

## **AUDIENCIA NACIONAL**

**Sentencia de fecha: 28 de junio de 2006**

Ponente: Ilma. Magistrada doña Nieves Buisán García

### **Incidencia de seguridad. Información bancaria disponible en Internet.**

La medida de seguridad estaba establecida y vigente, si bien por causa ajenas a la voluntad e interés del Banco falló, corrigiéndose en el plazo de 20 minutos desde que se advirtió. La incidencia tampoco permitió a personas que no fueran clientes del banco acceder al sistema, sino que exclusivamente se limitó a que algunos clientes recibieron información relativa a las cuentas de otros clientes. Es decir, no afectaba a las barreras de acceso al sistema, sino al reparto de información. No obstante, la Sala considera que la entidad (por su actividad) es una deudora de seguridad en materia de datos, y 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, 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.

## **SENTENCIA**

Madrid, a veintiocho de junio de dos mil seis.

La Sala constituida por los Sres. Magistrados relacionados al margen ha visto el recurso contencioso-administrativo número 290/2004, interpuesto por PATAGON INTERNET BANK, S.L. (PATAGON), representado por la procuradora Dña. Cristina Deza García, contra la Agencia de Protección de Datos de 28 de abril de 2004, que impone a la entidad Patagon Bank SA una multa de 6.101,21 euros. Ha sido parte demandada en las presentes actuaciones la Administración General del Estado, representada por la Abogacía del Estado.

## **ANTECEDENTES DE HECHO**

PRIMERO.- Por la entidad recurrente se interpuso recurso contencioso administrativo mediante escrito presentado el 17 de mayo de 2004, acordándose por providencia de 21 de mayo siguiente su tramitación de conformidad con las normas establecidas en la Ley 29/98 , y la reclamación del expediente administrativo.

SEGUNDO.- En el momento procesal oportuno tal parte actora formalizó la demanda mediante escrito presentado el 13 de julio de 2004, en el que, tras alegar los hechos y fundamentos de derecho que estimó procedentes, terminó suplicando se dictara sentencia en la que, estimándose la demanda, se declarara:

1. La preclusión de las actuaciones previas y la nulidad de la prueba aportada al expediente sancionador; o bien
2. La nulidad de la sanción impugnada.

TERCERO.- El Sr. Abogado del Estado contestó la demanda mediante escrito presentado el 29 de octubre de 2004, en el que, tras alegar los hechos y los fundamentos jurídicos que estimó aplicables, terminó suplicando se dictara sentencia en la que se desestimara el recurso y se confirmara la resolución administrativa impugnada por ser conforme a Derecho, con imposición de costas a tal parte recurrente.

CUARTO.- No habiéndose solicitado el recibimiento a prueba, y no considerándose necesaria la celebración de vista pública, se dio trámite de conclusiones a las partes, trámite que evacuaron por su orden, primero la defensa de la entidad actora y después el Abogado del Estado, mediante escritos en los que concretaron y reiteraron sus respectivos pedimentos.

QUINTO.- Concluidas las actuaciones, se señaló para votación y fallo del recurso el día 27 de junio de 2006, fecha en la que tuvo lugar la deliberación y votación, habiendo sido ponente la Ilma. Magistrada doña Nieves Buisán García, quien expresa el parecer de la Sala.

## **FUNDAMENTOS DE DERECHO**

PRIMERO.- Se impugna en el presente recurso contencioso-administrativo la resolución de la Agencia de Protección de Datos de 28 de abril de 2004, que impone a la entidad Patagon Bank SA una multa de 6.101,21 euros por la comisión de una infracción del artículo 9 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), tipificada como grave en el artículo 44.3.h) de dicha norma, de conformidad con lo establecido en el artículo 45.2 de la citada Ley Orgánica.

Tal resolución combatida declara como hechos probados los siguientes:

PRIMERO. El proceso de generación de documentos de la entidad Patagón para su envío a impresión (formato papel) e Internet, separa los documentos en dos ficheros: uno para el correo postal y otro para Internet. En el fichero de Internet se incluye una marca que contiene una clave para que dichos documentos estén relacionados con la cuenta y los intervinientes a los que pertenecen.

SEGUNDO. El día 28 de marzo de 2003 se implementó una nueva versión del sistema en el cual se modificó la forma de dividir los datos entre Internet y el correo postal. Esta implementación dio lugar a la inclusión de los datos del correo postal en el fichero de Internet, por lo que los documentos cargados en Internet contenían información de terceros no relacionados con dichas cuentas.

TERCERO. Esta información estuvo disponible en Internet el día 28 de marzo de 2003 desde las 12:18 horas hasta las 14:10 horas, en la que tuvo lugar la desactivación de dicha información tras la llamada telefónica de un cliente a las 13:49 en la que comunicó la detección del error.

CUARTO. El día 28 de marzo de 2003 D. Millán, al acceder a su información bancaria a través de Internet remitida por Patagón, pudo comprobar que además de su información bancaria aparecían informaciones de otros clientes y cuentas que no se correspondían con el afectado.

SEGUNDO. La parte actora sustenta su pretensión impugnatoria de la demanda en síntesis, en las siguientes consideraciones:

Preclusión del plazo para acordar el inicio del expediente, porque desde la fecha en que se practicó la Inspección, el 9 de junio de 2003, y hasta la que se notificó el acuerdo de inicio del expediente sancionador, el 10 de noviembre de 2003, transcurrió con creces el plazo de dos meses del Art. 6.2 del RD 1389/1993. No puede aceptarse la interpretación de la Administración porque "inicio del expediente" se refiere a inicio material de las actuaciones que forman o formaran parte del expediente, esto es, a la ejecución de actuaciones previas.

Inexistencia de la infracción imputada, pues la incidencia no ocurrió porque Patagón no cumpliera con las medidas de seguridad, sino que se debió a una fatalidad, a la mera concurrencia de una incidencia en un sistema que tiene implementadas las medidas de seguridad. No se ha incumplido el artículo 18 del Reglamento de Medidas de Seguridad pues mediante el sistema implementado por Patagón se garantiza la identificación inequívoca y personalizada de los usuarios con acceso al sistema. Así se desprende de los documentos 1,2 y 3 que acompañan a la demanda, que demuestran que dicha actora tiene establecido un control de acceso a su sistema informático que sólo permite tal acceso a los clientes que se identifican y autentifican su identidad, y que bloquea la posibilidad de acceder en el caso de que se sucedan tres intentos fallidos de acceso.

La medida de seguridad estaba establecida y vigente, si bien por causa ajenas a la voluntad e interés del Banco falló, corrigiéndose en el plazo de 20 minutos desde que se advirtió. Además, tal incidencia tampoco permitió a personas que no fueran clientes del banco acceder al sistema, sino que exclusivamente se limitó a que algunos clientes recibieron información relativa a las cuentas de otros clientes. Es decir, no afectaba a las barreras de acceso al sistema, sino al reparto de información.

TERCERO. Ha de ser resuelta, en primer término, la objeción de carácter formal invocada en la demanda consistente en la preclusión del plazo de dos meses que para acordar el inicio del expediente deriva del Art. 6.2 del Reglamento del procedimiento para el ejercicio de la potestad sancionadora, aprobado por RD 1389/1993, de 4 de agosto, dado que tal plazo, según la recurrente, ha de computarse desde la fecha en que se practicó la Inspección, el 9 de junio de 2003, y hasta la que se notificó el acuerdo de inicio del expediente sancionador, el 10 de noviembre de 2003.

Es esta una cuestión que ha sido ya resuelta en nuestra anterior sentencia de 2 de febrero de 2002, dictada en el Rec. 1260/2000, en la que expusimos lo siguiente:

El plazo de dos meses previsto en el artículo 6.2 del expresado Reglamento, para acordar el archivo de las actuaciones si no se hubiera notificado al imputado el inicio del procedimiento, comienza precisamente desde el inicio del procedimiento administrativo. Esta es la conclusión que se infiere del tenor literal de este precepto, que coincide con su interpretación sistemática, pues efectivamente el citado Reglamento regula la posibilidad de realizar actuaciones previas anteriores a la iniciación del procedimiento (artículo 12 del Reglamento de tanta cita), y con una interpretación lógica, toda vez que debe determinarse con carácter preliminar si concurren o no las circunstancias que justifiquen la iniciación del procedimiento.

Así, aplicando dicha interpretación al supuesto de autos, tenemos que como la fecha del Acuerdo de inicio del procedimiento sancionador es la de 5 de noviembre de 2003 (folio 29 del expediente administrativo) y la fecha de notificación de dicho Acuerdo la de 10 de noviembre siguiente, de ningún modo puede considerarse que haya transcurrido el plazo de dos meses a cuyo incumplimiento el citado artículo 6 del Reglamento anuda el archivo de las actuaciones, por lo que la nulidad pretendida en tal demanda por tal causa, ha de ser rechazada.

CUARTO. En cuanto al fondo de la controversia, la infracción imputada a Patagón Bank SA es la del Artículo 9 LOPD, que se expresa en los siguientes términos:

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.

Tal precepto ha de ponerse en relación, en el presente caso, con lo preceptuado en el Art. 18 del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad, a cuyo tenor: "El responsable del fichero 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. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información".

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, Rec. 1161/2001, y de 7 de febrero de 2003, Rec. 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 Patagon SA 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.

La argumentación de la actora de que tal incidencia, y en definitiva la exposición telemática de los datos bancarios de terceros clientes, sólo se produjo respecto de otros clientes suyos, y no respecto al público en general, lo cual exime de responsabilidad a la misma, nos conduciría al absurdo de que cualquier cliente del banco, una vez accedido al sistema general del mismo, podría acceder a la información bancaria de otros clientes, sin que ello fuese sancionable.

Se desprende, por tanto, de lo hasta aquí razonado, y sin necesidad de mayores consideraciones que la infracción grave del Art. 44.3.h) de la normativa sobre protección de datos impuesta a Patagón ("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") ha de ser confirmada por la Sala.

Y si bien es cierto que, como asimismo reitera la demanda, la situación anómala se mantuvo durante un breve espacio de tiempo, desde las 12.18 horas hasta las 14:10 horas del día 28 de marzo, corrigiéndose con rapidez la deficiencia. Tal circunstancia no evitó el acceso no autorizado a cuentas ajenas, pero sin embargo sí se tuvo en cuenta por la Agencia de Protección de Datos a fin de rebajar en grado la sanción, por lo que dicha sanción de 6.010,21 euros ha de ser asimismo confirmada por esta Sala.

QUINTO.- Razones las anteriores que conducen a la desestimación del recurso, sin que concurren las causas expresadas en el Art. 139 de la Ley de la Jurisdicción contencioso-administrativa para la imposición de las costas a ninguna de las partes.

## **FALLAMOS**

Que desestimando el recurso contencioso administrativo interpuesto por la representación procesal de Patagón Internet Bank SA contra la resolución del Director de la Agencia de Protección de Datos de 28 de abril de 2004 que impone a la recurrente una sanción de 6.010,21 euros, confirmamos dicha resolución, dada su conformidad a Derecho, sin imposición de costas a ninguna de las partes.

Así por esta nuestra sentencia, lo pronunciamos, mandamos y firmamos

PUBLICACIÓN.- Dada, leída y publicada fue la anterior sentencia en audiencia pública. Doy fe. Madrid a