# EL EMPLEADO DE BANCA EN SU PUESTO DE TRABAJO: RECOMENDACIONES EN EL TRATAMIENTO DE LA INFORMACIÓN

**José Antonio González Martínez**
*Profesor de Derecho de la Escuela Universitaria de Relaciones Laborales de Elda, adscrita a la Universidad de Alicante*

**Sumario**: 1ª. Recomendación: "Necesidad de cumplir el deber de secreto en el ejercicio de la actividad bancaria". 2ª. Recomendación.- "No entorpecer el ejercicio de los derechos de acceso, rectificación y cancelación". 3ª. Recomendación.- "Obligación de acreditar el consentimiento de los interesados para el tratamiento y cesión de sus datos". 4ª. Recomendación.- "Evitar los 3 riesgos potenciales respecto a la creación, mantenimiento y posterior tratamiento de los datos de estos ficheros por las entidades acreedoras". 5ª. Recomendación.- "Necesidad de adoptar las oportunas medidas de seguridad". 6ª. Recomendación.- "Ante los troyanos bancarios... ¡seguridad!". 7ª. Recomendación.- "Necesidad de un manual de recobros con el fin de garantizar el respeto al honor y la intimidad de los deudores recobrados".

**Recibido: 5 de Febrero de 2013**
**Aceptado: 6 de Febrero de 2013**

# EL EMPLEADO DE BANCA EN SU PUESTO DE TRABAJO: RECOMENDACIONES EN EL TRATAMIENTO DE LA INFORMACIÓN

**Sumario**: 1ª. Recomendación: "Necesidad de cumplir el deber de secreto en el ejercicio de la actividad bancaria". 2ª. Recomendación.- "No entorpecer el ejercicio de los derechos de acceso, rectificación y cancelación". 3ª. Recomendación.- "Obligación de acreditar el consentimiento de los interesados para el tratamiento y cesión de sus datos". 4ª. Recomendación.- "Evitar los 3 riesgos potenciales respecto a la creación, mantenimiento y posterior tratamiento de los datos de estos ficheros por las entidades acreedoras". 5ª. Recomendación.- "Necesidad de adoptar las oportunas medidas de seguridad". 6ª. Recomendación.- "Ante los troyanos bancarios... ¡seguridad!". 7ª. Recomendación.- "Necesidad de un manual de recobros con el fin de garantizar el respeto al honor y la intimidad de los deudores recobrados".

**Resumen:** El presente artículo tiene por objeto la difusión de una materia muy importante, y un tanto desconocida, como es la incidencia de la información que manejan las entidades de crédito con la protección de datos de carácter personal.

Surge una preocupación de los distintos Estados por la protección de la información privada de sus ciudadanos, ante el elevado número de delitos cometidos por el conocimiento por terceras personas de datos personales, sobre todo en cuestiones relacionadas con las entidades de crédito, por la gran cantidad de información que manejan. El sector de los servicios financieros, en la actualidad, ha de enfrentarse al incremento de competencia y a la pérdida de cuota de mercado en todos los frentes posibles. A pesar de las fusiones, de fomentar el autoservicio para ingresos automáticos, de la banca on line, la industria bancaria pierde terreno, e internet es la vía para reorientar su situación competitiva. Es cierto que la incorporación de las nuevas tecnologías de la información al *modus operandi* del sector financiero existe desde hace varios años, bien a traves del tratamiento automatizado de datos (back-office), bien a traves de una automatización interna (banca on-line). Pero tampoco es menos cierto, la necesidad de que las entidades han de adoptar los sistemas informáticos necesarios para preservar la intimidad, y en particular la "privacidad".

Y debido a que el sector crediticio es uno de los más problemáticos en materia de protección de datos de carácter personal, bien por la inclusión indebida de personas en registros de morosos, bien por las consecuencias que tiene el tratamiento automatizado de datos, planteamos una serie de recomendaciones, con el objetivo de que sirva a modo de guía con el que las entidades financieras culminen con el reconocimiento de este derecho, evitando así la consecuente falta de sensibilidad ante su desarrollo y ejercicio, que aún hoy día está presente.

**PALABRAS CLAVE:** Protección de Datos, Entidades financieras, Solvencia patrimonial, Datos bancarios.

**1ª. RECOMENDACIÓN: "*Necesidad de cumplir el deber de secreto en el ejercicio de la actividad bancaria".***

La actividad bancaria implica el manejo de multitud de datos personales, por lo que debería de prestarse una especial atención en la formación del personal en aspectos como el secreto profesional y la confidencialidad, para evitar posibles fugas de información, sobre todo del personal de rotación (becarios en prácticas con estancias de meses en oficinas), cuando dejan de prestar sus servicios. Todo trabajador que comience a prestar servicios para una empresa debería comprometerse por escrito de forma expresa a cumplir con las medidas de seguridad que en esta materia se implanten en la empresa, dentro del respeto y cumplimiento de la LOPD.

Lógicamente, la fórmula más segura y eficaz para lograr este compromiso es incluir una cláusula ad hoc en el propio contrato de trabajo y, para los trabajadores anteriores a la implantación del sistema de protección de datos, la firma de un anexo equivalente. Junto a esta cláusula de compromiso, si la empresa dispone -lo que sería muy recomendable- de alguna clase de manual de concienciación en esta materia, debería hacer entrega del mismo al trabajador justo al inicio de la prestación de servicios y siempre bajo recibí que, a ser posible, conste en el mismo contrato de trabajo. En la práctica, la vulneración de este deber sale airosa por problemas de prueba, por lo que se imponen muy pocas sanciones en este sentido.

En cumplimiento de lo preceptuado en el artículo 10 LOPD, se recomienda incluir en los contratos de trabajo cláusulas relativas al deber de secreto profesional respecto de los datos personales a los que tienen acceso los empleados como consecuencia de su actividad y al deber de guardarlos, ya sean los propios empleados de la entidad como los empleados de las empresas prestatarias de servicios para la entidad con acceso a los datos personales de los clientes.

A pesar de que se predica la buena fe contractual, básica en toda relación laboral, ello no es garantía suficiente de cara a garantizar la protección de los datos de carácter personal:

- Porque se considera que se ha transgredido la buena fe contractual cuando se produce una violación de los deberes de fidelidad, pues el empleado de banca puede ser fiel y al mismo tiempo incumplir con los deberes de protección de datos personales.
- Aunque no tiene que ser una transgresión dolosa, pues basta la concurrencia culpable, el trabajador tiene que ser consciente de su conducta

vulneradora y, sin embargo, esa consciencia falta en la mayoría de las veces, cuando se incumple la normativa de protección de datos personales.

- Para poderse apreciar la transgresión de la buena fe contractual, hemos de tener siempre muy presentes el cargo que ocupa el trabajador, desde empleado hasta cargo directivo, y sus circunstancias personales; mientras que el cumplimiento de las medidas para la protección de datos personales es un aspecto marcadamente más objetivo y en el que el cargo o las circunstancias personales pueden agravar o atenuar las consecuencias con respecto a terceros, pero no en el seno de la empresa.
- Porque la confidencialidad que se presume, y que en determinados cargos o puestos se pacta incluso por escrito, no suele referirse al ámbito de los datos personales sino más bien a los económico-empresariales (es común que cuando las empresas, sobre todo de gran tamaño, facilitan sus documentos financieros y contables a las entidades con el fin de que analicen una posible operación de crédito, se acompañe a los mismos un modelo de recibí con la cláusula de compromiso de confidencialidad).

Cabe matizar que el empleado de banca suele desconocer las consecuencias derivadas de un uso poco adecuado de los datos de carácter personal de los clientes, sin tener en cuenta que se manejan datos objeto de protección; y no hay que olvidar que este uso inadecuado conlleva infracciones y sanciones a las que tendrá que hacer frente la empresa únicamente, y no el trabajador, a diferencia, por ejemplo, del tema de la prevención de blanqueo de capitales de origen criminal, donde ambas partes serían responsables.

En la práctica, la vulneración de este deber sale airosa por problemas de prueba, por lo que se imponen muy pocas sanciones en este sentido. Es frecuente que el empleado de banca comunique los datos de un fallecido a un heredero avispado, y que dicha comunicación sea denunciada por otro. No surge aquí problema alguno, dado que la LOPD tiene por objeto la protección de datos personales de personas físicas, y el art. 30 Código Civil señala que la personalidad civil se extingue por la muerte de las personas.

En otro sentido, la AEPD no estima la reclamación por la denegación del derecho de acceso del reclamante a los datos de su causahabiente contenidos en los ficheros de una entidad bancaria (estimó que es un derecho personalísimo que se extingue con la muerte de su titular y, por tanto, la petición formulada por el reclamante no puede atenderse por cuanto se refiere a un derecho sobre el cual no ostenta la titularidad.

**2ª. RECOMENDACIÓN.- "*No entorpecer el ejercicio de los derechos de acceso, rectificación y cancelación".***

Cuando la entidad financiera le ceda a otra empresa los datos personales de un cliente con el propósito de reclamar impagos, o para realizar un *scoring* de su solvencia financiera, hay que tener presente que habrá que sistematizar los supuestos que legitiman la cesión de datos, pues el afectado no puede ser privado de conocer aquellos datos que puedan tener alguna incidencia en sus derechos, y máxime si solicita acceso a los mismos al responsable del fichero.

Así mismo, no cabe la inserción de datos en un fichero de morosos, a pesar de estar saldadas las deudas, por lo que una vez cancelada la deuda, e inscrita la misma en escritura pública, "se tendrá que observar una especial diligencia para mantener los datos al día", para evitar el menoscabo que para la imagen y el prestigio de la persona supone figurar indebidamente en un fichero de solvencia patrimonial y crédito. El responsable del fichero tiene la obligación de actualizar de oficio la información cuando tenga conocimiento de su inexactitud bien directamente, bien atendiendo las solicitudes de cancelación de los afectados.

**3ª. RECOMENDACIÓN.- "*Obligación de acreditar el consentimiento de los interesados para el tratamiento y cesión de sus datos*".**

Con el objetivo de no recibir publicidad no deseada, se han de promover los ficheros de exclusión, a los que podrán incorporarse voluntariamente los clientes que no deseen que sus datos bancarios sean cedidos a otras empresas del grupo, o terceras empresas con fines comerciales, o simplemente para verificar o confirmar datos de un cliente, que supuestamente es cliente común. En este sentido se estima conveniente introducir una casilla en el propio contrato que permita la posibilidad de oponerse a dicha cesión.

En los supuestos de fusiones o absorciones de entidades, no se exige consentimiento, pero existe el deber de informar a los interesados de forma expresa, precisa o inequívoca, y en plazo de 3 meses; en caso extremo, cabe solicitar a la AEPD la exención del deber de informar "cuando resulte imposible o exija esfuerzos desproporcionados", por el elevado número de interesados o antigüedad de los datos, y siempre que se arbitren otras medidas sustitutivas. De conformidad con el artículo 19 RLOPD, en los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la LOPD.

En estos tiempos de crisis, cobran actualidad las operaciones de fusiones o absorciones entre empresas, y como no, entre entidades financieras. Desde el punto de vista del interesado (clientes, empleados, terceros, etc.), sus datos personales se trasladan a unos ficheros cuyo titular ha cambiado, lo que en principio tendría la consideración de cesión o comunicación de datos personales y se debería requerir la autorización del interesado. Pero junto a esta regla general, la excepción es la prevista en el citado artículo que establece que en los casos de

operaciones de índole societaria contempladas en el Derecho mercantil en los que se produzca una variación del responsable del fichero, no existe cesión de datos. Así pues, tanto el anterior como el nuevo responsable del fichero se liberan de la obligación de contar con el consentimiento del interesado cuyos datos son objeto de comunicación. Ahora bien, en ningún caso exime del cumplimiento del deber de información, que se llevará a cabo según lo establecido en el artículo 5 de la LOPD.

El nuevo titular deberá informar a todos los interesados, de forma expresa, precisa e inequívoca, y en plazo no superior a 3 meses de: la razón social y domicilio del nuevo responsable del fichero, explicando los motivos por los que se ha producido la comunicación de datos; la finalidad y posibles cesiones de los datos personales mantenidos en el fichero; y la posibilidad y mecanismo de ejercicio de los derechos de acceso, rectificación, cancelación y oposición ante el nuevo titular.

Respecto a las posibles dudas sobre la inclusión indebida en ficheros de morosidad (errores datos), el responsable del fichero común ha de acreditar el requerimiento de pago al deudor, previo a su inclusión en un fichero de solvencia patrimonial, mediante la constancia de la concreta notificación al afectado en un domicilio válido (no valdría la típica comunicación telefónica que se suele hacer en banca para estos casos). Si el deudor niega haber recibido el requerimiento, recae sobre el responsable del fichero la carga de acreditar la comunicación sin que sea suficiente, a tal efecto, la mera acreditación de su envío.

En otro sentido, es válido que las entidades financieras cedan a la Seguridad Social los datos necesarios para el reintegro de prestaciones indebidamente satisfechas (un ejemplo muy común es el abono indebido de prestación de jubilación de persona fallecida recientemente), o a la Agencia Tributaria. A solicitud de la Confederación Española de Cajas de Ahorro, se analiza en el informe 72/06 la procedencia de la comunicación por una Caja a una Diputación Provincial de los domicilios efectivos de determinados deudores, incursos en procedimientos de apremio para la efectividad de las deudas tributarias, considerándose que revistiendo tales datos trascendencia tributaria la cesión se encuentra amparada en el art. 93.1 de la Ley General Tributaria.

**4ª. RECOMENDACIÓN.- "*Evitar los 3 riesgos potenciales respecto a la creación, mantenimiento y posterior tratamiento de los datos de estos ficheros por las entidades acreedoras*".**

**a. Comunicación o cesión de datos a terceros.** Es frecuente entre empresas dedicadas a la actividad de financiación, la comunicación o cesión de datos obtenidos de ficheros sobre solvencia patrimonial y crédito a terceras empresas, de forma que dicha comunicación pueda ser considerada ilícita, al no ser consentida por los afectados. Los afectados en el ejercicio del

derecho que les asiste de poder acceder y consultar los ficheros comunes, pueden comprobar que hay una entidad con la que no mantienen relación, que ha consultado el fichero común y obtenido información sobre su persona.

**b. Falta de actualización de los datos que conserven y constancia del "saldo cero".** Cuando una entidad acreedora hace una consulta a un fichero común, y recibe una gran cantidad de datos, existe el riesgo de falta de actualización de los mismos que afecta a la calidad. Existen dos formas de comunicación de datos a las entidades asociadas o afiliadas: la consulta singular y la obtención de una copia completa del fichero. En este sentido, la AEPD establece que deberán cumplirse las siguientes recomendaciones:

1ª) Garantizar que todas las copias de los ficheros existentes en cada entidad informante sean idénticas.

2ª) Habilitar los procedimientos necesarios para garantizar que a los afectados se les informa de forma cabal y actualizada de todos los destinatarios de la información contenida en el fichero.

3ª) Adoptar todas aquellas medidas que impidan la existencia de copias de dichos ficheros en manos de personas físicas o jurídicas no autorizadas a acceder a las mismas.

**c. Uso de aplicaciones informáticas para la gestión de créditos (*scoring*).** Se trata de una práctica basada en unas herramientas informáticas que incorporan una serie de factores de riesgo, cuya adecuada combinación entre sí ofrecen como resultado una puntuación de la calidad crediticia de la operación a realizar con el cliente, y en este sentido los afectados tienen los siguientes derechos:

1º) No verse sometido a decisiones con efectos jurídicos sobre ellos, que se basen únicamente en un tratamiento de datos personales destinados a evaluar determinados aspectos de su personalidad.

2º) Impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

3º) Obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizado en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

**5ª. RECOMENDACIÓN.- "*Necesidad de adoptar las oportunas medidas de seguridad".***

Se ha de evitar el hallazgo de documentación personal, como extractos bancarios, en lugares públicos (frecuentemente, vemos en prensa casos en este sentido, pues las empresas de limpieza se limitan a depositar la bolsa de basura, que contiene los documentos que cada empleado ha tirado a su papelera, al contenedor). Las entidades financieras han de implementar el nivel medio de seguridad, como la destrucción de los documentos que se generan por parte de

cada empleado. Y es aconsejable que formalicen con la empresa de limpieza un documento no solo de confidencialidad, sino de tratamiento de los documentos.

**6ª. RECOMENDACIÓN.- "*Ante los troyanos bancarios... ¡seguridad!"***

En torno a los delitos económicos en internet, día a día las prácticas para robar datos bancarios en la red son más sofisticadas. El *phishing* (correos engañosos y servidores fraudulentos para conseguir las claves de acceso a cuentas, o el número de la tarjeta de crédito) cede terreno a los troyanos (programas camuflados dentro de otros aparentemente útiles e inofensivos) que se instalan en el ordenador del afectado para capturar sus datos.

Podríamos confeccionar un catálogo de consejos de seguridad para frenar esta situación pues es cierto que las entidades financieras insisten en que nunca solicitan datos sensibles a través de internet. Pero no es menos cierto el constante aumento de correos electrónicos supuestamente remitidos por la Agencia Tributaria, y por entidades financieras. La tasa del *click*, es decir la proporción de destinatarios que pican y pulsan en el vínculo con el ratón, se sitúa en torno al 3% (y con solo lograr el 1% los ciber-delincuentes hacen negocio).

Así pues, convendría tener siempre en cuenta estos consejos de seguridad:

1º) No abrir correos electrónicos supuestamente enviados por una entidad financiera, incluso de las que no se es cliente.

2º) No abrir archivos adjuntos que tienen un origen desconocido.

3º) No utilizar claves fácilmente deducibles, como nombre o fecha de nacimiento.

4º) No responder a mensajes que pidan información inmediata ante el cese de actividades financieras.

5º) No dar datos personales ni códigos de acceso nunca.

6º) No confiar en supuestas campañas promocionales.

7º) Tener instaladas las oportunas actualizaciones del sistema operativo y del navegador.

8º) Informarse sobre la seguridad en el uso de internet.

9º) Instalar programas antivirus y antiespías, y que estos cortafuegos estén continuamente actualizados.

10º) No entrar en la web del banco mediante enlaces de otras webs.

11º) No apuntar claves de acceso, firmas electrónicas o similar en ningún sitio, sino que conviene memorizarlas.

12º) No atender correos electrónicos en idiomas que el usuario no hable.

13º) Usar un proveedor de acceso a internet que implemente tecnologías y políticas *anti-spam* y *anti-phising*.

14º) No llevar a cabo transacciones financieras en lugares públicos con acceso a internet para muchas personas (cibercafés).

En definitiva, ante el empleo de estos troyanos bancarios, las entidades financieras comienzan a dar cobertura y protección, ante la posibilidad de que un cliente se vea afectado por un vaciado de cuentas o el robo de las claves de la banca *on-line*, mediante un sistema de alertas.

**7ª. RECOMENDACIÓN.- "*Necesidad de un manual de recobros con el fin de garantizar el respeto al honor y la intimidad de los deudores recobrados".***

Hay que dialogar sin alzar la voz. Se dice que quien gana la batalla de la discusión, pierde la del cobro. Las entidades financieras suelen ser flexibles a la hora de renegociar las condiciones, alargando los plazos de cobro, dejando unas cuotas más asequibles.

Ante la inexistencia en España de una formación adecuada para todos aquellos dedicados a la gestión del recobro, debido a que suele ser gente inexperta con un alto porcentaje de rotación, conciben su trabajo no como una profesión, sino como una mera actividad laboral de carácter puntual.

¿Y porque no se regula la actividad de la gestión de recobros, y la reclamación extrajudicial de deudas?, ¿Hasta cuando esta ausencia de Ley? ¿Hasta qué punto un deudor ha de soportar amenazas e insultos telefónicos; o, llegado el caso, visitas personales, a familiares y a vecinos?

Las entidades financieras no deberían delegar a ninguna empresa la delicada tarea del recobro, pues actualmente este hecho roza el acoso en su más amplia acepción. Ante estos casos, se aconseja denunciar el caso ante la Agencia Española de Protección de Datos y presentar la oportuna denuncia ante la Comisaría de Policía.

Las situaciones de crisis, como la actual, provocan numerosos impagos y estos a su vez generan morosos, lo que dispara significativamente el recobro. No nos equivocamos al señalar que, por un lado, están los ciudadanos que atraviesan una situación económica delicada, apurada; y, por otro, los "morosos profesionales"; pero ello, no es justificación para que a la hora de localizar al moroso se viole la normativa en materia de protección de datos de carácter personal.

**JOSÉ ANTONIO GONZÁLEZ MARTÍNEZ:** Diplomado en Graduados Sociales en 1993 y Licenciado en Derecho en 1999 por la Universidad de Alicante. Tiene realizados los Cursos de Doctorado en "El Derecho y la Justicia", así como ha obtenido el DEA por la UMH. Durante el periodo 2000-2008 ha trabajado en banca desempeñado funciones como Gestor de Banca, Subdirector y Director, actualmente en excedencia. Es Profesor Asociado de la Escuela Universitaria de Relaciones Labores de Elda, adscrita a la Universidad de Alicante. Y ha participado como autor y coautor en varios libros, capítulos de libros, artículos, e impartido diversos cursos, seminarios y conferencias.

Dirección correo electrónico: jantonio.gonzalez@ua.es