



Procedimiento Nº PS/00532/2008

RESOLUCIÓN: R/00432/2009

En el procedimiento sancionador PS/00532/2008, instruido por la Agencia Española de Protección de Datos al **CLUB DEPORTIVO SOCIEDAD DE CAZA SAN ANTON DE ARQUILLOS**, vista la denuncia presentada por el **AYUNTAMIENTO DE OURENSE** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 22 de noviembre de 2007, tiene entrada en esta Agencia un escrito de la Policía Local de Ourense en el que declaran que con fecha 17 de noviembre de 2007, ha sido localizado en Internet, utilizando el programa e-Mule, un fichero denominado "*Sociedad de Caza 2006-2007.mdb*", que contiene datos personales correspondientes a 220 registros relativos a socios cazadores de Arquillos. Adjuntan copia de los citados ficheros, que contienen los datos de conexión así como de las tablas correspondientes donde figura la información.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas de investigación, por los Servicios de Inspección de esta Agencia se realizó visita de Inspección al Club Deportivo Sociedad de Caza San Antón de Arquillos (en lo sucesivo el Club de Caza) levantando Acta de Inspección E/00926/2007-I/1/2007, y se solicitó información a Telefónica España, S.A.U. teniendo conocimiento de los siguientes extremos:

1. La Sociedad de Caza San Antón, se encuentra inscrita en el Registro Andaluz de entidades Deportivas con el número *+*.

2. La documentación mostrada por las inspectoras se corresponde con un fichero de socios que actualmente ya no existe, dicho fichero fue creado por el anterior "Cargo 1" de la Sociedad, en el desarrollo de sus funciones, el mismo se encontraba ubicado en su propio ordenador personal, en el que también se instaló la aplicación que gestionaba el fichero de socios, no obstante, al cesar en sus funciones en el mes de marzo de 2008, los datos fueron borrados, no existiendo en la actualidad, nada más que el formato relativo a la aplicación. Asimismo, manifiesta que en el citado ordenador, ubicado en su domicilio, dejó de utilizarse a mediados del año 2007, y se encontraba instalado el programa de descargas eMule, dado que a pesar de que su domicilio era en ese momento el domicilio social de la Sociedad de Caza, el ordenador era de uso personal.

3. Con fecha 29 de marzo de 2008, el Sr. X.X.X. cesó en su cargo de "Cargo 1", siendo nombrado en esa fecha D. Y.Y.Y., dicho nombramiento consta en el Acta mostrado a las inspectoras, correspondiente a la Asamblea General Extraordinaria



celebrada en esa fecha.

4. El Sr. Y.Y.Y. manifiesta que desde el momento en que él fue nombrado "Cargo 1", únicamente cuenta con documentación en papel, ya que el Sr. X.X.X. no accedió a traspasar la información contenida en los ficheros que existían en su ordenador personal.

5. El Sr. Y.Y.Y. muestra a las inspectoras el Libro de Registro de Socios, verificándose la existencia en el mismo de 227 socios entre los que también se encuentran socios en situación de "Baja". Se realizan comprobaciones de los siguientes números de socios: (.....) verificándose que la información asociada a los mismos coincide con la existente en el fichero referenciado en el apartado 1. Asimismo, se verifica la coincidencia de datos personales asociada a los números de socio: (.....) que aparecen en el fichero de "Bajas", especificado en el apartado 1.

6. Las inspectoras de la Agencia solicitan al Sr. X.X.X. el acceso a su ordenador personal, por lo que el mismo procede a trasladarle desde su domicilio al local donde se realiza la presente inspección, realizándose las siguientes comprobaciones:

a) Se constató que existía una la aplicación instalada en el mismo, comprobándose que existe una base de datos con el nombre: "Sociedad de Caza San Antón 2007-2008" cuyos menús coinciden con los existentes en la aplicación especificada en el apartado 1 de este Acta, no obstante se verifica que al acceder a través de las diferentes opciones de la misma, las tablas existentes se encuentran vacías.

b) No se obtiene constancia de que en el citado ordenador se encuentre instalado el programa de descarga eMule.

7. Se realizan comprobaciones sobre el ordenador instalado en los locales donde se realiza la inspección, comprobándose que no se encuentra instalada la aplicación referenciada, asimismo no se obtiene constancia de la existencia de ningún fichero con información relativa a los socios de la "Sociedad de Caza San Antón".

8. Se ha comprobado mediante consulta realizada a la entidad Telefónica de España, S.A.U que la dirección IP en la que se encontró la Base de Datos (#####), la cual figura en uno de los documentos adjuntos a la denuncia, tenía como titular en el momento de la localización a Dña. Z.Z.Z., domiciliada en (C/.....).

TERCERO: Con fecha 28/10/2008, el Director de la Agencia Española de Protección de Datos acordó iniciar el presente procedimiento sancionador al citado Club de Caza, por la presunta infracción de los artículos 9 y 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificadas como graves en el artículo 44.3.h) y g), respectivamente, de la citada Ley Orgánica.



CUARTO: Notificado el citado acuerdo de inicio, el Club de Caza presenta escrito de alegaciones, comunicando que:

<<...Debo mostrar mi absoluta disconformidad con los hechos que se imputan a la Sociedad que represento en el citado expediente, y ello por cuanto esta Sociedad no ha sido ni es titular de ningún fichero automatizado que contenga datos de carácter personal de quienes integran en calidad de socios el citado club deportivo. Como consta en la relación de hechos que conforma el Acuerdo de inicio del expediente, este Club sólo posee un Libro Registro manuscrito con el nombre y apellidos de los socios que la componen. No tiene, ni ha tenido nunca, ninguna base de datos automatizada ni ninguna aplicación informática donde se registraran datos de sus socios.

En los hechos que dan pie al presente expediente, esta Sociedad no ha tenido la más mínima participación; ni siquiera ha tenido el más mínimo conocimiento respecto a aquellos. El único responsable de la creación de ese fichero informático que según parece el Sr. (...) creó, y luego difundió, es exclusivamente el Sr. (...). Dicho Sr. se valió de su condición de "Cargo 1" y, por ende, de encargado por disposición estatutaria de los libros y Documentación de la Sociedad para, SINCONOCIMIENTO, CONSTANCIA NI AUTORIZACIÓN NI DEL CLUB NI DE SU JUNTA DIRECTIVA, elaborar un fichero automatizado con datos personales de los socios.

En consecuencia, creemos que no procede imponer sanción alguna a esta Sociedad que represento por cuanto nadie de la misma ha realizado conducta alguna susceptible de sanción conforme a la LOPD. Sólo hay un responsable que está perfectamente identificado y que ha actuado a título exclusivamente personal...>>

QUINTO: Con fecha 4/12/2008, se acordó por la Instructora del procedimiento la apertura del período de práctica de pruebas.

SEXTO: El 20 de enero de 2009, se emite propuesta de resolución por la Instructora del procedimiento en el sentido que por el Director de la Agencia Española de Protección de Datos se sancione al Club de Caza con dos multas de 60.101,21 € (sesenta mil ciento un euro con veintinueve céntimos) por las infracciones de los artículos 9 y 10 de la LOPD, tipificadas como graves en el artículo 44.3.h) y 44.3.g) de dicha norma.

SÉPTIMO: Con fecha 23/02/2009, se recibe escrito de el Club de Caza reiterándose en las alegaciones anteriormente manifestadas a lo largo del procedimiento, y solicitando la aplicación del artículo 45.5 de la LOPD.

HECHOS PROBADOS



PRIMERO: Con fecha 22 de noviembre de 2007, tiene entrada en esta Agencia un escrito de la Policía Local de Ourense en el que declaran que con fecha 17 de noviembre de 2007, ha sido localizado en Internet, utilizando el programa e-Mule, un fichero denominado “*Sociedad de Caza 2006-2007.mdb*”, que contiene datos personales correspondientes a 220 registros relativos a socios cazadores de Arquillos (Jaén). Adjuntan copia de los citados ficheros, que contienen los datos de conexión así como de las tablas correspondientes donde figura información sobre los citados socios, entre ellos el dato de sus cuentas bancarias (folios 1 a 33)

SEGUNDO: La Sociedad de Caza San Antón, se encuentra inscrita en el Registro Andaluz de entidades Deportivas con el número ** (folio 35).

TERCERO: La Sociedad de Caza San Antón ha comunicado que la documentación mostrada por las inspectoras se corresponde con un fichero de socios que actualmente ya no existe, dicho fichero fue creado por el anterior “Cargo 1” de la Sociedad, en el desarrollo de sus funciones, el mismo se encontraba ubicado en su propio ordenador personal, en el que también se instaló la aplicación que gestionaba el fichero de socios, no obstante, al cesar en sus funciones en el mes de marzo de 2008, los datos fueron borrados, no existiendo en la actualidad, nada mas que el formato relativo a la aplicación. Asimismo, manifiesta que en el citado ordenador, ubicado en su domicilio, dejó de utilizarse a mediados del año 2007, y se encontraba instalado el programa de descargas eMule, dado que a pesar de que su domicilio era en ese momento el domicilio social de la Sociedad de Caza, el ordenador era de uso personal (folio 35).

CUARTO: Con fecha 29 de marzo de 2008, el Sr. X.X.X. cesó en su cargo de “Cargo 1”, siendo nombrado en esa fecha D. Y.Y.Y., dicho nombramiento consta en el Acta mostrado a las inspectoras, correspondiente a la Asamblea General Extraordinaria celebrada en esa fecha (folio 35).

QUINTO: El Sr. Y.Y.Y. manifiesta que desde el momento en que él fue nombrado “Cargo 1”, únicamente cuenta con documentación en papel, ya que el Sr. X.X.X. no accedió a traspasar la información contenida en los ficheros que existían en su ordenador personal (folio 35).

SEXTO: El Sr. Y.Y.Y. muestra a las inspectoras el Libro de Registro de Socios, verificándose la existencia en el mismo de 227 socios entre los que también se encuentran socios en situación de “Baja”. Se realizan comprobaciones de los siguientes números de socios: (.....) verificándose que la información asociada a los mismos coincide con la existente en el fichero referenciado en el apartado 1. Asimismo, se verifica la coincidencia de datos personales asociada a los números de socio: (.....) que aparecen en el fichero de “Bajas”, especificado en el apartado 1 (folio 35).



SÉPTIMO: Las inspectoras de la Agencia solicitan al Sr. X.X.X. el acceso a su ordenador personal, por lo que el mismo procede a trasladarle desde su domicilio al local donde se realiza la presente inspección, realizándose las siguientes comprobaciones:

a) Se constató que existía una la aplicación instalada en el mismo, comprobándose que existe una base de datos con el nombre: "Sociedad de Caza San Antón 2007-2008" cuyos menús coinciden con los existentes en la aplicación especificada en el apartado 1 de este Acta, no obstante se verifica que al acceder a través de las diferentes opciones de la misma, las tablas existentes se encuentran vacías.

b) No se obtiene constancia de que en el citado ordenador se encuentre instalado el programa de descarga eMule (folios 35 y 36).

OCTAVO: Se realizan comprobaciones sobre el ordenador instalado en los locales donde se realiza la inspección, comprobándose que no se encuentra instalada la aplicación referenciada, asimismo no se obtiene constancia de la existencia de ningún fichero con información relativa a los socios de la "Sociedad de Caza San Antón" (folio 36).

NOVENO: Se ha comprobado mediante consulta realizada a la entidad Telefónica de España, S.A.U que la dirección IP en la que se encontró la Base de Datos (#####), la cual figura en uno de los documentos adjuntos a la denuncia, tenía como titular en el momento de la localización a Dña. Z.Z.Z., domiciliada en (C/.....) (folio 47).

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

Procede en primer lugar, analizar la alegación del Club de Caza, de no ser titular de ningún fichero automatizado que contenga datos de carácter personal.

Los artículos 1 y 2.1 de la LOPD, disponen al regular el *Objeto y Ámbito de aplicación*:



“1. La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento 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.

2.1. 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 público y privado.”

Ha de tenerse en cuenta que el artículo 1 de la LOPD ha ampliado el ámbito de aplicación de la misma en relación con la LORTAD por cuanto garantiza y protege el tratamiento automatizado o no de los datos personales.

El artículo 3.b) de la LOPD, igualmente define:

“b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.”

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 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, señala:

Considerando 15: *“(15) Considerando que los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata;*

Considerando 27 : *“(27) Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva;”*

Artículo 2.c): *“c)“fichero de datos personales” (“fichero”): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;”*



Por otra parte el Considerando 26 de la misma Directiva señala “ *que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicaran a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado*”

III

Entrando en el análisis de las cuestiones de fondo planteadas en el presente procedimiento sancionador, 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 citado 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 aquella, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el “*acceso no autorizado*” por parte de terceros.

Para poder delimitar cuáles son los accesos que la LOPD 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 3 permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente expediente, la “*conservación*” 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 artículo 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 conservación 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 refiere 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 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, que continuaba en vigor en el momento de producirse la infracción, de acuerdo con lo estipulado en la disposición transitoria tercera de la LOPD, previa para garantizar que no se produzcan accesos no autorizados a los ficheros.

El artículo 2.10 del citado Reglamento de Seguridad considera “soporte” al “objeto físico susceptible de ser tratado en su sistema de información sobre el cual se pueden grabar o recuperar datos”. El precepto no distingue entre soportes informáticos o no, sino que resulta omnicomprendido 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 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”.

Así, el Club de Caza estaba obligado a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para los ficheros de la naturaleza indicada, y, entre ellas, las dirigidas a impedir el acceso a los datos contenidos en tales ficheros por parte de terceros. Sin embargo, ha quedado acreditado que incumplió esta obligación.

IV

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”.

De acuerdo con la disposición transitoria tercera de la LOPD, *“hasta tanto se lleven a efecto las previsiones de la Disposición Final Primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo, 1332/1994, de 20 de junio y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley”.*

Dado que ha existido vulneración del *“principio de seguridad de los datos”*, se considera que el Club de Caza ha incurrido en la infracción grave descrita.

V

Asimismo, el presente procedimiento tiene por objeto determinar las responsabilidades que se derivan de la revelación de los datos contenidos en los ficheros del Club de Caza que permanecieron accesibles para terceros a través de la red Internet.

El artículo 10 de la LOPD dispone: *“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.

Este deber de secreto comporta que el responsable de los datos almacenados no pueda 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 o, en su caso, con el responsable del mismo”*. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática, a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30/11, y, por lo que ahora interesa, comporta que los datos tratados no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, 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 Constitución Española. En efecto, este precepto contiene un *“instituto de garantía 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”* (Sentencia del Tribunal Constitucional 292/2000, de 30/11). Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino 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, ha quedado acreditado que, empleando el programa *“eMule”*, se podía acceder sin restricción a través de Internet al fichero, que contienen datos de carácter personal relativos a los socios del Club de Caza.

Por tanto, queda acreditado que por parte del Club de Caza, responsable de la custodia de los datos en cuestión, se vulneró el deber de secreto garantizado en el artículo 10 de la LOPD, al haber posibilitado el acceso no restringido a datos personales sin consentimiento de sus titulares.

VI

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

“La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo”



De acuerdo con los fundamentos anteriores, entendemos que por parte del Club de Caza se ha producido una vulneración del deber de secreto y dado que dichos documentos contienen información, entre otros, a datos bancarios (números de cuentas bancarias) de sus socios, procede calificarla como infracción grave.

VII

No puede ser tenida en cuenta la alegación de falta de culpabilidad por parte del Club de Caza, por cuanto si bien, el principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisibles en el ámbito del Derecho administrativo sancionador una responsabilidad sin culpa. Pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada y a este respecto el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone *“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.”*

El Tribunal Supremo (STS 16/04/91 y STS 22/04/91) considera que del elemento culpabilista se desprende *“que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable.”* El mismo Tribunal razona que *“no basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa”* sino que es preciso *“que se ha empleado la diligencia que era exigible por quien aduce su inexistencia.”* (STS 23/01/98).

A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que *“basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia...”* (SAN 29/06/01).

VIII

Por tanto, de acuerdo con lo señalado en los Fundamentos de Derecho II a VII, ambos inclusive, de esta resolución, ha quedado probado que la difusión de los datos personales de personas físicas que mantienen un vínculo con el imputado, a través de la red, constituía una base fáctica para fundamentar la imputación de las infracciones de los artículos 9 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto, de concurso medial, 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 tercero tiene acceso a un documento que contiene información sobre datos personales de sus clientes, 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 profesional.



Por lo tanto, aplicando el artículo 4.4 del Real Decreto 1398/1993, por el que se aprueba el Reglamento del Procedimiento para el ejercicio de la potestad sancionadora que establece: *“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, ambas infracciones están tipificadas como grave, se considera que procede imputar únicamente la infracción grave del artículo 9 de la LOPD como infracción originaria que ha implicado la comisión de la otra.

IX

El artículo 45.2, 4 y 5 de la 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.”

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.

Dicho artículo, que no es sino la manifestación del llamado principio de proporcionalidad (art. 131 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común), incluido en el más general de prohibición de exceso reconocido por la Jurisprudencia como Principio General del Derecho (Sentencia del Tribunal Constitucional 62/1982), y es consecuencia del valor justicia que informa nuestro Ordenamiento Jurídico (Art. 1 de la Constitución Española), sin embargo debe aplicarse con exquisita ponderación, y sólo en los casos en los que la culpabilidad resulte sustancialmente atenuada atendidas las circunstancias del caso concreto.

En el presente caso, no consta acreditada intencionalidad ni reincidencia en la conducta imputada al Club de Caza, consistente en vulnerar las medidas de seguridad en relación con los datos de carácter personal de sus clientes o personas que



mantienen un vínculo con el mismo, apreciándose una cualificada disminución de la culpabilidad.

Teniendo en cuenta la rapidez para corregir la infracción cometida una vez tuvo conocimiento de la misma, las medidas adoptadas para evitar que se vuelva a producir una nueva infracción, que los hechos denunciados derivan de un error de difícil detección, así como el criterio establecido en la Sentencia de la Audiencia Nacional de fecha 24/03/04, Recurso 445/2002 “...*La diligencia observada por la parte recurrente (...) son circunstancias que no exoneran a la recurrente de responsabilidad cuando, como hemos señalado, se ha realizado la conducta que integre el tipo sancionador. Ahora bien, las citadas circunstancias deben tenerse en cuenta (...) para apreciar la concurrencia de una cualificada disminución de la culpabilidad...*”, por todo ello, procede imponer al Club de Caza una sanción de 6.000 € en aplicación de lo dispuesto en el transcrito artículo 45.5 de la LOPD.

Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: IMPONER al **CLUB DEPORTIVO SOCIEDAD DE CAZA SAN ANTON DE ARQUILLOS**, 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 € (seis mil euros) de conformidad con lo establecido en el artículo 45.2 y 5 de la citada Ley Orgánica.

SEGUNDO: NOTIFICAR la presente resolución al **CLUB DEPORTIVO SOCIEDAD DE CAZA SAN ANTON DE ARQUILLOS** y al **AYUNTAMIENTO DE OURENSE**.

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, 4 de marzo de 2009

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte