



Procedimiento Nº PS/00705/2008

**RESOLUCIÓN: R/01446/2009**

En el procedimiento sancionador PS/00705/2008, instruido por la Agencia Española de Protección de Datos a la entidad **ABANIKO MEDIA, S.L.**, vista la denuncia presentada por **D. R.R.R.** y en base a los siguientes,

**ANTECEDENTES**

**PRIMERO:** Con fecha de 29 de mayo de 2008 tiene entrada en esta Agencia un escrito de D. R.R.R. en el que declara lo siguiente:

*“...que el año pasado participé en el concurso promocional online de la película "7 Mesas de Billar Francés", sito en "http://www....X..../...." donde introduje mis datos personales al inscribirme (nombre completo, login, password, dirección, teléfono, edad y correo electrónico).*

*Tiempo después volví a entrar en dicha página web y ésta redirigió a "http://www....X..../..../links/" donde se listaban una serie de ficheros (listado que adjunto como documento nº 1). En uno de ellos (llamado prueba.php) se mostraba mi dirección de correo, mi login y password, así como el de todos los demás participantes (...)*

*Que a fecha de 28 de Mayo de 2008 este listado sigue disponible para su visualización por cualquier usuario de Internet, sin ningún tipo de control de acceso, y cuenta con aproximadamente 1500 usuarios, correos y contraseñas. Adjunto la impresión de este enlace "http://www....X..../..../linksprueba.php/" como documento nº 2 (mis datos aparecen en la página 23 de dicho documento) (...)*

*Que el password mostrado en esa web (\*\*\*\*\*) es mi contraseña habitual para el acceso a ciertas páginas y cuentas de correo, razón por la cual he tenido que modificar todas ellas, y es muy posible que buena parte de los 1500 usuarios mostrados en ese fichero se encuentren en la misma situación sin saberlo. Estas contraseñas se almacenan en texto claro, sin ningún tipo de seguridad o cifrado (...)*

*Que la web no contaba ni cuenta actualmente con ninguna dirección de contacto para ejercer mi derecho a cancelar, rectificar o modificar los datos personales exhibidos en ese fichero (...)*

*Que el periodo de concurso parece haber terminado pero la web sigue permitiendo inscribirse y no ha destruido mis datos ni los del resto de participantes.”*

**SEGUNDO:** A la vista de los hechos denunciados, en fase de actuaciones previas, por los



Servicios de Inspección de esta Agencia se realiza visita de Inspección a la entidad ABANIKO MEDIA, S.L. (en adelante ABANIKO), levantando Acta de Inspección E1354/2008, el 3 de noviembre de 2008, teniendo conocimiento de que:

a) Se ha comprobado que accediendo en diferentes fechas (23/06/2008, 23/09/2008 y 03/11/2008) por Internet a la URL "<http://www....X.../links/prueba.php>", indicada por el denunciante, se obtiene acceso a la tabla que éste manifiesta y aporta. Dicha tabla expone los siguientes datos: nombre de usuario, contraseña, email y tres campos más denominados "validación", "totaltiradas" y "tiradashechas". La tabla contiene más de 1400 registros.

b) También, se ha comprobado que la página web <http://www....X.../> permite el registro de usuarios al incluir enlaces (*links*) que llevan a formularios de recogida de datos. Se ha realizado una prueba de registro de usuario, completando el proceso de alta de un usuario de nombre "*prueba*".

c) Se ha comprobado asimismo que el dominio [abaniko.net](http://abaniko.net) se encuentra registrado a nombre de D. F.F.F., y el dominio [abaniko.es](http://abaniko.es) por ABANIKO constando como contacto administrativo también D. F.F.F. con email [..2..@..X....](mailto:..2..@..X....). En el sitio web [www...X...](http://www...X...) aparece, en su página principal, únicamente los datos de una entidad: ABANIKO MEDIA, S.L.

d) Realizada el 03/11/2008 una inspección a la entidad ABANIKO sus representantes realizaron las siguientes manifestaciones:

*"ABANIKO es una sociedad constituida en el año 2005 con el siguiente objeto social: creación, diseño y producción audiovisual de publicidad. Así mismo, ofrecen servicios de desarrollo de software, hosting (alojamiento en sus propios sistemas de ficheros, bases de datos y programas de terceras entidades clientes).*

*Entre las promociones realizadas para otras empresas se encuentra la denominada "7mesas", consistente en un juego de billar on-line ofrecido por Internet por su cliente, la productora cinematográfica K.K.K. BC SL (en adelante K.K.K.), con dirección en (C/.....) (o su distribuidora ALTA FILMS).*

*ABANIKO realizó el desarrollo de la aplicación que incluía el registro de los usuarios, el desarrollo del software correspondiente al juego, así como el hosting tanto de los datos con de las aplicaciones, incluyendo en el coste de desarrollo el servicio de posting del fichero de usuarios.*

*En la página web de su cliente K.K.K., durante el proceso de promoción de la película "SIETE MESAS DE BILLAR FRANCES", se incluía un enlace que redirigía a los usuarios a una URL (Dirección de Internet) propia de ABANIKO, donde se encontraba físicamente el programa de juego así como el fichero de usuarios registrados. Una vez finalizada la promoción de la película, aproximadamente en octubre de 2007, en enlace a la URL de ABANIKO fue eliminado.*



*Respecto al fichero que contiene los datos personales de los usuarios registrados en el juego, ABANIKO es únicamente encargado del tratamiento, entendiéndose que es K.K.K. la responsable del fichero.”*

e) Durante la inspección los inspectores de la Agencia solicitaron el acceso a un ordenador dotado de conexión a Internet ubicado en la entidad, efectuando las siguientes comprobaciones:

Se accedió, mediante un navegador de Internet, a la URL: “http://www....X..../...../links”. Se verificó que el navegador mostró una serie de enlaces, entre los que se encuentra “prueba.php”.

Se accedió al enlace “prueba.php”, mostrando el navegador una tabla conteniendo alrededor de 1500 registros con los siguientes campos: usuario, contraseña, email, validación, totaltiradas y tiradashechas.

Los inspectores actuantes indicaron a los representantes de la entidad que habían podido realizar el alta de un nuevo usuario introduciendo como nombre de usuario “prueba” y como contraseña “clave”. Se verificó que dicho usuario aparece reflejado en la tabla.

A la vista de las comprobaciones realizadas por los inspectores, los representantes de la entidad manifestaron que desconocían la existencia de la posibilidad de acceso abierto desde Internet a la tabla de usuarios registrados en el juego “7mesas”, si bien indican que es muy poco probable que un usuario en Internet pueda acceder a dichos datos, al tener que conocer cual es la dirección URL exacta y concreta que permite el acceso a la tabla.

Durante la inspección realizada los inspectores actuantes realizaron las siguientes comprobaciones en el sistema de información utilizado por la entidad para el almacenamiento de los datos de las personas inscritas en el citado juego:

Se extrajo la estructura de la base de datos, verificando que figuran, entre otros, los siguientes campos: “usuario”, “nombre”, “apellidos”, “dirección”, “código postal”, “ciudad”, “teléfono” y “email”.

Se verificó la existencia de 1474 registros en la base de datos.

Se realizó una búsqueda del usuario denominado “prueba”, verificándose que se encontraba incluido en la base de datos.

Se realizó una búsqueda del usuario denominado “harpago”, verificándose también que se encontraba incluido en la base de datos constando contraseña, nombre y apellidos, dirección postal, teléfono y email.

**TERCERO:** Con fecha 16/03/2009, el Director de la Agencia Española de Protección de Datos acordó iniciar el presente procedimiento sancionador a ABANIKO, por las presuntas infracciones 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 grave y leve, respectivamente en el artículo 44.3.h) y 44.2.e), respectivamente, de la citada Ley Orgánica.



**CUARTO:** Notificado el citado acuerdo de inicio, ABANIKO presentó escrito de alegaciones, solicitando la aplicación del artículo 45.5, concurso medial y alegando entre otros:

*<<...se aclaraba, tanto los servicios realizados por la sociedad ABANIKO MEDIA, S.L., como la total dependencia hacia nuestro cliente para la realización de los mismos y la necesaria intervención de otras empresas.*

- a) *Se manifestaba que los servicios realizados era la creación de un juego de billar.*
- b) *Que para poder jugar a dicho juego se debía registrar el usuario, pero no ante ABANIKO MEDIA, S.L., pues la sociedad que represento, se limitó a la elaboración del citado juego, y a nada más.*
- c) *Que para poner dicho juego en la red, se necesitaba un alojamiento, esto es, una empresa de HOSTING, circunstancia que no se da en ABANIKO MEDIA, S.L., por no ser, ni su objeto social, ni su actividad, además de no estar preparada para ello, y que la empresa de HOSTING, era BREONET, y no la sociedad que represento.*
- d) *Que además, para poner el juego en la red, se necesita de otra empresa especializada en ello, pues dicho juego debe de ser programado, que quiere decir, codificación del mismo, pues constituye una necesidad, y que para ello, fue realizado, como no podía ser de otra manera, por una empresa dedicada y especializada en la programación, que en este caso, fue la empresa D4 Imagen y Comunicación, dado que ABANIKO MEDIA, S.L., al igual que con el alojamiento o HOSTING, tampoco desarrolla esas actividades, ni se encuentra preparada para ello.*
- e) *También se manifestó, lo que a su vez nos comunicó las dos empresas anteriormente citadas, y específicamente, la empresa D4 Imagen y Comunicación, nos manifestó, y así lo expuse en el citado escrito, que el tipo de archivo "prueba.php" no disponía de ninguna de las especificaciones que esa empresa utiliza, desconociendo su origen y autoría, pues dicho archivo, para su uso, como lo es el propio juego de billar, debe de ser programado, y por tanto, tenían conocimiento para manifestar si esa programación concreta había sido realizada por ellos o no, manifestándonos que ellos no habían programado dicho archivo. Y en este sentido, como si que manifiesta el Acta de Inspección, nadie de ABANIKO MEDIA, S.L., conocía dicho archivo, precisamente por la sencilla razón de que constituía un archivo sin ninguna función en el programa desarrollado por ABANIKO MEDIA, S.L.*

*En consecuencia, en dicho escrito referido, se aclaraban algunas manifestaciones vertidas en el Acta de Inspección, pues lo que figura en dicha Acta no era correcto:*

*1°.- ABANIKO MEDIA, S.L. no podía, ni puede ofrecer servicios de HOSTING, pues no se dedica a ello. No puede prestar servicios de posicionamiento, pues ello lo realizan otras empresas que nada tienen que ver con la empresa que represento.*



2º.- La URL donde se alojo el juego de 7 Mesas de billar., no es propiedad de ABANIKO MEDIA, S.L., es una empresa dedicada al alojamiento de dominios, (BreoNET), desde donde se redirige al dominio correspondiente, pero esa URL, no es propiedad de ABANIKO MEDIA, S.L.

A modo de recordatorio, manifestar que **URL** significa Uniform Resource Locator, es decir, **localizador uniforme de recurso** y se refiere a la dirección única que identifica a una página web en Internet...>>

<< Tal y como se manifestó en dicho escrito, sólo la pericia de alguien muy especializado podía haber aprovechado algún resquicio de vulnerabilidad en los sistemas (mucho más allá de lo razonable) para introducirse en el dominio con finalidades ilegítimas, y producto de mis averiguaciones he podido comprobar que la persona del denunciante se corresponde con un asiduo de páginas de (...)

Se aporta (...) Algunas páginas extraídas del buscador GOOGLE donde aparece relacionado el nombre de D. R.R.R., acreditativas de la cualificación y preparación en temas informáticos y de redes sociales de la persona que se corresponde con el denunciante...>>

**QUINTO:** Con fecha 25/05/2009 ABANIKO presenta escrito en el que comunica:

*“...No obstante a ello, y entendiendo lo difícil de llegar a concluir el expediente, por las numerosas sociedades intervinientes, desde la responsabilidad que ostento en la representación de ABANIKO MEDIA, S.L., y en aras de no perjudicar a la sociedad que represento, de conformidad al artículo 8 del Real Decreto 1398/1993, vengo a reconocer voluntariamente la responsabilidad de ABANIKO MEDIA, S.L. en los hechos inspeccionados, con el exclusivo fin, de conseguir una resolución lo menos gravosa posible a los intereses que represento, por cuanto la situación económico-financiera y de tesorería de ABANIKO MEDIA, S.L. se encuentran en estos momentos muy delicada, resultando incluso, el mantenimiento de los puestos de trabajo altamente comprometida...”*

**SEXTO:** Al haber reconocido la entidad interesada los hechos que se le imputan, se procede a elevar al Director de la Agencia Española de Protección de Datos el expediente a los efectos de dictar resolución al respecto.

## **HECHOS PROBADOS**

**PRIMERO:** Con fecha de 29 de mayo de 2008 tiene entrada en esta Agencia un escrito de D. R.R.R. comunicando:



*“...que el año pasado participé en el concurso promocional online de la película “7 Mesas de Billar Francés”, sito en “http://www....X.../....” donde introduje mis datos personales al inscribirme (nombre completo, login, password, dirección, teléfono, edad y correo electrónico).*

*Tiempo después volví a entrar en dicha página web y ésta redirigió a “http://www....X.../..../links” donde se listaban una serie de ficheros (listado que adjunto como documento n° 1). En uno de ellos (llamado prueba.php) se mostraba mi dirección de correo, mi login y password, así como el de todos los demás participantes (...)*

*Que a fecha de 28 de Mayo de 2008 este listado sigue disponible para su visualización por cualquier usuario de Internet, sin ningún tipo de control de acceso, y cuenta con aproximadamente 1500 usuarios, correos y contraseñas. Adjunto la impresión de este enlace “http://www....X.../..../linksprueba.php/” como documento n° 2 (mis datos aparecen en la página 23 de dicho documento) (...)*

*Que el periodo de concurso parece haber terminado pero la web sigue permitiendo inscribirse y no ha destruido mis datos ni los del resto de participantes” (folios 1 a 36).*

**SEGUNDO:** Se ha comprobado por esta Agencia que accediendo en diferentes fechas (23/06/2008, 23/09/2008 y 03/11/2008) por Internet a la URL “http://www....X.../..../links/prueba.php”, indicada por el denunciante, se obtiene acceso a la tabla que éste manifiesta y aporta. Dicha tabla expone los siguientes datos: nombre de usuario, contraseña, email y tres campos más denominados “validación”, “*totaltiradas*” y “*tiradashechas*”. La tabla contiene más de 1400 registros (folios 38 a 83).

**TERCERO:** También, se ha comprobado que la página web http://www....X.../..../ permite el registro de usuarios al incluir enlaces (*links*) que llevan a formularios de recogida de datos. Se ha realizado una prueba de registro de usuario, completando el proceso de alta de un usuario de nombre “*prueba*” (folios 84 a 85)

**CUARTO:** El dominio abaniko.net se encuentra registrado a nombre de D. F.F.F., y el dominio abaniko.es por ABANIKO constando como contacto administrativo también D. F.F.F. con email ...2..@..X..... En el sitio web www...X... aparece, en su página principal, únicamente los datos de una entidad: ABANIKO MEDIA, S.L. (folios 99 a 102).

**QUINTO:** ABANIKO ha manifestado que:

*<<...ABANIKO es una sociedad constituida en el año 2005 con el siguiente objeto social: creación, diseño y producción audiovisual de publicidad (...)*

*Entre las promociones realizadas para otras empresas se encuentra la denominada “7mesas”, consistente en un juego de billar on-line ofrecido por Internet por su cliente, la productora cinematográfica K.K.K. BC SL (...)*



*En la página web de su cliente K.K.K., durante el proceso de promoción de la película “SIETE MESAS DE BILLAR FRANCES”, se incluía un enlace que redirigía a los usuarios a una URL (Dirección de Internet) propia de ABANIKO, donde se encontraba físicamente el programa de juego así como el fichero de usuarios registrados. Una vez finalizada la promoción de la película, aproximadamente en octubre de 2007, en enlace a la URL de ABANIKO fue eliminado (...)>>*

Que desconocían la existencia de la posibilidad de acceso abierto desde Internet a la tabla de usuarios registrados en el juego “7mesas”, si bien indican que es muy poco probable que un usuario en Internet pueda acceder a dichos datos, al tener que conocer cual es la dirección URL exacta y concreta que permite el acceso a la tabla (folios 86 a 88).

*<<...Que para poner dicho juego en la red, se necesitaba un alojamiento, esto es, una empresa de HOSTING, circunstancia que no se da en ABANIKO MEDIA, S.L., por no ser, ni su objeto social, ni su actividad, además de no estar preparada para ello, y que la empresa de HOSTING, era BREONET, y no la sociedad que represento.*

*Que además, para poner el juego en la red, se necesita de otra empresa especializada en ello, pues dicho juego debe de ser programado, que quiere decir, codificación del mismo, pues constituye una necesidad, y que para ello, fue realizado, como no podía ser de otra manera, por una empresa dedicada y especializada en la programación, que en este caso, fue la empresa D4 Imagen y Comunicación, dado que ABANIKO MEDIA, S.L., al igual que con el alojamiento o HOSTING, tampoco desarrolla esas actividades, ni se encuentra preparada para ello...>> (folios 152).*

## **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 8.1 del Real Decreto 1398/93, de 4 de agosto, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora, dispone:

*“Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento, con la imposición de la sanción que proceda.”*

En aplicación del anterior precepto y teniendo en cuenta que ABANIKO ha reconocido los hechos imputados, procede resolver el procedimiento iniciado.



### III

La LOPD en sus art. 1 y 2.1) establece:

*“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.”*

*“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.”*

### IV

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 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, vigente desde el 20 de abril de 2008 y aplicable al presente procedimiento, por cuanto los hechos probados del mismo constituyen una infracción continuada, como mínimo hasta el 23/09/2008, fecha en la que desde la Inspección de esta Agencia, se accedió al fichero de la entidad ABANIKO.

El artículo 88 de dicho citado Real Decreto establece al regular el *documento de seguridad*:

*<<1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.*

*2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.*



3. *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 de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.*

c) *Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.*

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 en los ficheros o tratamientos automatizados.*

g) *Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.*

4. *En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:*

a) *La identificación del responsable o responsables de seguridad.*

b) *Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.*

5. *Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.*

6. *En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlos en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.*

*En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.*

7. *El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como*



consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

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

Asimismo los artículos 91 y 93 del citado Real Decreto, establecen al regular el Control de acceso, la Identificación y autenticación:

<<1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. *El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.*

3. *El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.*

4. *Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.*

5. *En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.>>*

<<1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. *El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.*

3. *Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.*

4. *El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.>>*

Así, ABANIKO estaba obligada 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.



## V

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 vulneración del *“principio de seguridad de los datos”*, se considera que ABANIKO ha incurrido en la infracción grave descrita.

## VI

La LOPD delimita su ámbito de aplicación en el párrafo primero de su artículo 2.1, indicando que *“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”.*

Definiendo el concepto de dato de carácter personal en su artículo 3.a) como *“cualquier información concerniente a personas físicas identificadas o identificables”.*

El tratamiento de datos se define en la letra c) del mismo precepto como las *“Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”.*

A la vista de lo anterior, se deduce que la dirección de correo electrónico, considerando que contiene información acerca de su titular, o en la medida en que permita proceder a la identificación del mismo, ha de ser considerada como dato de carácter personal y su tratamiento sometido a la citada Ley Orgánica, por lo que, con carácter general, no será posible su utilización o cesión si el interesado no ha dado su consentimiento para ello.

La dirección de correo electrónico se forma por un conjunto de signos o palabras libremente elegidos, generalmente por su titular, con la única limitación de que dicha dirección no coincida con la correspondiente a otra persona. Esta combinación podrá tener significado en sí misma o carecer del mismo, atendiendo al grado de identificación del titular de la cuenta de correo que proporcione la dirección de que se trate. Así, existirán supuestos en los que voluntaria o involuntariamente la dirección de correo electrónico contenga información acerca de su titular que lo identifique, en los cuales no existe duda de que dicha dirección ha de ser considerada como dato de carácter personal, o supuestos en los que la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta, de modo que no nos encontramos ante un dato de carácter personal, a no ser que otros datos (dominio, domicilio, etc.), conjunta o separadamente, permitan, como en el presente supuesto, la identificación del sujeto sin un esfuerzo desproporcionado por parte de quien procede a la identificación, en



cuyo caso, la dirección de correo electrónico quedará amparada por el régimen establecido en la LOPD.

## VII

Asimismo, el presente procedimiento tiene por objeto determinar las responsabilidades que se derivan de la revelación de los datos contenidos en los ficheros de ABANIKO, 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 actividad no querida.

En el caso que nos ocupa, ha quedado acreditado que, se accedía libremente a través de Internet a los datos de usuario, contraseña y dirección de correo electrónico (email) de los participantes en el juego de promoción de la película de 7 Mesas de Billar Francés, desde <http://www....X..../links/>.

Por tanto, queda acreditado que por parte de ABANIKO, 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.

## VIII

La LOPD califica como infracción leve, grave o muy grave la infracción del artículo 10 de la citada norma, dependiendo del contenido de la información que ha sido indebidamente facilitada a terceros.

El incumplimiento del deber de guardar secreto establecido en el citado artículo 10 de la LOPD constituye, por regla general, una infracción leve tipificada en el artículo 44.2.e) como: *“Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave”*.

En el presente caso, teniendo en cuenta los datos recogidos en el citado fichero: usuario, contraseña y email (dirección de correo electrónico), ha de calificarse la vulneración del artículo 10 por parte de ABANIKO como infracción leve.

## IX

No puede ser tenida en cuenta la alegación de falta de culpabilidad por parte de ABANIKO, 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).



## X

La Agencia Española de Protección de Datos ha resuelto numerosos procedimientos sancionadores por infracciones en las medidas de seguridad al haber permitido diversas entidades, el acceso a través de Internet a la información de los datos personales y bancarios de sus clientes que obra en sus ficheros. Asimismo la Sala 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: 290/2004, de fecha 28 de junio de 2006, en el Fundamento de Derecho Cuarto señala: *“Esta misma Sala, resolviendo supuestos anteriores en los que los hechos se tipificaron a tenor de dicho Artículo 9 de la Ley Orgánica 15/1999, de Protección de Datos, ha establecido la siguiente doctrina (sentencias de 13 de junio de 2002, Reo. 1161/2001, y de 7 de febrero de 2003, Reo. 1182/2003, entre otras):*

*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 impone, en consecuencia, una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva y como manifiesta el Abogado del Estado en la contestación, la recurrente es, por disposición legal, una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues también es responsable de que las mismas se cumplan y se ejecuten con rigor. En definitiva toda responsable de un fichero (o encargada de tratamiento) debe asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica sin que, bajo ningún concepto, datos bancarios o cualesquiera otros datos de carácter personal puedan llegar a manos de terceras personas.*

*En definitiva, y puesto que XXX es una deudora de seguridad en materia de datos, debe por tanto dar una explicación adecuada y razonable de cómo los datos personales de sus clientes se hallaban a disposición y se podían encontrar por el afectado (en el lapso temporal en que aconteció el incidente) al acceder éste a la información telemática de sus - datos bancarios, siendo insuficiente, según se desprende de la doctrina de la Sala que se acaba de exponer, con acreditar que se adoptaron una serie de medidas, pues dicha entidad bancaria también es responsable de que las mismas se cumplan y ejecuten con rigor.”*

## XI



Por tanto, de acuerdo con lo señalado en los Fundamentos de Derecho III a X, ambos inclusive, de esta resolución ha quedado probado que la difusión de los datos personales de los clientes del 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, una está tipificada como infracción leve y otra 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.

## XII

El artículo 45.2, 4 y 5 de la LOPD, establece:

*“2. Las infracciones graves serán sancionadas con multa de 60.101,21 euros a 300.506,05 euros.”*

*“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. En el presente caso, teniendo en cuenta que ABANIKO no es una empresa vinculada directamente al



marco de las nuevas tecnologías de la información, es por ello, que no cabe atribuirle un grado de culpabilidad en la no adopción de sus medidas de seguridad equivalente en supuestos como el presente vinculados a profundos conocimientos técnicos. Por otro lado, a la vista de las medias adoptadas, y la rapidez con la que se atajó la incidencia, aplicando especial diligencia en la adopción de una amplia serie de medidas correctoras, es posible apreciar la concurrencia de disminución de la culpabilidad y procede imponer la sanción en su cuantía de 6000 €.

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 **ABANIKO MEDIA, 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 € (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 a **ABANIKO MEDIA, S.L.** y a **D. R.R.R..**

**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 000000000 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, 17 de junio de 2009

EL DIRECTOR DE LA AGENCIA ESPAÑOLA  
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte