Procedimiento nº.: PS/00185/2015

ASUNTO: Recurso de Reposición Nº RR/00861/2015

Examinado el recurso de reposición interpuesto por la entidad BANKIA, S.A. contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00185/2015, y en virtud de los siguientes,

HECHOS

PRIMERO: Con fecha 24 de septiembre de 2015, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00185/2015, en virtud de la cual se imponía a la entidad BANKIA, S.A., una sanción de 6.000 €, por la vulneración de lo dispuesto en el artículo 9.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), infracción tipificada como grave en el artículo 44.3.h), de conformidad con lo establecido en el artículo 45.1.2.4 y .5 de la citada Ley Orgánica.

Dicha resolución, que fue notificada al recurrente en fecha 28 de septiembre de 2015, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en el artículo 127 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00185/2015, quedó constancia de los siguientes:

*<<PRIMERO: Con fecha de 15 de abril de 2014 tiene entrada en esta Agencia un escrito en el que se declara que junto a una papelera de basura en el suelo en la calle del Puente en Benidorm, cerca de la oficina de Bankia nº *****, se ha encontrado documentación conteniendo datos de carácter personal de sus clientes. Aporta copia de la documentación encontrada que consiste en:*

- *Tres cartas de remisión de tarjetas de crédito a clientes de BANKIA fechadas entre el 25 de enero y el 18 de febrero de 2014.*
- *Impresión de pantalla del proceso de alta de aportación de fondos de una clienta identificada con nombre y apellidos. Aparece fechada el 14/2/2014 y se aprecia que la sucursal de las cuentas es la *****.*
- *Comprobante de transferencia de fecha 27/2/2014 de la oficina *****, figurando como ordenante y beneficiario un cliente identificado con nombre y apellidos.*
- *Test de conveniencia de fondos de inversión de una clienta identificada con nombre y apellidos, fechado el 26/2/2014. Dicho documento expone datos como la formación, experiencia profesional y conocimientos financieros de dicha persona.*
- *Documento de mantenimiento de canales y medios de pago, a nombre de un cliente identificado con nombre y apellidos, fechado el 27/2/2014.*
- *Correo electrónico de fecha 26/2/2014 remitido desde Dirección Levante a Oficina*

***** con el asunto "Extracto de cuenta en cuentas. Gestor Morosidad." en el que aparece una relación de cinco personas, de las que aparecen sus nombres, documento identificativo (DNI, pasaporte o tarjeta de residente), número de cuenta, su situación de descubierto o de posible fallido o su situación de parado.*

- *Correo electrónico de fecha 19/2/2014 en el que figuran nombre y apellidos de remitentes y destinatarios, con destino a Oficina *****. El asunto de dicho correo es "REQUERIMIENTO DE INFORMACIÓN A.E.A.T. (Comunicados por vía electrónica dirigidos a la oficina)". En dicho correo se solicita el extracto de las cuentas corrientes de las que un cliente, identificado con nombre y apellidos y NIF, figura como titular o autorizado.*

SEGUNDO: Solicitada información a la entidad Bankia sobre los hechos denunciados, aporta el Documento de Seguridad Maestro y el anexo sobre Medidas de Seguridad Soporte Papel, la Circular sobre Política General y Normativa General de Seguridad de la Información, publicada en la Intranet de la entidad y aporta captura de la normativa LOPD publicada en intranet a la que tienen acceso todos los empleados de la entidad.

*TERCERO: Con respecto a los certificados de destrucción y las copias de albaranes de entrega correspondientes a la oficina ***** en el período indicado, aporta la entidad copia del contrato firmado con la empresa de retirada y destrucción de documentación vigente durante el primer trimestre de 2014 e informa que se está implantando un procedimiento por el cual cada oficina cuenta con una "Saca Roja" donde depositar la documentación confidencial a destruir.*

Aporta la entidad detalle del procedimiento establecido en el Manual Operativo de Archivo y Documentación Histórica.

Informa de que cuenta con certificados globales de todo el papel confidencial destruido en un mes.

*Aporta BANKIA detalle de las cinco solicitudes de retirada de documentación realizadas por la Oficina ***** en fechas comprendidas entre el 17 de enero y el 8 de abril de 2014.>>*

TERCERO: La entidad BANKIA, S.A. ha presentado en fecha 28 de octubre de 2015, en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo, básicamente, en que se reitera en las alegaciones ya presentadas a lo largo del procedimiento y solicitando que:

"…*proceda a la anulación de la Resolución de 24 de septiembre de 2015 dejándola sin efecto, por entender que la misma es contraria a Derecho y, en consecuencia, no imponga mayor sanción a esta entidad que la correspondiente a las infracciones leves en su grado mínimo, esto es, por un importe no superior a 900 euros, pues la sanción ahora impuesta a BANKIA de 6.000 euros es, a todas luces, desproporcionada ya que además de las circunstancias atenuantes de la graduación de la sanción, la AEPD debiera haber tomado en consideración las circunstancias recogidas en artículo 45.4 de la LOPO, con especial mención a la letra e) de dicho artículo.*

Subsidiariamente, de no tener en cuenta lo anterior, solicita esta parte a la AEPD que

rebaje considerablemente la sanción impuesta en la Resolución de 24 de septiembre de 2015, todo ello en aplicación del principio de proporcionalidad previsto en el artículo 131 de la LRJPAC."

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto 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 (en lo sucesivo LRJPAC).

II

En relación con las manifestaciones efectuadas por la entidad BANKIA, S.A., reiterándose básicamente, en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho del II al VII ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

<<II

El artículo 9 de la LOPD, dispone:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

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

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar

exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de "fichero" y "tratamiento" contenidas en la LOPD.

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

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

Para completar el sistema de protección en lo que a la seguridad afecta, el art. 44.3.h) de la LOPD tipifica como infracción grave el "mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

Es necesario analizar las previsiones que el R. D. 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, prevé para garantizar que no se produzcan accesos no autorizados a los ficheros.

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

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

Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104.

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

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

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

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

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

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

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

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

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

*La entidad BANKIA, debió, adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información que contenían dichos documentos. Tales medidas no fueron adoptadas totalmente en el presente caso. Prueba de ello es el hecho de que la documentación fue encontrada por el denunciante en la calle el Puente de Benidorm en el suelo junto a una papelera de basura, cerca de la oficina ***** de Bankia.*

BANKIA ha alegado al acuerdo de inicio del procedimiento sancionador que dispone de Documento de Seguridad con un anexo sobre Medidas de Seguridad Soporte Papel. Aporta constancia de que cuenta con la Circular sobre Política General y Normativa General de Seguridad de la Información, publicada en su Intranet y aporta la normativa LOPD publicada en la intranet a la que tienen acceso todos los empleados de

la entidad. Informa también del contrato firmado con una empresa para la retirada y destrucción de documentación y del procedimiento que se sigue para la destrucción de documentación confidencial.

La Audiencia Nacional, en sus sentencias de 13 de junio de 2002 y de 7 de febrero de 2003, entre otras, ha establecido que: "No basta, entonces, con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto. Y, por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva ...".

La necesidad de especial diligencia en la custodia de la documentación ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: "Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…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 es también responsable de que las mismas se cumplan y se ejecuten con rigor"

Por todo esto no pueden estimarse las manifestaciones de la entidad denunciada relativas a que se tenían implantadas unas medidas de seguridad, porque éstas no fueron suficientes para impedir la recuperación posterior de la información por un tercero no autorizado.

Alega la entidad denunciada a la propuesta de resolución que no resulta acreditado que Bankia, sus empleados o sus prestadores de servicios abandonaran documentación alguna en la vía pública ni que fueran negligentes en la custodia de la documentación aportada por el denunciante y ello porque cualquier ciudadano podría acusarles de haber encontrado una documentación sin que se contemple la existencia de una duda razonable sobre la posible sustracción y obtención de la misma por alguna otra vía.

Esta alegación no puede ser tenida en cuenta, dado que, si bien el principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisible en el ámbito del Derecho administrativo sancionador una responsabilidad sin culpa, este 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 de 16 de abril de 1991 y STS de 22 de abril de 1991) considera que del elemento de culpabilidad 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 de 23 de enero de 1998).

A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que "Sobre la falta de culpabilidad, ha de decirse que generalmente este tipo de conductas no tienen un componente doloso, y la mayoría de ellas se producen sin malicia o intencionalidad. Basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros (...) lo que denota una falta evidente en la observancia de esos deberes que conculcan claramente los principios y garantías establecidas en la Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento de Datos de Carácter Personal..." (SAN de 29 de junio de 2001).

En el presente caso la prueba de la infracción cometida es el hecho de que un tercero no autorizado se encuentre en posesión de documentación interna, propia de la entidad denunciada con datos de carácter personal de sus clientes, hecho que constituye un acceso no autorizado y como tal, una pérdida de seguridad de esos datos.

Podemos recordar que entre los documentos aportados por el denunciante, se encuentran: impresiones de pantalla del sistema informático de la entidad con operaciones de clientes de esa sucursal, correos electrónicos internos de la entidad con datos de clientes de esa oficina, de manera que la documentación interna propia de dicha entidad, se encontraba en poder de un tercero no autorizado. Este hecho acredita que Bankia no ha garantizado la seguridad de los datos de carácter personal de sus clientes, para evitar 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. De manera que la conclusión es que habrán de adoptarse las medidas de seguridad necesarias que eviten, según sus palabras, "la posible sustracción o su obtención por alguna otra vía", pues esa es la finalidad de la implantación de las medidas de seguridad, evitar los riesgos a que están expuestos los datos personales de sus clientes ya provengan de la acción humana o del medio físico.

De manera que si bien en materia sancionadora rige el principio de culpabilidad, la expresión "simple inobservancia", del art. 130.1 de la Ley 30/92, permite la sanción por inobservancia del deber de cuidado. Existe una obligación de resultado, que no se ha cumplido, existiendo una falta de negligencia del responsable del tratamiento.

En el presente caso y teniendo en cuenta la documentación encontrada por el denunciante, ha quedado acreditado que la entidad BANKIA, no adoptó las medidas de índole técnica y organizativas necesarias que garantizasen la seguridad de los datos de carácter personal de sus ficheros, de manera que se evitase el acceso no autorizado a los datos de los mismos.

III

El artículo 44.3.h) de la LOPD, considera infracción grave:

"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen."

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

IV

El artículo 10 de la LOPD establece que: "El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento.

Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así el Tribunal Superior de Justicia de Madrid ha declarado en su Sentencia de 19 de julio de 2001: "El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)".

En este sentido, la sentencia de la Audiencia Nacional de fecha 18 de enero de 2002, recoge en su Fundamento de Derecho Segundo, y tercer párrafo: "El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable –en este caso, la entidad bancaria recurrente- de los datos almacenados –en este caso, los asociados a la denunciante- no puede revelar ni dar a conocer su contenido teniendo el "deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo" (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente, como el teléfono de contacto, no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez mas complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE. En efecto, este precepto contiene un "instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos" (STC 292/2000). Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino" (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, "es decir, el poder de resguardar su vida privada de una publicidad no querida"

*En el caso que nos ocupa, la entidad BANKIA es responsable del fichero en el que constan los datos de sus clientes, así como de la custodia de la documentación relativa a los mismos y que apareció en la vía pública cerca de la oficina *****. Atendiendo a las medidas de seguridad adoptadas por dicha entidad, se comprueba la existencia de un incumplimiento del deber de secreto, constatado por el acceso de un tercero no autorizado a documentación interna de la sucursal denunciada con datos de carácter personal de sus clientes, produciéndose una ausencia de confidencialidad, por lo que se considera que se ha cometido una infracción del transcrito artículo 10 de la LOPD.*

La Audiencia Nacional en su Sentencia de 7 de mayo de 2009 respecto del secreto profesional ha comunicado que: "El Art. 10 de la LOPD regula de forma concreta el deber de secreto de quienes tratan datos personales, dentro del título dedicado a los principios de protección de datos. Este deber de secreto pretende que los datos personales no puedan conocerse por terceros, salvo de acuerdo con lo dispuesto en otros preceptos de la LOPD, como el Art. 11 (comunicación de datos) o 12 (acceso a los datos por cuenta de terceros). El artículo 10, junto con el artículo 9 LOPD, que regula las medidas de seguridad, contiene una regla que afecta a la confidencialidad como parte de la seguridad, por lo que se refiere especialmente al responsable del fichero y a las personas que hayan participado en el tratamiento".

V

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

"La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley."

De acuerdo con los fundamentos anteriores, entendemos que por parte de la entidad BANKIA se ha producido una vulneración del deber de secreto que procede calificar como infracción grave.

En el presente caso ha quedado acreditado que ha tenido lugar una difusión de datos personales fuera del ámbito de la entidad denunciada porque se ha constatado el acceso a los mismos de un tercero no autorizado. Estos hechos suponen una vulneración de las medidas de seguridad así como del deber de guardar secreto por lo que la citada entidad ha incurrido en las infracciones graves descritas.

VI

El hecho constatado de la difusión de datos personales fuera del ámbito de la entidad BANKIA, establece la base de facto para fundamentar la imputación de las infracciones de los artículos 9 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto en el que un mismo hecho deriva en dos infracciones, dándose la circunstancia que la comisión de una implica necesariamente la comisión de la otra. Esto es, si un documento interno que contiene información sobre datos personales sale del ámbito de la entidad responsable de su

confidencialidad, 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.

Por lo tanto, aplicando el artículo 4.4 del Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora que señala que: "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, se ha producido una vulneración de las medidas de seguridad, calificada como grave por el artículo 44.3.h) de la LOPD y también un incumplimiento del deber de guardar secreto calificado como grave en el artículo 44.3.d) de la misma norma, procede imputar únicamente la infracción del artículo 9 de la LOPD por tratarse de la infracción originaria que ha dado lugar a la comisión de la otra infracción.

VII

El artículo 45 de la LOPD, apartados 1 a 5, según redacción introducida por la Ley 2/2011, de 4 de marzo, de Economía Sostenible, establece:

"1. Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.

2. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.

3. Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:
a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza.
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. 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, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente."

Expone la entidad denunciada en sus alegaciones que "de no estimarse las pretensiones aducidas por esta parte en las alegaciones anteriores, teniendo en cuenta que no ha habido intencionalidad por parte de Bankia, que mi representada ha implantado las medidas de seguridad de los datos referidas en el cuerpo del presente escrito, que no ha obtenido beneficio alguno por el hecho que supuestamente se le imputa y la cantidad de datos que trata, esta parte entiende que es indudable que se ha producido una disminución cualificada de la culpabilidad. En consecuencia, a tenor de lo dispuesto en el artículo 45.5 de la LOPD, procedería la imposición de las sanciones aplicando la escala relativa a la clase de infracción que precede inmediatamente en gravedad a aquéllas en que se integran las consideradas en este caso, esto es, las de las infracciones leves, que se sancionan con multa de 900 euros a 40.000 euros, tal y como se recoge en el artículo 45.1 de la LOPD. (…)

De conformidad con lo dispuesto en este precepto e invocando el principio de proporcionalidad consagrado en el artículo 131.3 de la LRJAP, teniendo en cuenta que teniendo en cuenta que no ha habido intencionalidad por parte de Bankia, que mi representada ha implantado las medidas de seguridad de los datos referidas en el cuerpo del presente escrito, que no ha obtenido beneficio alguno por el hecho que supuestamente se le imputa y la cantidad de datos que trata, esta parte entiende que las eventuales sanciones graves deberían imponerse en su grado mínimo."

El citado apartado 45.5 de la LOPD deriva del principio de proporcionalidad de la sanción y permite establecer "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", pero para ello es necesario la concurrencia de una cualificada disminución de la culpabilidad del imputado, o bien de la antijuridicidad del hecho, o bien alguna otra de las circunstancias que el mismo precepto cita. Así, el citado artículo debe aplicarse de forma excepcional y cuando se den suficientes circunstancias para ello.

En el presente caso se ha constatado que la entidad denunciada dispone de Documento de Seguridad que incluye medidas de seguridad para soporte papel y que existen normas operativas en relación a la seguridad de la información, valorando además que se trató de un hecho puntual, debe entenderse que operan dichas circunstancias atenuantes de la responsabilidad.

En segundo lugar, el art. 45.4 recoge una serie de criterios relativos a la

aplicación del principio de proporcionalidad en la graduación del importe de la sanción, según las indicaciones del art. 131.3 de la LRJPAC (Ley 30/92 de 26 de noviembre), que establece: "en la determinación normativa del régimen sancionador, así como en la imposición de sanciones por las Administraciones Públicas se deberá guardar la debida adecuación entre la gravedad del hecho constitutivo de la infracción y la sanción aplicada, considerándose especialmente los siguientes criterios para la graduación de la sanción a aplicar: a) la existencia de intencionalidad o reiteración, b) la naturaleza de los perjuicios causados, c) la reincidencia". Pues bien la secuencia de hechos expuesta en este caso, valoradas en aplicación de dichos criterios, permiten, que en este caso, se considere procedente que se fije la cuantía de la sanción en 6.000 euros, al haberse constatado una disminución cualificada de la culpabilidad.>>

III

Solicita la entidad recurrente en su escrito de recurso que se imponga la sanción mínima de las previstas para las infracciones leves en la cuantía de 900 euros o al menos se reduzca la sanción impuesta de forma considerable. Expone que la Agencia Española de Protección de Datos debiera haber tomado en consideración las circunstancias recogidas en el artículo 45.4 de la LOPD y en especial la letra e) de dicho artículo.

A este respecto cabe responder que, tal y como se expuso en la resolución, el importe de la sanción ya se ha minorado, teniendo en cuenta que la infracción cometida está tipificada como grave, pudiendo ser sancionada con multa de 40.001 a 300.000 euros.

Se ha tenido en cuenta que operan las circunstancias atenuantes de la responsabilidad previstas en el artículo 45.5 de la LOPD y por ello se ha establecido la cuantía de la sanción aplicando la escala relativa a las infracciones leves y ello porque se ha constatado que la entidad denunciada dispone de Documento de Seguridad que incluye medidas de seguridad para soporte papel y que existen normas operativas en relación a la seguridad de la información, valorando además que se trató de un hecho puntual.

Por otra parte, para la graduación del importe de la sanción ahora recurrida, también han sido tomados en consideración los criterios relativos a la aplicación del principio de proporcionalidad en la graduación del importe de la sanción impuesta y ello considerando tanto los criterios del artículo 45.4 de la LOPD, como los del artículo 131 de la LRJPAC. En el presente caso se han valorado como circunstancias agravantes, la vinculación de la actividad de la entidad infractora con la realización de tratamientos de datos de carácter personal y el volumen de negocio o actividad del infractor. Con todo ello se ha fijado la cuantía de la sanción del procedimiento ahora recurrido que se considera proporcionada a la gravedad de la infracción cometida.

Por lo tanto, en el presente recurso de reposición, la entidad BANKIA, S.A. no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

la Directora de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por la entidad BANKIA, S.A. contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 24 de septiembre de 2015, en el procedimiento sancionador PS/00185/2015.

SEGUNDO: NOTIFICAR la presente resolución a la entidad BANKIA, S.A.

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, se podrá interponer 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 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, 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 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos