Procedimiento PS/00051/2011

RESOLUCIÓN: R/01577/2011

En el procedimiento sancionador PS/00051/2011, instruido por la Agencia Española de Protección de Datos a la entidad **CAJA RURAL ARAGONESA Y DE LOS PIRINEOS, S. COOP. DE CRÉDITO, (MULTICAJA)**, vista la denuncia presentada por ***A.A.A.*** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 10 de mayo de 2010 tiene entrada en esta Agencia un escrito de ***A.A.A.*** en el que declara que siendo cliente de CAJA DE ABOGADOS (Ahora Multicaja), al acceder el 21 de abril de 2010 a sus datos a través de la página web de la entidad, constata que consultando el detalle de las transferencias realizadas por ella, aparece información completamente distinta de otro ordenante, otra cuenta de cargo y otro beneficiario, indicando que este hecho sucedía con todas y cada una de la transferencias consultadas lo que denotando un claro cruce de información.

Declara que contactó con la entidad financiera donde le confirmaron que eran conscientes del hecho y que estaban tratando de solucionarlo. Como durante la mañana del día 21 el problema seguía sin solventarse, por la tarde remitió un correo electrónico a Director de la sucursal, siendo contestado el mismo el día 23 de abril de 2010, reconociendo la existencia de un cruce de información entre las transferencias realizadas por los usuarios *"fruto de la migración y fusión del sistema informático de ambas entidades",* confirmando que el problema informático había quedado definitivamente solucionado.

Sin embargo, el 28 de abril de 2010 volvió a acceder a su cuenta y detectó que el problema seguía, hecho que también puso en conocimiento del banco, vía correo electrónico, pero no obtuvo respuesta.

SEGUNDO: A la vista de los hechos denunciados se inicia la fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se solicita información a la entidad CAJA RURAL ARAGONESA Y DE LOS PIRINEOS, S. COOP. DE CRÉDITO, (MULTICAJA) y concluye con el preceptivo informe del Inspector de Datos.

TERCERO: Con fecha 28/01/11 el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a CAJA RURAL ARAGONESA Y DE LOS PIRINEOS, S. COOP. DE CRÉDITO, (MULTICAJA) con arreglo a 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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por las presuntas infracciones de los artículos 9 y 10 de la LOPD, tipificada la primera como grave en el artículo 44.3.h) y como leve la segunda en el artículo 44.2.e) de la citada Ley Orgánica.

CUARTO: Notificado el acuerdo de inicio, Multicaja mediante escrito con entrada de 08/03/11 formula reconocimiento espontáneo de los hechos. Que el origen de los mismos esta en una anomalía derivada de la fusión en la entidad absorbida Que se efectuó rapida subsanación; ausencia de ilicito subjetivo y compromiso de cumplimiento de la normativa de protección de datos.

QUINTO: Con fecha 15/03/11 se inició el período de práctica de pruebas, acordándose las siguientes:

1. *Se dan por reproducidos a efectos probatorios la denuncia interpuesta por A.A.A. y su documentación, los documentos obtenidos y generados por los Servicios de Inspección ante CAJA RURAL ARAGONESA Y DE LOS PIRINEOS, S. COOP. DE CRÉDITO, (MULTICAJA) , y el Informe de actuaciones previas de Inspección que forman parte del expediente E/02044/2010.*

2. *Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio PS/00051/2011 presentadas por CAJA RURAL ARAGONESA Y DE LOS PIRINEOS, S. COOP. DE CRÉDITO, (MULTICAJA) , y la documentación que a ellas acompaña.*

3. Solicitar de A.A.A. que, en el plazo de DIEZ DÍAS hábiles, a contar desde la recepción de este escrito, se ratifique y amplíe -si lo estima conveniente- de forma pormenorizada la descripción de los hechos; aporte copia de todas las comunicaciones, notificaciones o escritos –en formato papel o electrónico- que haya recibido –dirigidas a su nombre de MULTICAJA. o de cualquier otra persona o entidad en su nombre, y de las reclamaciones, solicitudes o escritos dirigidos a dicho banco o a sus agentes, copia de los contratos suscritos con la entidad financiera o solicitudes de servicios dirigidos a la misma, QUE NO HUBIEREN SIDO YA APORTADOS.

5 Solicitar a MULTICAJA. que, en el plazo de DIEZ DÍAS hábiles, a contar desde la recepción de este escrito, aporte copia de todos los contratos de cuenta corriente, libretas de ahorro, tarjeta de crédito o cualquier modalidad de producto financiero suscritos por la persona denunciante; documentación que acredite el consentimiento de la persona denunciante para tratar sus datos personales; copia de los documentos que obren en poder de la entidad en relación a la apertura, movimientos y cancelación de las cuentas y depósitos o contratos de tarjetas de crédito – en cualquiera de los formatos en que consten- en que la persona denunciante figuraba como solicitante, titular o beneficiaria, QUE NO HUBIEREN SIDO APORTADOS.

Igualmente deberá aportar los documentos que como "documento número 1" dice acompañan a su escrito de alegaciones de 22/02/11, y no han sido remitidos. Si es posible en su contenido integro y copia completa de la cabecera de los correos electrónicos que alude".

En su respuesta la denunciada aporta copia de facturas generadas por la empresa de servicio técnico informático para la reparación de la Somalia denunciada y copia del contrato de cuenta Iurisbank por Internet y de banca a distancia de la denunciante.

En su respuesta la denunciante se ratifica en su denuncia sin añadir o presentar nada a lo dicho o adjuntado entonces.

SEXTO: Con fecha 13/06/11 se formuló propuesta de resolución, proponiendo se sancione a CAJA RURAL ARAGONESA Y DE LOS PIRINEOS, S. COOP. DE CRÉDITO, (MULTICAJA) con multa de 60.101,21 € (sesenta mil ciento un euro y veintiún céntimos) por la infracción del artículo 4.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, tipificada como grave en el artículo 44.3.d) de dicha norma.

Notificada la propuesta a la imputada, no se han presentado alegaciones.

De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes

HECHOS PROBADOS

1. La denunciante ha aportado impresiones de pantalla en las que figura el día 28/04/10 en la información que muestra la propia página web, es decir, como fecha que consta en la propia aplicación bancaria. También consta dicha fecha en el pie de página, fecha que pone el navegador de acuerdo con la fecha del ordenador desde que se accede a Internet. Aporta cinco impresiones de pantalla con nombres y apellidos, cuentas corrientes y datos de transferencias, correspondientes a personas físicas, y una impresión de pantalla relativa a una persona jurídica.

También aportó copia de los correos electrónicos remitidos al banco de fecha 21 y 28 de abril de 2010, así como la contestación emitida por la entidad bancaria de fecha 23 de abril de 2010.

2. CAJA RURAL ARAGONESA Y DE LOS PIRINEOS, S. COOP. DE CRÉDITO, en lo sucesivo MULTICAJA, es la entidad sucesora de la extinta CAIXA DELS ADVOCATS (CAJA ABOGADOS, S. COOP. DE CRÉDITO) en razón de absorción de esta última por aquélla, formalizada en virtud de escritura de fusión por absorción otorgada en fecha 29/12/2009 bajo fe del Notario de Huesca Don Francisco Rodríguez Boix, con número protocolar 1860, inscrita junto con otra de adición en el Registro Mercantil de Huesca al Tomo 467, Libro 7, Folio 211**,** Hoja HU-6254, inscripción 178**.**

3. El servicio de tratamiento de datos de MULTICAJA es realizado por RURAL SERVICIOS INFORMÁTICOS, S.C., con domicilio en Avenida de la Industria, 23, Tres Cantos (Madrid) y C.I.F. J-80/458.417, sociedad participada por la cuasi totalidad de las Cajas Rurales y cooperativas de crédito españolas que asume la gestión informática del negocio de éstas en su práctica integridad.

Aporta impresiones de los datos básicos de Doña Inmaculada Hernández Sandoval y igualmente copia del documento de seguridad de MULTICAJA, de cuyo tenor literal, y por su aplicabilidad al supuesto que nos ocupa, deben resaltarse las previsiones contenidas en los artículos 4.1.6 (notificación de incidencias) y 8.2 (gestión de incidencias), a los que se dio debido curso, como se verá, con ocasión del acontecer que da lugar a la denuncia origen del expediente.

4. Acompaña copia del Registro de Incidencias, indicando que refleja la ocurrida con relación al acceso a los datos de unos clientes a otros descritos en los e-mails que se anexan al propio requerimiento de información. En todo caso, y siendo cierta la concurrencia de incidencia debidamente registrada, que fue oportunamente resuelta, es menester hacer constar que, como quedará aclarado en los siguientes parágrafos, resulta imposible que los datos relativos a transferencias efectuadas por la denunciante Hernández Sandoval fuesen desvelados a terceros.

En el registro de incidencias se puede leer :

*EFECTOS DERIVADOS:**"**Afectados:clientes de multicaja. Efectos:Cuando se va a realizar la consulta de transferencias realizadas en Caja de Abogados antes de la fusión, desde los movimientos de una cuenta, cuando se pincha en el origen, la transferencia que se muestra corresponde con transferencias realizadas en MultiCaja**."***

MEDIDAS CORRECTORAS: "Se decidió no migrar documentos financieros, pero no se puso un filtro en el origen de modo que cuanto van a consultar el documento, el que encuentra es el de Multicaja. Con fecha 21/04/2010 está preparada la corrección, a falta de pasar la distribución…."

5. La incidencia registrada, consistente en el visionado de datos correspondientes a transferencias no coincidentes con la realmente consultada (y que, sin embargo, no comporta que los datos de la transferencia que se pretendía consultar luzcan donde no deben como consecuencia de consultas de terceros) por parte de una cliente de la extinta CAJA DE LOS ABOGADOS, tuvo las características que seguidamente se detallan, y siguió la cronología que oportunamente se precisa:

a. Se parte del proceso de integración informática de las entidades absorbente y absorbida -MULTICAJA y CAJA DE LOS ABOGADOS- debiéndose reseñar que ambas entidades eran, con anterioridad al proceso de fusión, usuarias de los servicios de R.S.I., S.C. Dicho proceso de integración informática se inició precisamente el día 19 de abril de 2010, se encuentra todavía en curso de desarrollo y ha sido en todo momento objeto de la debida supervisión por los afectados. En ese sentido, el próximo hito -en el que se determinará, en su caso, la extinción de los ficheros de datos de que se valía la extinta CAJA DE LOS ABOGADOS- es precisamente la auditoría externa de los procesos correspondientes, que tendrá lugar a partir del próximo día dieciocho.

b. La cliente detecta el acontecer del error antes referido, y lo pone en conocimiento de la oficina de MultiCaja: cuando se va a realizar consulta de transferencias realizadas a partir de cuentas abiertas en Caja de Abogados antes de la fusión, desde los movimientos de una cuenta, cuando se pincha el origen, la transferencia que se muestra corresponde con transferencias realizadas en MultiCaja. Esta puesta en conocimiento comporta la apertura de la incidencia genérica que se contiene en el Registro de Incidencias.

c. Debe reseñarse que, si bien la consulta de la denunciante conducía a datos relativos a transferencias no coincidentes con la/s pretendidamente consultada/s, EN NINGÚN CASO los datos de ésta o éstas últimas se reflejaban en otros lugares.

d. La cronología de acontecimientos a partir de ese momento es la siguiente:

-i. 2010/04/19: Se pone en conocimiento de RSI la incidencia de constante mención.

-ii. 2010/04/20: Según se nos indica por RSI, el área de Core Bancario de dicha empresa efectúa las correcciones precisas para solventar la incidencia.

-iii. 2010/04/28: Según se nos ha informado por RSI, el área de Banca a Distancia de RSI recibe una Incidencia adicional de análoga naturaleza detectada por otro cliente.

-iv. 2010/04/29: Según se nos indica por RSI, el área de Banca a Distancia de RSI efectúa las correcciones precisas por su parte para solventar la incidencia.

-v. 2010/05/08: pase a producción en RSI mediante proceso automático 'inimig' de las correcciones efectuadas por su área de Core Bancario, quedando así solventadas las incidencias, introduciendo, según se nos tiene dicho por R.S.I., S.C. un sistema de validación y control y un bloqueo de manera que se evite en el futuro nueva incidencia de este tipo

7. No hay noticia de informes de error a la Entidad ni a R.S.I., S.C. diferentes de lo expuesto en los parágrafos anteriores de este escrito.

8. Esta Entidad considera esencial en este punto poner de manifiesto:

a. Por una parte, que la preocupación por la seguridad en los datos personales es elemento crítico en el proceso de los mismos, encontrándose en el momento actual en vía de implementación la revisión del Plan Director de Seguridad de la Entidad;

b. Por otra, que la praxis negocial de MULTICAJA se fundamenta en el rigurosísimo respeto por el derecho a la intimidad y en el mantenimiento de la confidencialidad de los datos e información que tiene encomendados para el desarrollo de aquélla.

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 (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).

II.

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 dicha seguridad, 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 artículo 3.a) los define como *"todo conjunto organizado de datos de carácter personal"* con independencia de la modalidad de acceso al mismo. Por su parte, la letra c) del mismo artículo 3 permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente expediente, la *"conservación"* o *"consulta"* de los datos personales, tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.

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

Sintetizando las previsiones legales puede afirmarse que:

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

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

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

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

Partiendo de tales premisas, deben analizarse a continuación las previsiones que el Real Decreto 994/1998, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, que continúa en vigor de acuerdo con lo estipulado en la disposición transitoria tercera de la LOPD, prevé para garantizar que no se produzcan accesos no autorizados a los ficheros.

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

El artículo 4.1 del Reglamento prevé que *"todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico"*, reguladas en el Capítulo II del citado Reglamento de medidas de seguridad, artículos 8 a 14 del mismo.

Esta previsión resulta aplicable en el presente caso, por cuanto, considerando la estructura del fichero automatizado *"CLIENTES"*, declarado de *"Nivel básico"*, procede aplicarle el nivel básico de medidas de seguridad, reguladas en el citado Capítulo II del Reglamento de medidas de seguridad.

Así, **Multicaja** está 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 no autorizado por parte de terceros a los datos de sus clientes contenidos en el fichero mencionado. Sin embargo, ha quedado acreditado que la citada entidad incumplió esta obligación, al posibilitar que un tercero pudiera acceder a datos personales de titulares de otros contratos de cuenta.

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".

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

Dado que ha existido vulneración del *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, se considera que **Multicaja** ha incurrido en la infracción grave descrita.

IV.

Asimismo, el presente procedimiento tiene por objeto determinar las responsabilidades que se derivan de la revelación de los datos contenidos en el fichero *"CLIENTES"*.

El artículo 10 de la LOPD dispone:

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

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

Este deber de secreto comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido, teniendo el *"deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática, a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30/11, y, por lo que ahora interesa, comporta que los datos tratados no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española. En efecto, este precepto contiene un *"instituto de garantía de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos"* (Sentencia del Tribunal Constitucional 292/2000, de 30/11). Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino que impida que se produzcan situaciones atentatorias con la dignidad de la persona, es decir, el poder de resguardar su vida privada de una publicidad no querida.

Igualmente, cabe destacar la Sentencia dictada por la Audiencia Nacional, de fecha 14/09/2001, que en los Fundamentos de Derecho Tercero y Cuarto señala:

"Pues bien, la conducta que configura el ilícito administrativo -artículo 43.3.g) de la Ley Orgánica 5/1992- requiere la existencia de culpa, que se concreta, por lo que ahora interesa, en el simple incumplimiento del deber de guardar secreto, deber que se transgrede cuando se facilita información a terceros de los datos que sobre el titular de una cuenta bancaria dispone la entidad recurrente, siendo indiferente a estos efectos que los datos se facilitaran mediante engaño, pues la entidad bancaria no observó una conducta diligente tendente a salvaguardar el expresado deber de secreto, y esta conducta basta para consumar la infracción cuya sanción se recurre en el presente recurso. En consecuencia, esa falta de diligencia configura el elemento culpabilístico de la infracción administrativa y resulta imputable a la recurrente. En definitiva, concurren los requisitos exigibles para que la conducta sea culpable, pues la conducta desarrollada vulnera el deber de guardar secreto, es una conducta tipificada como infracción administrativa, y la voluntariedad reviste forma de culpa".

En el presente caso, la entidad **Multicaja**, con el sistema que tuvo implementado, permitió el acceso de tercero a datos de contratos y su gestión de sus clientes, cuestión que ha quedado acreditada en el presente procedimiento sin que el titular de los datos hubiese prestado su consentimiento para ello.

Por tanto, queda acreditado que por parte de **Multicaja**, 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 por terceros a datos personales de consumo y facturación de los titulares de los contratos de suministro de agua, sin contar con el consentimiento de éstos.

V.

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, conviene analizar la incidencia de la infracción cometida por **Multicaja**, al objeto de su correcta tipificación conforme a lo señalado anteriormente. Así, teniendo en cuenta que los datos aportados por la citada entidad a un tercero, no permiten obtener una evaluación de la personalidad de los afectados, titulares de dichos datos, la vulneración del artículo 10 de la LOPD constatada ha de calificarse como infracción leve, tipificada en el citado artículo 44.2.e) de la misma norma.

VI.

Los hechos constatados, consistentes en facilitar a terceros el acceso a datos personales sin el consentimiento del titular de los datos, constituye una base fáctica para fundamentar la imputación a **Multicaja** 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 una información contenida en un fichero de clientes 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 profesional.

Por lo tanto, aplicando el artículo 4.4 del citado Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora, procede subsumir ambas infracciones en una, procediendo imponer únicamente la sanción correspondiente a la infracción más grave que, en este caso, corresponde a la prevista para la infracción del artículo 9 de la LOPD que, además, se trata de la infracción originaria que ha implicado la comisión de la otra.

VII.

El artículo 45 de la LOPD, en la redacción dada por la Ley 2/2011, de 4 de marzo, de Economía Sostenible, establece, en sus apartados 1 a 5, lo siguiente:

"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.»

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, o bien una cualificada disminución de la culpabilidad el imputado, o bien de la antijuridicidad del hecho, o bien de alguna otra de las circunstancias que el mismo precepto cita.

Las citadas circunstancias no se dan en el presente caso, lo que impide apreciar la existencia de motivos para la aplicación de la facultad contemplada en el artículo 45.5, debido, por un lado, a que no obra en el expediente ningún elemento que lleve a apreciar la concurrencia de alguna de las circunstancias previstas en los apartados c), d) y e) del referido artículo y, por otro, a la especial diligencia y conocimiento de la normativa de protección de datos que se ha de exigir a las entidades profesionales cuando, como ocurre con la entidad imputada, el tratamiento de datos personales constituye parte habitual y esencial de su actividad. Las empresas que por su actividad están habituadas al tratamiento de datos personales deben ser especialmente diligentes y cuidadosas al realizar operaciones con ellos y deben optar siempre por la interpretación más favorable a la salvaguarda del derecho fundamental a la protección de datos .

Por todo ello, procede imponer una multa cuyo importe se encuentre entre 40.001 € y 300.000 €, en aplicación de lo previsto en el apartado 2 del citado artículo 45, al tener la infracción imputada la consideración de grave. En el presente caso, teniendo en consideración los criterios de graduación de las sanciones establecidos en el artículo 45.4, y en particular, la vinculación de la actividad de la entidad infractora con la realización de tratamientos de datos de carácter personal y el volumen de negocio de la misma, se impone una multa de 50.000 €.

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 **CAJA RURAL ARAGONESA Y DE LOS PIRINEOS, S. COOP. DE CRÉDITO, (MULTICAJA)** , por una infracción del artículo **9** de la LOPD, tipificada como grave en el artículo **44.3.h)** de dicha norma, una multa de **50.000** € (cincuenta mil euros) de conformidad con lo establecido en el artículo 45.2 y 4 de la citada Ley Orgánica –según redacción dada por la Ley 2/2011-.

SEGUNDO: **NOTIFICAR** la presente resolución a **CAJA RURAL ARAGONESA Y DE LOS PIRINEOS, S. COOP. DE CRÉDITO, (MULTICAJA)** y a ***A.A.A.*** .

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 0182 2370 43 0200000785 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, 20 de julio de 2011

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: José Luis Rodríguez Álvarez