



Procedimiento Nº PS/00287/2009

RESOLUCIÓN: R/02427/2009

En el procedimiento sancionador PS/00287/2009, instruido por la Agencia Española de Protección de Datos a la entidad Banco Etchevarría S.A. y vista la denuncia presentada por Dña A.A.A. y en base a los siguientes:

ANTECEDENTES

PRIMERO: Con fecha de 24/06/08 tuvo entrada en esta Agencia un escrito de D^a A.A.A. (en lo sucesivo la denunciante) contra la entidad Banco Etchevarría S.A. (en lo sucesivo la denunciada). En dicho escrito manifiesta que el día 12/06/08, cuando disponía a echar a la basura en unos contenedores situados en la (C.) se encontró en el suelo una serie de documentos procedentes del Banco Etchevarría, comprobando la existencia de documentación similar dentro de los contenedores que estaban al lado.

Se han aportado diversas fotografías tomadas en ese lugar y parte de la documentación encontrada, y en concreto:

- 1.1 Escritos, emitidos el 9/06/08 remitiendo pin (número secreto para poder acceder al servicio de Banca Electrónica) a diversas direcciones correspondientes a clientes de dicho Banco (22 en total).
- 1.2 Remisión de un contrato de apertura de depósito a plazo
- 1.3. Impresión de pantalla de "mantenimiento de clientes" relativo a un cliente

SEGUNDO: A la vista de los citados hechos, en fase de actuaciones previas, se levantó Acta de Inspección: (E/1520/2008/I-01) en la sede de la sucursal del Banco Etchevarría, sita en la (C/.), el día 7/11/08, acreditándose los siguientes hechos:

2.1 El Banco dispone del correspondiente documento de seguridad, cuya copia se ha aportado al expediente

2.2 Actualmente han contratado los servicios de una consultora al objeto de adecuar los procedimientos establecidos al nuevo reglamento de protección de datos. Además, tiene implantados distintos procedimientos relacionados con las exigencias que se recogen en la



normativa de protección de datos. Todos ellos están disponibles en la Intranet del Banco para su consulta por cualquier empleado.

2.3 Respecto de los procedimientos utilizados para destruir los documentos en soporte papel, todos los empleados que ingresan cuentan con un período de formación durante 15 días que se imparte en los servicios centrales del Banco y donde se les explica, entre otros temas relacionados con la banca, la importancia de la confidencialidad de la información a la que tendrán acceso y de la prohibición de depositar documentos con datos personales en la papelerera.

Los empleados tienen instrucciones sobre cómo deben destruir los documentos, el procedimiento recoge que todos los empleados son responsables de la destrucción de los documentos innecesarios utilizando la destructora, queda prohibido tirar documentos a la papelerera.

Por otra parte, todos los contratos de trabajo que el banco firma con sus empleados llevan anexo un documento que hace referencia a la confidencialidad de la información manejada en su puesto de trabajo.

2.4 Los representantes del Banco hacen las siguientes manifestaciones:

2.4.1. El Banco ha realizado un esfuerzo enorme por dotar a todos los despachos en todas las sucursales del Banco, de destructoras de papel. Además, ha contratado los servicios de una empresa que se encarga de recoger los documentos y destruirlos.

2.4.2. El personal de la limpieza también tiene instrucciones en el sentido de vaciar únicamente el contenido de las papeleras.

2.4.3. El Banco realiza auditorias internas bianuales siguiendo la normativa de protección de datos respecto de las medidas de seguridad implantadas en el banco.

2.4.4. Desconocen que se hayan depositado en un contenedor ubicado en la vía pública, documentos procedentes del Banco y no pueden aportar ninguna justificación o aclaración al respecto. Únicamente puede deberse al incumplimiento, por parte de algún empleado, del protocolo establecido para destruir documentos o por una posible imprudencia del personal de limpieza

2.4.5. Reconocen que los documentos mostrados tienen su origen en la oficina donde se realiza la inspección y que algunos de ellos hacen referencia al servicio de banca electrónica. Sin embargo, no entienden por qué se encontraban todos esos documentos en el contenedor ya que tienen muchos protocolos establecidos y divulgados entre sus empleados.

2.5 Por parte de los inspectores actuantes se realizaron las siguientes comprobaciones:

2.5.1 Que para acceder a la intranet del Banco es necesario introducir usuario y contraseña y que se encuentra a disposición de todos los empleados normativa relacionada con temas de seguridad y de la LOPD, entre la que se encuentra la norma denominada "*norma consulta y destrucción de documentos*".



2.5.2 En el fichero donde se gestionan los datos personales de los clientes, se realizaron distintas búsquedas relacionadas con tres documentos escogidos al azar entre los mostrados a los inspeccionados verificándose lo siguiente:

- o Se realiza una búsqueda por los apellidos “C.G.” y se comprueba que consta como cliente D. B.C.G. con la misma dirección que aparece en el documento mostrado.
- o Se realiza una búsqueda por los apellidos “A. D.” y se comprueba que consta como cliente D. C.A.D. con la misma dirección que aparece en el documento mostrado.
- o Se realiza una búsqueda por los apellidos “M.V.” y se comprueba que consta como cliente D^a. D.M.V. con la misma dirección que aparece en el documento mostrado.

2.5.3. Se comprobó que el despacho donde se desarrolló la inspección dispone de una destructora de papel.

2.5.4 Que el Banco dispone de distinta documentación interna sobre medidas en materia de protección de datos de carácter personal y donde consta textualmente “*Cumplir con el protocolo de consulta y destrucción de documentos con datos de carácter personal para evitar su acceso o recuperación, por parte de personas no autorizadas*”.

2.5.6. Que se ha elaborado un protocolo de consulta y destrucción referenciado en el documento anterior y que se denomina “*Norma consulta y destrucción de documentos*”.

2.5.7. Que se dispone de contrato firmado con la empresa de limpieza y con la empresa destructora de documentos.

2.5.8 Finalmente, a fecha de la inspección, el Banco se encuentra en fase de adecuación a la nueva normativa de protección de datos.

QUINTO: En fecha 01/06/09 el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a Banco Etcheverría S.A. por posible infracción de los artículos 9 y 10, tipificada como grave en los artículos: 44.3.h) y 44.3.g), de la citada ley orgánica.

SEXTO: Notificado el acuerdo de inicio, el representante de Banco Etcheverría formuló, en síntesis, las siguientes alegaciones al Acuerdo de Inicio:

6.1 Que el número secreto de acceso al servicio de banca electrónica (PIN) que se envía no es suficiente para entrar en la consulta de un cliente. Es necesario además de disponer de la tarjeta (que se envía en otra carta separada) de la que se pedirá la numeración y una coordenada.

6.2 Los PIN se envían directamente a la dirección que el cliente ha proporcionado en sobres cerrados. Ocasionalmente se realizan impresiones de prueba de PIN no reales y “serían en todo caso, estas pruebas los únicos documentos que podrían ser objeto de destrucción por la entidad bancaria y, por lo tanto los que podrían haber aparecido en el contenedor”. Los únicos datos personales reales que constarían serían los propios del envío: nombre y apellidos y dirección. En conclusión “los datos a los que se refiere la denuncia son datos calificados por el RLOPD como de nivel básico o se trataría de datos ficticios”.

6.3 Que le entidad dispone de procedimientos internos para cumplir la normativa vigente, teniendo elaborado e implementado el Documento de Seguridad. Dispone además de una serie



de protocolos en relación con la destrucción de documentación y deber de secreto, que se han aportado al procedimiento. Se manifiesta que la entidad desconocía que hubieran fallado las medidas implantadas, "se podrían haber debido al incumplimiento, por parte de algún empleado, de los protocolos internos establecidos para asegurar la correcta destrucción de los documentos o a una posible imprudencia del personal externo de la limpieza".

6.4 Como consecuencia de los hechos descritos la entidad realizó una auditoría interna y realizó un proceso de revisión de los procedimientos elaborados y su efectiva implantación. Realizándose una serie de actuaciones aportadas en el procedimiento.

6.5 Que entiende que, en todo caso, los hechos deben ser tipificados como infracción leve y no grave. Existiendo además concurrencia entre las dos infracciones por lo que procedería a aplicar la más grave.

6.6 Con carácter subsidiario, aplicación del art. 45.5 estimando que se dan suficientes circunstancias para apreciar una disminución cualificada de la culpabilidad.

SEPTIMO: Con fecha 22/07/09 se inició el período de práctica de pruebas, practicándose las siguientes:

7.1 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 Banco Etchevarría S.A, y el Informe de actuaciones previas de Inspección que forman parte del expediente E/01520/2008.

7.2 Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio PS/00287/2009 presentadas por BANCO ETCHEVERRIA, S.A., con fecha 3/07/09, y la documentación que a ellas acompaña.

OCTAVO: El día 30/9/09 se emitió propuesta de resolución por el instructor del procedimiento, notificada el 5/10/09 en el sentido que por el Director de la Agencia Española de Protección de Datos se sancionase a Banco Etchevarría con multa de 6.000 € por la infracción del artículos 9 de la Ley orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, tipificada como grave en el artículo 44.3.h) de dicha norma

No se han presentado alegaciones a la propuesta de resolución

HECHOS PROBADOS

PRIMERO: Con fecha de 24/06/08 tuvo entrada en esta Agencia un escrito de D^a A.A.A. (en lo sucesivo la denunciante) contra la entidad Banco Etchevarria S.A. (en lo sucesivo la denunciada). En dicho escrito manifiesta que el día 12/06/08, cuando disponía a echar a la basura en unos contenedores situados en la (C.) se encontró en el suelo una serie de documentos procedentes del Banco Etchevarría, comprobando la existencia de documentación similar dentro de los contenedores que estaban al lado. (Folios 1-4)

SEGUNDO: Se han aportado diversas fotografías tomadas en ese lugar y parte de la documentación encontrada, y en concreto:



A)- Escritos, emitidos el 9/06/08 remitiendo pin (número secreto para poder acceder al servicio de Banca Electrónica) a diversas direcciones correspondientes a clientes de dicho Banco (22 en total).

En dichos escritos figuran los siguientes datos personales:

- Nombre y apellidos
- Dirección
- PIN de acceso a la Banca Electrónica

B)- Remisión de un contrato de apertura de depósito a plazo.

C)- Impresión de pantalla de “mantenimiento de clientes” relativo a un cliente (Folios 5-40)

TERCERO: Los representantes de la entidad reconocen que los documentos mostrados tienen su origen en la oficina donde se realiza la inspección y que algunos de ellos hacen referencia al servicio de banca electrónica. Sin embargo, no entienden por qué se encontraban todos esos documentos en el contenedor ya que tienen muchos protocolos establecidos y divulgados entre sus empleados. (Folio 49)

CUARTO: El Banco dispone del correspondiente documento de seguridad, cuya copia se ha aportado al expediente. En el anexo II (funciones y responsabilidades) se establece como obligación del personal del Banco: “cumplir con el protocolo de consulta y destrucción de documentos de carácter personal”. (Folios 55-86)

QUINTO: Se ha aportado por la entidad documento titulado: “Normas de seguridad”, de fecha mayo de 2008, donde se recogen instrucciones concretas, dirigidas a todos los empleados, para el tratamiento y protección de la documentación de carácter personal. (Folios 135-142)

SEXTO: Los empleados tienen instrucciones sobre cómo deben destruir los documentos, el procedimiento recoge que todos los empleados son responsables de la destrucción de los documentos innecesarios utilizando la destructora, queda prohibido tirar documentos a la papelera. (Folios 120-121)

SEPTIMO: En el fichero donde se gestionan los datos personales de los clientes, se realizaron distintas búsquedas relacionadas con tres documentos escogidos al azar entre los mostrados a los inspeccionados verificándose lo siguiente:

- Se realiza una búsqueda por los apellidos “C.G.” y se comprueba que consta como cliente D. B.C.G. con la misma dirección que aparece en el documento mostrado.
- Se realiza una búsqueda por los apellidos “A.D.” y se comprueba que consta como cliente D. C.A.D. con la misma dirección que aparece en el documento mostrado.
- Se realiza una búsqueda por los apellidos “M.V.” y se comprueba que consta como cliente D^a. D. M. V. con la misma dirección que aparece en el documento mostrado. (Folios 49-50)



OCTAVO: Se dispone de contrato firmado con la empresa de limpieza y con la empresa destructora de documentos. (Folios 127-134)

NOVENO: Se ha adjuntado copia del informe de auditoría interna (Folios 143-157) y externa (Folios 58-172) para adecuar el banco a la nueva normativa de protección de datos.

DECIMO: La sucursal donde se realizó la inspección disponía de destructora de papel. (Folio 50)

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

El Art. 7 Del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

“Seguridad de los datos:

Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados”.

El Art 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

“Seguridad del tratamiento:

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse”

La ley Orgánica de Protección de Datos, (en so sucesivo LOPD), traspuso al ordenamiento interno el contenido de la Directiva 95/46. En el Art 32.1 de la citada Directiva se daba un plazo de tres años desde la adopción de la misma para que se adoptasen las disposiciones legales para dar cumplimiento a lo establecido en ella. Plazo que se extendían hasta los 12 años en relación a “el tratamiento de los datos que ya se encuentran incluidos en ficheros manuales en la fecha de entrada en vigor de de las disposiciones nacionales adoptadas en aplicación de la presente Directiva”.



III

La LOPD en su artículo 1 dispone que:

“la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos 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”.

El artículo 2.1 de la misma ley orgánica establece:

“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 públicos y privados”.

El artículo. 3 de la LOPD establece las definiciones de responsable de fichero o tratamiento, de encargado de tratamiento y de cesión de datos:

“d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento

.....

g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento

.....

l) Cesión o comunicación de datos: toda revelación de datos realizada a la persona distinta del interesado.”

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 la 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.”

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.



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.

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. Dichas medidas, en el caso que nos ocupa, deben salvaguardar la confidencialidad y seguridad de los datos de carácter personal contenidos en los ficheros de la entidad bancaria. Siendo aquellas que deben ser adoptadas las calificadas de nivel medio, en atención al tipo de información sensible que se manejan las entidades financieras, y tal como se especifica en el art. 81.2d) del RD 1720/2007, de 21 de diciembre, (Reglamento de desarrollo de la LOPD).

Al contrario de la normativa anterior, 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). Dentro de estas últimas, en lo referente al nivel medio, deben tenerse en cuenta las siguientes prescripciones:

“Artículo 106. Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo

Artículo 107. Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. Custodia de los soportes.



Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.”

De los hechos probados en este procedimiento, se deduce que Banco Etchevarria, en su calidad de responsable del tratamiento, debió adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información de carácter personal que contenían dichos documentos. Tales medidas no fueron adoptadas totalmente en el presente caso, como lo acredita el hecho que dicha documentación fue encontrada por la denunciante, en la vía pública. Esta necesidad de especial diligencia en la custodia de la documentación por el encargado del tratamiento 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”*

En cuanto al tipo de información encontrada: a)- 22 Escritos, emitidos el 9/06/08 remitiendo pin (número secreto para poder acceder al servicio de Banca Electrónica) a diversas direcciones correspondientes a clientes de dicho Banco b) - Remisión de un contrato de apertura de depósito a plazo. c)- impresión de pantalla de “mantenimiento de clientes” relativo a un cliente, procede manifestar lo siguiente:

Se acreditó en la inspección realizada en la entidad denunciada, tomando tres documentos escogidos al azar, que el nombre y apellidos y la dirección postal coincidía con clientes de la entidad (según consulta efectuada en el fichero donde se gestionan los datos personales de los clientes),

Se alega por Banco Etchevarria “Que el número secreto de acceso al servicio de banca electrónica (PIN) que se envía no es suficiente para entrar en la consulta de un cliente. Es necesario además de disponer de la tarjeta (que se envía en otra carta separada) de la que se pedirá la numeración y una coordenada.” considerando que los “Los únicos datos personales reales que constarían serían los propios del envío: nombre y apellidos y dirección. En conclusión “los datos a los que se refiere la denuncia son datos calificados por el RLOPD como de nivel básico o se trataría de datos ficticios”

El artículo 2.1 de la Ley Orgánica dispone establece 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”.

Por su parte, el artículo 3 a) de dicha Ley añade que se entenderá por datos de carácter personal “cualquier información concerniente a personas físicas identificadas o identificables”. En este mismo sentido se pronuncia el artículo 2 a) de la Directiva 95/46/CE del Parlamento y del



Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos profesionales y a la libre circulación de estos datos, que dispone *“toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”*.

Para interpretar cuándo ha de considerarse que nos encontramos ante un dato de carácter personal esta Agencia ha venido siguiendo el criterio sustentado por las distintas Recomendaciones emitidas por el Comité de Ministros del Consejo de Europa, en las que se indica que la persona deberá considerarse identificable cuando su identificación no requiere plazos o actividades desproporcionados.

Queda fuera de toda duda que tanto el nombre y apellidos, como la dirección son datos de carácter personal, siendo en todo caso suficientes para considerar que por parte de la entidad denunciada se ha infringido lo dispuesto en la LOPD. En cuanto al carácter del “pin” (- Número de Identificación Personal entregado a un usuario de un servicio para acceder al mismo), se ha alegado que su solo conocimiento no permite el acceso al servicio de banca electrónica, ya que es necesario además de disponer de la tarjeta (que se envía en otra carta separada) de la que se pedirá la numeración y una coordenada). No obstante al venir asociado a una persona concretada, y el uso que pudiera darse de ese dato, significa que no debe estar accesible a terceros.

Debe tenerse en cuenta la definición de documento, que establece el artículo 5.2.f del Reglamento de desarrollo de la LOPD como “todo escrito, gráfico, sonido, imagen o cualquier clase de información como una unidad diferenciada”, la documentación encontrada en la vía pública procedente de ese Banco entra en la consideración de documento de trabajo, incorporando información derivada de un fichero automatizado, que contiene datos personales, debiéndosele aplicar las medidas de seguridad previstas reglamentaria a este tipo de ficheros. Además el art. 92.4 del citado Reglamento dispone lo siguiente:

“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”

Este artículo regula las obligaciones, que tendrán que aplicarse cuando vaya a desecharse cualquier documento o soporte que contenga datos personales, estableciéndose que deberá procederse a su destrucción o borrado. No se definen cuales son esas medidas, pero en cualquier caso, se establece que serán aquellas que eviten el acceso a la información contenida en los mismos, así como su posible recuperación posterior

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 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 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 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, Banco Etchevarria es responsable de la custodia de la documentación relativa a sus clientes y que apareció abandonada en la vía pública. Existiendo pues, una omisión del deber de secreto, produciéndose una ausencia de confidencialidad, por lo que se considera que se ha cometido una infracción del transcrito artículo 10 de la LOPD.

V

El art. 44.3.h) de la LOPD, califica como 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”

Así mismo el artículo 44.3.g) de la LOPD, califica como infracción grave:

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

De acuerdo con los fundamentos anteriores, se deduce que por parte de Banco Echevarria se ha producido una vulneración del deber de secreto y de seguridad de los datos, que ha tenido como consecuencia que los datos personales de varios clientes pudieran ser vistos por un tercero, infracciones que procede calificarlas como graves. sin que pueda exonerarse su responsabilidad tal como se ha demostrado en este procedimiento, por lo que procede su imputación, elemento necesario en el derecho administrativo sancionador tal como establece la STS de 27/5/99: “Para la imposición de una sanción y las consecuencias derivadas del ilícito administrativo, no basta que la infracción esté tipificada y sancionada...sino que es necesario que se aprecie en el sujeto infractor el elemento o categoría denominado culpabilidad. La culpabilidad es el reproche que se hace a una persona, porque ésta debió haber actuado de modo distinto de cómo lo hizo”.

VI

El hecho constatado de la difusión de datos personales fuera del ámbito de la entidad denunciada 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.g) de la misma norma, procede imputar únicamente la infracción del artículo 9 de la LOPD.

VII

El artículo 45 apartados 2,4 y 5 de la LOPD estipula:



“3. Las infracciones graves serán sancionadas con multa de 60.101,21€ a 300.506,05 €.

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora”

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate”.

Se ha solicitado, de forma subsidiaria, por la entidad denunciada la aplicación del art 45.4 y 5 en base al principio de proporcionalidad.

En primer lugar hay que tener en cuenta lo establecido en el art. 45.5, que trata de hacer efectivo hasta sus últimas consecuencias el principio de proporcionalidad, mediante la aplicación de la sanción correspondiente relativa a la escala inferior y ello cuando se aprecie disminución de la culpabilidad del imputado o de la antijuridicidad del hecho. Estos dos criterios no son sino criterios jurídicos indeterminados que deben concretarse en cada supuesto en el que se pretenda su aplicación. Debe tenerse en cuenta la interpretación establecida la Audiencia Nacional, en sus Sentencias, entre otras, de 24/05/2002 y 16/02/2005, *“la presente regla debe aplicarse con exquisita ponderación y solo en los casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas atendidas las circunstancias del caso concreto, de forma que repugne a la sensibilidad jurídica, siempre guiada por el valor justicia, la imposición de la sanción correspondiente al grado. Lo cual insistimos puede darse, por excepción, en casos muy extremos y concretos.”*

Valorando las circunstancias del presente caso, donde se ha establecido en los hechos probados que se trató de un hecho puntual; que la entidad ha reconocido su responsabilidad y que la documentación procedió de dicha sucursal, que dispone de documento de seguridad, que ha realizado dos auditorías para adecuar el Banco a la normativa de protección de datos, se imparte a los trabajadores instrucciones sobre la destrucción de documentación, disponiendo la entidad de medidas de seguridad. Debe entenderse que operan dichas circunstancias atenuantes de la responsabilidad; aplicadas ya por esta Agencia, en otros procedimientos similares relativos a la localización en la vía pública de documentación con datos de carácter personal.

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 esta resolución, valorándolas en aplicación de dichos criterios, permiten, que en este caso, se considere procedente fijar la sanción en 6.000 euros, al haberse constatado una disminución cualificada de la culpabilidad.

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 Banco Etchevarría, S.A., 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 45.3, 4 y 5 de la citada Ley Orgánica.

SEGUNDO: REQUERIR a Banco Etchevarría S.A., para que adopte las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 9 de la LOPD, con indicación de que, de acuerdo con lo preceptuado en el artículo 49 de la citada Ley Orgánica, si el requerimiento fuera desatendido la Agencia Española de Protección de Datos podrá inmovilizar el fichero.

Las medidas y actuaciones adoptadas deberán ser comunicadas a esta Agencia Española de Protección de Datos, en el plazo de un mes.

TERCERO: NOTIFICAR la presente resolución a Banco Etchevarría S.A. y a Dña A.A.A..

CUARTO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida Nº 0000 0000 00 0000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo



25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Madrid, 16 de noviembre de 2009

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte