ENERGIA S.A. en el sentido de que las labores comerciales entre los meses de marzo y abril de 2015 en las zonas de ***LOCALIDAD.1 c. postal ***CP.1 y ***LOCALIDAD.2 c. postal ***CP.2 se realizaron a través de las Fuerzas de Venta Externas UNOLEC y Redes de Impulso.

4º Consta que al iniciar una campaña comercial, se prepara un target de clientes potenciales y se remite el mismo a la Fuerza de Venta Externa, en este caso UNOLEC, en base a los acuerdos de colaboración formalizados. Una vez recibido ese target son los comerciales que realizan la campaña quienes visitan los distintos domicilios -direcciones de suministro- a fin de ofertar los servicios de EDP Comercializador.

5º Consta que el presente procedimiento se sometió a tramite de audiencia previa que fue notificado mediante publicación en BOE de fecha 27/5/16, al ser devuelta la notificación.

6º Que consultada la situación de UNOLEC CATALUNYA , a través de Internet, se constata que no se han presentado cuentas desde 2013 y aparentemente carece de actividad en la actualidad.

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, UNOLEC, como encargada de tratamiento de EDP ENERGIA S.A., era responsablemente de aquellos tratamientos de datos según el acuerdo suscrito con la empresa responsable y según las órdenes recibidas. Estando 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 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.

Los hechos, que traen causa en este procedimiento, derivan de la localización, por un vigilante de seguridad de RENFE y abandonados en la papelera de una estación, de contratos de suministros de energía de la empresa EDP, en relación a una campaña comercial que era gestionada por la Fuerza de Venta Externa, es esta caso UNOLEC

Ante estos hechos debe tenerse en cuenta lo establecido 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 se 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 Real Decreto 1720/07, Reglamento de desarrollo de la LOPD, de 21 de diciembre, 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 este 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 contenido en los mismos, así como su posible recuperación posterior. En este caso, la aparición de documentación procedente de la entidad denunciada permite deducir que está no observó la diligencia adecuada, ya que tenía que haberse asegurado las medidas que imposibilitaran la recuperación posterior de la misma, o en el caso que se cediera a un tercero para su destrucción haber detallado por escrito la documentación entregada.

V

El hecho constatado en el presente procedimiento, relativo a la aparición de documentación procedente de la entidad denunciada abandonada en una papelería 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 Públicas 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

El artículo 10 de la LOPD establece que: *“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”.*

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento. Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así el Tribunal Superior de Justicia de Madrid ha declarado en su Sentencia de 19 de julio de 2001: *“El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)”.*

En este sentido, la sentencia de la Audiencia Nacional de fecha 18 de enero de 2002, recoge en su Fundamento de Derecho Segundo, y tercer párrafo: *“El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable –en este caso, la entidad bancaria recurrente- de los datos almacenados –en este caso, los asociados a la denunciante- no puede revelar ni dar a conocer su contenido teniendo el “deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo” (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto.*

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE. En efecto, este precepto contiene un “instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos” (STC 292/2000). Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino” (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, “es decir, el poder de resguardar su vida privada de una publicidad no querida”

En el caso que nos ocupa, el denunciante es responsable de la custodia o de la adecuada destrucción de la documentación generada en relación a su actividad laboral y que ha sido recuperada por el denunciante, existiendo pues, una omisión del deber de secreto, produciéndose una ausencia de confidencialidad, por lo que se considera que se ha cometido una infracción del transcrito artículo 10 de la LOPD.

VII

El artículo 44.3.d) de la LOPD, califica como infracción grave:

“La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente ley”

De acuerdo con los fundamentos anteriores, se deduce que por parte de la entidad denunciada se ha producido una vulneración del deber de secreto y de seguridad de los datos, infracciones que procede calificarlas como graves. Sin que pueda exonerarse su responsabilidad tal como se ha demostrado en este procedimiento, por lo que procede su imputación, elemento necesario en el derecho administrativo sancionador tal como establece la STS de 27/5/99: *“Para la imposición de una sanción y las consecuencias derivadas del ilícito administrativo, no basta que la infracción esté tipificada y sancionada...sino que es necesario que se aprecie en el sujeto infractor el elemento o categoría denominado culpabilidad. La culpabilidad es el reproche que se hace a una persona, porque ésta debió haber actuado de modo distinto de cómo lo hizo”*.

VIII

El hecho constatado de la difusión de datos personales fuera del ámbito de la entidad denunciada establece la base de facto para fundamentar la imputación de las infracciones de los artículos 9 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto en el que un mismo hecho deriva en dos infracciones, dándose la circunstancia que la comisión de una implica necesariamente la comisión de la otra. Esto es, si un documento interno que contiene información sobre datos personales sale del ámbito de la entidad responsable de su confidencialidad, se está produciendo un incumplimiento de las medidas de seguridad exigidas a dicho responsable que, a su vez, deriva en una vulneración del deber de secreto.

Por lo tanto, aplicando el artículo 4.4 del Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora que señala que *“en defecto de regulación específica establecida en la norma correspondiente, cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida”*, procede subsumir ambas infracciones en una. Dado que, en este caso, se ha producido una vulneración de las medidas de seguridad, calificada como grave por el artículo 44.3.h) de la LOPD y también un incumplimiento del deber de guardar secreto, calificado como grave en el artículo 44.3.g) de la misma norma, procede imputar únicamente la infracción del artículo 9 de la LOPD.

IX

En el presente caso, según ha quedado expuesto, produjo la recuperación por vigilante de una estación de dichos contratos con documentación con datos de carácter personal. Por tanto, se concluye que la conducta imputada se ajusta a la tipificación prevista en el 44.3.d) de la LOPD.

En este caso, el hecho de que la documentación a destruir no lo fuera, supone que la entidad denunciada no observó la diligencia adecuada, ya que tenía que haberse asegurado que la documentación fuera destruirse 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*

X

De acuerdo con lo expuesto, se iniciaron actuaciones contra por la presunta vulneración deber de secreto recogidos en los artículos señalados.

Por otra parte, se tuvo en cuenta que la entidad denunciada no ha sido sancionado o apercibido 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) ha añadido 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 concurren 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.

XI

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 los citados documentos, cumpliendo la finalidad del apercibimiento, procede el archivo del presente procedimiento, dada la naturaleza del mismo.

De acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1.- ARCHIVAR el procedimiento A/00160/2016 seguido contra a **UNOLEC CATALUNYA S.L.** 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 **UNOLEC CATALUNYA S.L y DIRECCION GENERAL DE LA POLICIA**

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 reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

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 esta 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