Procedimiento Nº PS/00248/2008

RESOLUCIÓN: R/01202/2008

En el procedimiento sancionador **PS/00248/2008**, instruido por la Agencia Española de Protección de Datos a la entidad **NORD 3000 ASSESSORS, S.L**., vista la denuncia presentada por Ayuntamiento De Terrassa y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 1/06/2006, tuvo entrada en esta Agencia, un escrito remitido por la Concejalía de Servicios de Régimen Interior del Ayuntamiento de Terrassa, en el que acompañaba un informe de la Policía Municipal de la localidad, mediante el cual informaba del hallazgo de documentos el día 25/05/2006, en la concurrencia de la (c/.....) y (c/.....) de dicha localidad.

El informe de 26/05/2006 de la Policía Municipal señala que el día 25/05/2006 recibió una llamada del "*Diari de Terrassa*" notificando que había aparecido documentación esparcida por el suelo, en las (c/.....) y (c/.....). La Policía Municipal detalla que se trata de impresos con el membrete de "*Asesoría Nord Assesors*", relativos a "*borradores de hacienda*" y otros documentos de particulares. La Policía contactó el 26/05/2006, con D. J.J.J., responsable de la Asesoría, manifestando este , que "*dejó en la tarde de ayer dicha documentación dentro de una caja de cartón en la puerta de su oficina*", para que se la llevase "*una empresa de recogida*", sin saber como pudo ir al lugar del hallazgo.

Adjunta la Concejalía los siguientes documentos:

1) Copia de correos electrónicos remitidos el 12/05/2006 contiendo al menos 50 líneas de direcciones de correos electrónicos con el asunto "*Torneo de verano*"

2) Hoja "*Listado recordatorios*", con datos de nombre y apellido y modalidad de contratación, y de empresas,

3) Portada de un fax enviado el 12/05/2006, por la colocación de una puerta, conteniendo nombres y apellidos y DNI de una persona.

4) Fax de 18/12/2001 conteniendo nombre y apellidos de un usuario y un NIE, faxes de petición de alta de trabajadores con su nombre y NIE

5) Copia de modificación de datos de tres trabajadores realizado mediante la aplicación Winsuite, para la Tesorería General de la Seguridad Social constando el NIF, nombre y apellidos, y la empresa, así como, por otro lado, nombre y apellidos y NIE de la empleada que gestiona dichos trámites, así como las claves de acceso al Sistema Red de dicha Tesorería.

6) Relación de TC2, en formato justificante de transmisión de fax, a la Tesorería General de la Seguridad Social, conteniendo NAF de la empresa Estructures y Construccions Serjo.

7) Copia de fax remitida el 28/04/2006 conteniendo nombre y apellidos de una persona dirección y NIF

8) NIF y nombres y apellidos de personas de diferentes empresas, otorgando representación para trámites en Seguridad Social a Dña A.A.A..

9) Datos de liquidación y finiquito de un trabajador de "Estructuras y Construcciones Emerjo, conteniendo nombre apellidos, NIF y motivo de baja

10) Nómina de una trabajadora fechada a 8/05/2006.

11) Documento de la Oficina de extranjeros conteniendo nombre y apellidos y NIE "Resolución de concesión de autorización de residencia y trabajo por cta. Ajena"

SEGUNDO El Director de la Agencia Española de Protección de Datos, tras la recepción de la denuncia, ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

- Se procedió por los Servicios de Inspección a la consulta de los 4 ficheros registrados en el Registro General de Protección de Datos por la empresa Nord 3000, apareciendo inscritos desde 12/06/2006 los denominados "*Clientes.DBF*" de facturación y contabilidad, "*A3NOM*" de programas de nóminas, y "*Agentes.DBF*" fichero del programa de facturación y contabilidad.

- Se realizó visita de Inspección el 21/09/2006 a la empresa Nord 3000 Assessors, S.L., nombre que figura en la página www….X…., inscrita en el Registro Mercantil Central, manifestando su representante:

1. Disponen de 4 ficheros inscritos, entre ellos el *A3NOM*, que gestiona materia laboral.
2. La destrucción de documentación de la Gestoría se realiza con destructoras de papel, y después se deposita en la puerta del establecimiento, recogiéndose por el Ayuntamiento.
3. El día 25/05/2006, el personal de la Asesoría detectó que faltaba una caja que contenía documentación y que iba a ser destruida, situada cerca de la puerta de salida.
4. El día 26/05/2006, tuvo una conversación con personal del Diari de Terrassa, que le informaron que habían encontrado documentación de Nord 3000, teniéndose conocimiento de la publicación el 27 de la noticia en el citado diario.
5. Con fecha 29/05/2006, el representante de Nord 3000 interpuso denuncia ante la Policía Municipal de la localidad, por hurto sucedido el 25/05/2006 haciendo constar que "*Se depositó una caja cerrada con documentación de archivo cerca de la puerta de salida de la oficina con el objeto de entregar al servicio de recogida de papel y cartón para reciclaje del ayto Terrassa…aproximadamente una hora después ya no estaba allí*."
6. Se mostró parte de los documentos hallados al representante de Nord 3000, que reconoció como propia y detalló en que consistía: notificaciones de envíos de

altas a la Tesorería General de la Seguridad Social, impresión de borradores de declaraciones de actividades empresariales de actividades empresariales en estimación objetiva, confeccionadas con el programa de módulos de la AEAT, copia de DNI y tarjeta sanitaria de una trabajadora, comunicaciones efectuadas al Sistema red con datos personales, solicitud de registro de personal de Nord 3000 para el acceso a servicios de certificación efectuadas ante la Fábrica Nacional de Moneda y Timbre y listados de trabajadores y empresas resumen de nómina, nóminas y finiquitos.

7. Los Inspectores accedieron a la aplicación *A3NOM* en la que se realizó una búsqueda con los criterios contenidos en una relación de trabajadores de la Empresa Padua 33, coincidiendo la que se visualiza con la que se halló, también coinciden y se hallan los datos del DNI y tarjeta sanitaria, asimismo, se accedió al Programa de Módulos de la AEAT, imprimiendo los datos de un documento de Morante Robles Juan Pedro, que coincide con el hallado.

8. El representante aportó previo requerimiento de los Inspectores, copia del documento de seguridad de los ficheros automatizados, constando copia de la resolución de inscripción de ficheros de12/06/2006. También se aportaron contratos con tres empresas, de cuyos trabajadores figuran datos personales hallados, fechados todos el 1/07/2006

TERCERO: Con fecha 14/05/2008, el Director de la Agencia Española de Protección de Datos acordó iniciar, procedimiento sancionador a NORD 3000 ASSESSORS, S.L., por presunta infracción de los artículos 9 y 10 de la Ley Orgánica 15/1999, de 13/12, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificadas como graves en el artículo 44.3.h y 44.3.g) de dicha norma, pudiendo ser sancionada cada una, con multa de 60.101,21 € a 300.506,05 €, de acuerdo con el artículo 45.2 de dicha Ley Orgánica.

CUARTO: Notificado el acuerdo de inicio, mediante escrito de fecha 4/06/2008, Nord 3000 formuló alegaciones, significando:

1) La caja que contenía la documentación estaba dentro de las oficinas, y fue depositada para que se trituraran los documentos y luego ser entregados al servicio de reciclaje del Ayuntamiento. La caja conteniendo la documentación desapareció sin que se sepa quien fue el autor de los hechos, si bien alguien pudo creer que contenía material de oficina, tirando luego los papeles en el parque cercano.

2) Nord 3000 aporta copia de la denuncia que presentó el día 30/05/2006, afirmando en la declaración que los hechos ocurrieron entre las 17,30 y las 18 h del 25/05/2006, y que "*se deposito una caja cerrada con documentación de archivo cerca de la puerta de salida de la oficina con el objeto de entregarla al servicio de recogida de papel y cartón para reciclaje…al efecto de que fuera triturada y reciclada. Aproximadamente una hora después observamos que ya no estaba allí*".

3) Nord 3000 ha empleado una diligencia más alta de la exigible, pues no puede evitar que terceros de mala fé entren en las oficinas y sustraigan la caja, sin que exista culpabilidad por parte de Nord 30000.

4) Nord 3000 cumple las medidas de seguridad, por cuanto tiene los ficheros registrados y el documento de seguridad, lo que debe llevar junto a la diligente actuación al denunciar

los hechos, a la ausencia de intencionalidad, además, no obtuvo beneficio, y solicita que sea impuesta una sanción inferior, aplicándose el 45. 4 y 5 de la LOPD.

QUINTO: Emitida propuesta de resolución, a la que se acompañó la relación de documentos para obtención de copia, se propuso al Director de la Agencia la imposición a Nord 3000 Assessors S.L., de una sanción de 60.101, 21 €, por la vulneración del artículo 9 de la LOPD, tipificada como grave en el 44.3.h).

Con fecha 12/08/2008 se remitió copia del expediente, previa petición de la denunciada.

Con fecha 26/08/2008, se formularon alegaciones a la propuesta en la que además de reiterar anteriores argumentos, se matizan los hechos en el sentido de que la caja que contenía los documentos estaba dentro del establecimiento y sería después triturada y entregada al servicio de reciclaje. El lugar en que estaba la caja es de "*acceso privado*", y "*los documentos están vigilados*". Este lugar "*no forma parte del recorrido normal de terceros ajeno a la oficina*", adjuntando copia de un plano en el que figuraban la caja, al lado de una mesa en recepción, frente a la puerta de entrada de la oficina. Se muestra diligencia ya que se interpuso a los pocos días denuncia por sustracción. Resulta por encima del nivel de diligencia exigible el hecho de que alguna persona, de mala fé entre en unas oficinas y sustraiga una caja y esparza luego su contenido, concurriendo cuando menos una ausencia de culpabilidad en NORD 3000. La propuesta no establece ce las medidas que tenían que haber sido adoptadas, solo señala que no se adoptaron mediadas necesarias para evitar los hechos denunciados.

HECHOS PROBADOS

PRIMERO: Con fecha 25/05/2006 una dotación de Policía Local de Terrassa es alertada por personal de Diari de Terrassa de que en un parque de la localidad existe documentación que contiene datos personales esparcida por el suelo (folio 6).

SEGUNDO: La documentación hallada pertenecía a la empresa "*Nord 3000 Assessoria*", de Terrassa (folios 5 y 6).

TERCERO: Entre la documentación hallada como mas relevante figura entre otros: direcciones de correo electrónico, contratos de trabajo con datos identificativos, (folios 9, copias de altas de trabajadores en la Seguridad Social en versión Winsuite (folios 24, 29,45, 56) datos de NIE y nombre y apellidos de empleada de la gestoría (folios 22, 30, 34), nombre y apellidos y dirección de una persona (folio 50, 55), modelo 184 retención socios del IRPF (folio 68), nómina de liquidación y finiquito (folio 93), y otros datos referidos a empresas.

CUARTO: Con fecha el 29/05/2006, el representante de Nord 3000 interpuso denuncia ante la Policía Municipal de la localidad por hurto de una caja que según manifestaba, contenía la documentación hallada en la vía pública, y que sucedió el 25/05/2006 (folio.

QUINTO: La documentación de Nord 3000 Assessors se deposita en la puerta del establecimiento una vez que la misma ha sido destruida (folio 156). La caja cuya documentación fue esparcida en la vía pública, fue dejada al lado de la mesa de recepción, situada frente a la entrada de la oficina (folios 5 y 386), para que fuera recogida por la empresa que el Ayuntamiento tiene para dicho fin. La documentación de la caja se hallaba en dicho lugar, aún no había sido triturada (folios 156 y 380. En la denuncia ante la Policía, formulada por el denunciante el 29/05/2006, este manifiesta que dejó la caja cerca de la puerta de salida de la

oficina, al efecto de que fuera triturada y reciclada (folio 161 y 162). La empresa disponía de dos máquinas destructoras de papel (folio 158).

SEXTO: Los ficheros de Nord 3000 fueron inscritos en la Agencia el 12/06/2006 (folio 150, 287 a 290)

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director 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."

III

El artículo 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" y "pérdida".*

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 *"...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.

Partiendo de tales premisas deben analizarse, a continuación las previsiones que el Real Decreto 994/1998, de 11/06, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personales que se encuentra en vigor a tenor de lo previsto en la disposición transitoria tercera de la LOPD.

El artículo 2.10 del citado Reglamento, considera *"soporte"* al objeto físico susceptible de ser tratado en su sistema de información sobre el cual se pueden gravar o recuperar datos. El precepto no distingue entre soportes informáticos o no, sino que resulta omnicomprensivo de todos ellos en congruencia con los preceptos de la LOPD ya expuestos, que tratan de evitar accesos no autorizados a los datos cualquiera que sea el procedimiento u operación para llevarlo a cabo.

El artículo 4.1 del Reglamento prevé que "*todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico*", reguladas en el Capítulo II del citado Reglamento de medidas de seguridad, artículos 8 a 14 del mismo. En el presente supuesto los datos de carácter personal hallados son datos básicos, entendiendo por tales nombre y apellidos, DNI, domicilio, considerándose de nivel básico.

El artículo 8 de dicho Reglamento de seguridad establece:

"1. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un ***documento de obligado cumplimiento*** *para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.*

2. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
c) Funciones y obligaciones del personal.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

3. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

4. *El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal*".

El artículo 13, determina;

"*1.- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.*

2.- La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada, por el responsable del fichero."

"El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del presente Reglamento, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado."

El artículo 20, incorpora las previsiones específicas que han de aplicarse en la gestión de soportes.

"*1.- Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada*.

2.- Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

3.- Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

4.- Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos."

Sus dos primeros apartados, se refieren específicamente a soportes informáticos, calificativo que no aparece en el apartado 3, debiendo, por ello, acudirse a la definición general de soporte antes citada. Conforme a dicho apartado, *"cuando un soporte vaya a ser desechado... se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en el..."* (el subrayado es de la APD).

En el presente caso, ha quedado acreditado que la Policía Local del Ayuntamiento de Terrassa, constató que el día 25/05/2006, se hallaba en un parque, diferentes tipos de documentación esparcida, pudiendo apreciar el logotipo de la gestoría Nord 3000 Assessors, con quien contactaron y su representante manifestó que una caja de cartón contenía documentación de su empresa, y que la caja fue cogida sin su permiso. La caja se hallaba en el interior, junto a la mesa de reopción, situada frente a la puerta de entrada, sin que se supiera quien la cogió, aunque debió ser alguna persona que entró en dicha Oficina. Los documentos estaban por destruir.

En todo caso, la documentación dejada en la caja, se dejó sin triturar, contrariamente a lo manifestado por Nord 3000 en la Inspección, que en el punto 2.3 señala que "*una vez la documentación ha sido destruida se deposita en la puerta del establecimiento"*. Según los planos que acompañó Nord 3000, se deduce que existe un archivo en el que se guarda la documentación, pero la documentación hallada, se encontraba al lado de un puesto de trabajo, en recepción, frente a la puerta de entrada, y alguien desconocido entró, y se llevó la caja. En tal sentido, se posibilita que sucedan los hechos por cuanto por un lado, no existe una persona en el puesto de trabajo constantemente que se encuentre vigilando la caja, dando lugar a que pudiera suceder que alguien entrara y se la llevara, porque si no, no se debería dejar la caja conteniendo la información que contenía. El deber de custodia vulnerado sucede, por cuanto el lugar no es el dispuesto para almacenar o dejar, ni siquiera momentáneamente los datos personales, existiendo como se señala en el gráfico un archivo en el interior de la Oficina. Por otro lado, pese a que se cumple con la normativa de inscripción de ficheros, este cumplimiento pudo constatarse en la Inspección realizada, pero con fecha de inscripción de los mismos y del documento de seguridad posterior a acontecer los hechos, 12/06/2006. También se debe tener en cuenta que la denuncia, pese a apercibirse el personal el mismo día 25/05/2006 de la desaparición de la caja, no se le debió de dar la importancia necesaria sino hasta cuando se publica la noticia en un medio de comunicación el 27, formulando efectivamente la denuncia el 29.

Los documentos, que fueron hallados en la vía pública, se encuentran en soporte papel, reconociendo Nord 3000 que fueron documentos gestionados por ella misma, y así se desprendió de la Inspección realizada.

La documentación hallada, hacía referencia a copias de diversos documentos, de clientes los que la Asesoría gestiona sus asuntos, encontrándose abundante documentación de personas jurídicas o empresas, y también de personas físicas, sobre todo trabajadores.

Por tal motivo, dicha entidad debió adoptar las medidas de seguridad necesarias para evitar la que los datos de que dispone en formato papel, sean desechados correctamente, y no dando lugar a posibilitar su hallazgo dejándolos en una caja, ya sea al alcance del público, al no

controlar el acceso a su oficina, y por tanto dejándolos al alcance de las personas, ya fuese en la vía pública al alcance de cualquier viandante.

La Audiencia Nacional se ha pronunciado sobre medidas de seguridad en las Sentencias de fecha 7/02/2003 (recurso 1182/2001) y 13/06/2002 (recurso 1517/2001), en el sentido de "*que no basta entonces, con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto. Y por supuesto, no basta con la adopción formal de las* ***medidas de seguridad,*** *pues resulta exigible que aquellas se instauren y pongan en practica de manera efectiva*.", doctrina que se ha reiterado en la reciente Sentencia de 25/01/2006 (recurso 227/04).

En cuanto a las alegaciones efectuadas por NORD de que no se indican las medidas a adoptar o las que se tenían que haber adoptado, estas por un lado, responden por un lado al sentido común e importancia que la documentación de datos personales tiene, por cuanto no es un lugar idóneo colocar estos en una caja cerca de una puerta de entrada, cuando no ha estado custodiada permanentemente, como lo ha sido en este caso, como muestra que alguien desconocido la sustrajera, sin control tampoco en cuanto a las personas que entraban y salían del establecimiento.

Por ello, procede deducir que Nord 3000 ha vulnerado el principio de seguridad en materia de protección de datos, que se encuentra recogidos en el artículo 9 de la LOPD.

IV

El hecho constatado de la difusión de datos personales fuera del ámbito de la entidad Nord 3000, establece la base de facto para fundamentar la imputación de las infracciones de los artículos 9 y 10 de la Ley Orgánica 15/1999.

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 generado por la entidad Nord 3000, en calidad de responsable del fichero, que contiene información sobre datos personales de clientes sale del ámbito de la entidad responsable de su confidencialidad, se está produciendo un incumplimiento de las medidas de seguridad exigidas que, a su vez, deriva en una vulneración del deber de secreto profesional.

Por lo tanto, aplicando el artículo 4.4 del Real Decreto 1398/1993, de 4/08, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora procede subsumir ambas infracciones en una. Dado que, en este caso, ambas infracciones están tipificadas como graves, se considera que procede imputar únicamente la infracción del artículo 9 de la Ley Orgánica 15/1999 como infracción que originariamente implicado la comisión de otra.

V

Señala Nord 3000 que alguna persona que entró en la oficina pudo coger la caja creyendo que contenía otra cosa.

La Agencia española de Protección de Datos ha resuelto numerosos procedimientos sancionadores por infracciones en las medidas de seguridad de otras entidades al haber depositado en la vía pública documentación en la que consta información sobre los datos

personales de sus clientes o trabajadores que obran en sus ficheros. Asimismo las Salas de lo Contencioso Administrativo de la Audiencia Nacional han dictado sentencias en los recursos contenciosos –administrativos interpuestos por las entidades sancionadoras.

Entre ellas, en la Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección Primera, núm. Recurso: 1182/2001, de fecha 7/02/2003, en el Fundamento de Derecho Tercero señala: "*No basta, entonces, con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto. Y, por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Así, de nada sirve que se aprueben unas instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales si luego no se exige a los empleados del banco la observancia de aquellas instrucciones (...) se trataba de documentos de uso interno a los que no debían tener acceso personas ajenas al organigrama de...y si lo tuvieron fue de manera anómala, esto es, por una insuficiencia o deficiente puesta en práctica de las medidas de seguridad."*

En tal sentido, el aartículo 130 de la Ley 30/1992, de 26/11, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC), señala:

"*1 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*"

Aunque en materia sancionadora rige el principio de culpabilidad, la jurisprudencia (Sentencias del Tribunal Supremo de 5/06/1989 y 12/03/1990, entre otras muchas), señala que la expresión simple inobservancia de dicho artículo, permite la imposición de la sanción, sin duda en supuestos dolosos, y asimismo en supuestos culposos, bastando para la imposición de la sanción, la inobservancia del deber de cuidado. Falta de diligencia, que, en el presente supuesto, resulta atribuible a Nord 3000, ya que debería haber extremado el cuidado a fin de no dejar la caja conteniendo datos con documentos que contenía datos de carácter personal en una parte de su oficina de acceso al público, además sin controlar quien pudo cogerla, o en todo caso deberían haberla dejado con los documentos triturados.

El Tribunal Supremo (Sentencias de 05/07/1998 y 02/03/1999) viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el sujeto infractor no se comporta con la diligencia exigible. Diligencia cuyo grado de exigencia se determinará en atención a las circunstancias concurrentes en cada caso, tales como el especial valor del bien jurídico protegido o la profesionalidad exigible al infractor. En este sentido, la citada Sentencia de 05/07/98 exige a los profesionales del sector "*un deber de conocer especialmente las normas aplicables".*

Aplicando la anterior doctrina, la Audiencia Nacional exige a las entidades que operan en el mercado de datos una especial diligencia a la hora de llevar a cabo el uso o tratamiento de tales datos o la cesión a terceros. Y ello porque siendo el de la protección de datos un derecho fundamental (Sentencia del Tribunal Constitucional 292/2000), los depositarios de estos datos deben ser especialmente diligentes y cuidadosos a la hora de operar con ellos y deben optar siempre por la interpretación más favorable a la protección de los bienes jurídicos protegidos por la norma. En este sentido, entre otras, Sentencias de la Audiencia Nacional de fechas 14/02 y 20/09/2002 ,13/04 y 18/05/2005.

Nord 3000 no adoptó las medidas de seguridad de que disponía, dando lugar a que los documentos se hallaran en la vía pública, resultando insuficiente en este supuesto la manifestación de que habitualmente los documentos de la caja estaban triturados, siendo insuficiente la razón que motiva para exculpar su conducta señalando que alguien entró en la oficina, sin que se sepa quien, y se llevó la caja conteniendo la documentación, por cuanto en un establecimiento de atención al público que gestiona asuntos administrativos no se puede dejar a disposición de cualquier persona una caja, sin controlar las personas que entran a la misma, y sin que sirva esa conducta de tercero para aminorar la falta de diligencia en su conducta.

Conforme a este criterio, es evidente que Nord 3000 no actuó con la diligencia debida que le resulta exigible.

VI

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."

En el presente caso, ha quedado acreditada la vulneración en las medidas de seguridad de Nord 3000, conducta que encuentra su tipificación en el citado artículo 44.3.h).

VII

El artículo 45. 2, 4 y 5 de LOPD, establece:

"*2. Las infracciones graves serán sancionadas con multa de 60.101,21 € a 300.506,05 €"*

"4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora."

*"5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate***."**

Nord 3000 solicitó la aplicación el artículo 45.4 y 5 de la LOPD, por cumplir con las medidas de seguridad, tiene los ficheros registrados y el documento de seguridad, no obtuvo beneficio.

La Sentencia de 21/01/2004 de la Audiencia Nacional, en su recurso 1939/2001*, señaló que* dicho precepto <<*…no es sino manifestación del llamado principio de proporcionalidad (artículo 131.1 de la LRJPAC), incluido en el más general del prohibición de exceso, reconocido por la jurisprudencia como principio general del Derecho. Ahora bien, la presente regla debe*

aplicarse con exquisita ponderación y sólo en los casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas, atendidas las circunstancias del caso concreto. Lo cual insistimos puede darse, por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos.

La aplicación con carácter excepcional del citado artículo 45.5 de la LOPD, exige la concurrencia de, al menos**,** uno de los siguientes requisitos: a) Disminución de la culpabilidad del imputado y b) Disminución de la antijuridicidad del hecho.

Por un lado, respecto a la ausencia de beneficios obtenidos, es preciso señalar que, se trata de un criterio de valoración que ha de tenerse en cuenta a tenor del artículo 45.4 de la LOPD.

En este caso, ha quedado acreditado que se inscribieron los ficheros y se dispone de documento de seguridad, los accesos a los sistemas de información se hallaban convenientemente protegidos con claves de acceso, se disponen de diversas destructoras de documentos, y se han tomado medidas como efectuar auditoria de comprobación de ajuste a la LOPD, que suponen que hechos como los sucedidos sean algo más difíciles de reproducirse, dando lugar a una cierta reducción de la antijuridicidad y culpabilidad por haber podido ser producido por un tercero, pudiéndose aplicar el artículo 45.5 de la LOPD.

En cuanto a los criterios de graduación de las sanciones recogidos en el citado artículo 45.4 de la LOPD, y, en especial, a la ausencia de reincidencia y de intencionalidad acreditadas en el presente procedimiento, procede la imposición de la sanción en una cuantía de 6.000 € en función de la cantidad de documentación, que no puede dar lugar al grado mínimo del grado inferior.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: **IMPONER** a la entidad **NORD 3000 ASSESSORS, S.L**., por una infracción del artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de dicha norma, una multa de 6.000 €, de conformidad con el artículo 45.2, 4 y 5 de dicha Ley Orgánica.

SEGUNDO: **NOTIFICAR** la presente resolución a **NORD 3000 ASSESSORS, S.L**. representada por "*Oficina Técnica Jurídica de patentes y Marcas, SUGRAÑES*", (c/…….) y al **AYUNTAMIENTO DE TERRASSA** , con domicilio en Pza. Dido, 5 - 08221 TERRASSA (Barcelona).

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0000 0000 00 0000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la

notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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.

Madrid, 9 de octubre de 2008

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte