Procedimiento Nº: A/00096/2017

RESOLUCIÓN: R/01288/2017

En el procedimiento A/00096/2017, instruido por la Agencia Española de Protección de Datos a la entidad INFORMATICA ZARAGOZA (JAVAL INFORMATICA, S.L.), vista la denuncia presentada por Doña ***A.A.A.,*** y en virtud de los siguientes

ANTECEDENTES

PRIMERO: Con fecha 16 de junio de 2016, tuvo entrada en esta Agencia un escrito remitido por Doña ***A.A.A.,*** en el que manifiesta lo siguiente: En el mes de junio de 2015, la entidad denunciada, a la que acudió para la reparación de un disco duro, propiedad de la denunciante, procedió a la descarga de toda su información personal en un disco duro propiedad de la empresa, sin su autorización, el cual fue vendido con posterioridad a una tercera persona con toda la información contenida en el mismo, aunque supuestamente para el nuevo comprador se trataba de un disco duro nuevo.

El nuevo comprador hizo una copia de sus datos y amenazó a la empresa para obtener lucro. Este hecho fue juzgado en el Juzgado de Instrucción número 7 de Zaragoza.

Anexa, entre otros, copia de las Diligencias Previas llevadas a cabo en el Juzgado de Instrucción número 7 de Zaragoza, donde queda constancia de los hechos denunciados ante esta Agencia.

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:

a. La empresa efectúa todo tipo de actividades relacionadas con la informática.

b. Con fecha 20 de junio de 2015, la denunciante encargó a la empresa el trabajo de recuperar información de un disco duro estropeado. Dicho volcado se realizó con su consentimiento en un disco duro del establecimiento, pero posteriormente y a petición de la denunciante se hizo a otro de su propiedad.

c. Los datos volcados al disco duro de la tienda se dejó para su formateo, pero, por error de un empleado, se colocó en la estantería como nuevo.

d. Posteriormente se personó un cliente interesado en la compra de un disco duro y le fue entregado dicho disco con el volcado de la información de la denunciante.

e. Al recibir un correo en el que se comunicaba lo sucedido, la empresa se puso en contacto con el comprador dando

la posibilidad de darle otro disco nuevo y solicitando que no tocase la información existente en el que se habían llevado, y a su vez dicho comprador se puso en contacto con la denunciante para explicar lo sucedido.

f. Así mismo, dicho comprador ha procedido a realizar amenazas al establecimiento con fines de lucro, lo cual fue denunciado y ha sido instruido en Diligencias Previas seguido en el Juzgado nº 7 de Zaragoza.

TERCERO: Con fecha 28 de marzo de 2017, la Directora de la Agencia Española de Protección de Datos acordó someter a trámite de audiencia previa el presente procedimiento de apercibimiento A/00096/2017. Dicho acuerdo fue notificado al denunciado.

CUARTO: Con fecha 25 de abril de 2017, se recibe en esta Agencia escrito del denunciado en el que comunica: que ya han reconocido el error que sucedió. Fueron ellos mismos los que advirtieron a la denunciante lo que pasó e informando a los cuerpos y fuerzas de seguridad. Se han adoptado las medidas necesarias para que no vuelva a ocurrir.

HECHOS PROBADOS

PRIMERO: Doña ***A.A.A.*** acudió a la entidad Javal Informática, S.L., para la reparación de un disco duro de su propiedad.

SEGUNDO: Javal Informática, S.L., procedió a la descarga de toda la información personal contenida en el disco duro de Doña ***A.A.A.*** en un disco duro propiedad de la empresa.

TERCERO: El disco duro, propiedad de la empresa, donde se copió la información de la denunciante, fue vendido con posterioridad, como si fuese nuevo, a una tercera persona con toda la información contenida en el mismo.

CUARTO: La entidad responsable expone que cuando tuvieron conocimiento de los hechos, adoptaron las siguientes **medidas correctoras.**

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 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 su 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."

El art. 9 de la LOPD *establece* el principio de *"seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquélla, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado".*

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.

En lo que respecta a los ficheros el art. 3.a) los define como *"todo conjunto organizado de datos de carácter personal"* con independencia de la modalidad de acceso al mismo.

Por su parte la letra c) del mismo artículo permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente expediente, la *"comunicación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.

Para completar el sistema de protección en lo que a la seguridad afecta, el art. 44.3.h) de la LOPD tipifica como infracción grave el "*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".*

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.

Es necesario analizar las previsiones que el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el R. D. 1720/2007, de 21 de diciembre, realiza para garantizar que no se produzcan accesos no autorizados a los ficheros.

El citado Reglamento define en su artículo 5.2 ñ) el *"Soporte"* como el "*objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos*".

Por su parte, en el artículo 81.1 del mismo Reglamento se establece que "*Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico*".

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma.

El Reglamento citado, distingue entre medidas de seguridad aplicables a ficheros y tratamientos automatizados (Capítulo III Sección 2ª del Título VIII) y las medidas de seguridad aplicables a los ficheros y tratamientos no automatizados (Capítulo IV Sección 2ª del Título VIII).

Entre las medidas de seguridad de nivel básico, el Reglamento expone en su artículo 92, respecto de la gestión de soportes y documentos, que:

"1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. 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 medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas."

La entidad Javal Informática, S.L., debió, por ello, adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información que se contenían en el disco duro de la denunciante. Tales medidas no fueron adoptadas en el presente caso. Prueba de ello es el hecho de que el disco duro con la información de la

denunciante se vendió a una tercera persona.

En el presente caso, ha quedado acreditado que la entidad Javal Informática, S.L., no adoptó las medidas de índole técnica y organizativa necesarias que garantizasen la seguridad de los datos de carácter personal, de manera que se evitase el acceso no autorizado a los datos de los mismos.

III

El artículo 44.3.h) de la LOPD, considera 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."

Dado que ha existido una vulneración en las medidas de seguridad de la entidad Javal Informática, S.L., se considera que la citada entidad ha incurrido en la infracción grave descrita.

IV

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.

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, como el teléfono de contacto, 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, la entidad Javal Informática, S.L., es responsable de que los datos de su cliente no se facilitase a terceros. Se comprueba la existencia de un incumplimiento 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.

V

El artículo 44.3.d) de la LOPD, califica como infracción muy 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, entendemos que por parte de la entidad Javal Informática, S.L., se ha producido una vulneración del deber de secreto que procede calificar como infracción grave.

VI

En el presente caso ha quedado acreditado que la entidad Javal Informática, S.L., facilitó a un tercero un disco duro conteniendo datos de carácter personal de la denunciante. Estos hechos suponen una vulneración de las medidas de seguridad así como del deber de guardar secreto por lo que la citada entidad ha incurrido en las infracciones graves descritas.

El artículo 45.6 de la LOPD, dispone:

"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."

Trasladando las consideraciones expuestas al supuesto que nos ocupa, se observa que la infracción de la LOPD de la que se responsabiliza a la denunciada es una infracción "grave"; que la denunciada no ha sido sancionada o apercibida por este organismo en ninguna ocasión anterior; y que concurren de manera significativa varias de las circunstancias descritas en el artículo 45.5 de la LOPD. Todo ello, unido a la naturaleza de los hechos que nos ocupan, justifica que la AEPD no acuerde la apertura de un procedimiento sancionador y que opte por aplicar el artículo 45.6 de la LOPD.

Ahora bien, es obligado hacer mención a la Sentencia de la Audiencia Nacional

de 29/11/2013, (Rec. 455/2011), Fundamento de Derecho Sexto, que sobre el apercibimiento regulado en el artículo 45.6 de la LOPD y a propósito de su naturaleza jurídica advierte que "*no constituye una sanción"* y que se trata de "*medidas correctoras de cesación de la actividad constitutiva de la infracción"* que *sustituyen* a la sanción. La Sentencia entiende que el artículo 45.6 de la LOPD confiere a la AEPD una "*potestad"* diferente de la sancionadora cuyo ejercicio se condiciona a la concurrencia de las especiales circunstancias descritas en el precepto.

En congruencia con la naturaleza atribuida al apercibimiento como una alternativa a la sanción cuando, atendidas las circunstancias del caso, el sujeto de la infracción no es merecedor de aquella y cuyo objeto es la imposición de medidas correctoras, la SAN citada concluye que cuando no se requieran medidas correctoras, lo procedente en Derecho es acordar el archivo de las actuaciones.

En este caso concreto, atendida la naturaleza de la infracción consistente en un hecho puntual que no admite corrección ni la adopción de una concreta medida correctora, y teniendo en consideración las manifestaciones efectuadas acerca de las medidas adoptadas por la entidad denunciada, debe procederse en consecuencia, a resolver el archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la denunciada, en aplicación de la interpretación del artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica. Recordando que la reiteración en conductas como la denunciada constituye un supuesto sobre el que concurren las circunstancias previstas para la aplicación del régimen sancionador contemplado en la LOPD.

A la vista del pronunciamiento recogido en la SAN de 29/11/2013 (Rec. 455/2011) de acuerdo con lo señalado se debe proceder al archivo de las actuaciones.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- ARCHIVAR (**A/00096/2017**) las actuaciones practicadas a la entidad Javal Informática, S.L.**,** con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, con relación a la denuncia por infracción de los artículos 9.1 y 10 de la LOPD, tipificadas como graves en los artículos 44.3.h) y 44.3.d) de la citada Ley Orgánica.

2.- NOTIFICAR el presente Acuerdo a INFORMATICA ZARAGOZA (JAVAL INFORMATICA S.L.)**.**

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 los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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