



Expediente N°: E/07631/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **BANKIA, S.A.**, en virtud de la denuncia presentada por **C.P. XXXX**, y en consideración a los siguientes

HECHOS

PRIMERO: Con fecha 30/05/2014 ha tenido entrada en la Agencia Española de Protección de Datos (AEPD) un escrito de **C.P. XXXX**, (en lo sucesivo la denunciante) en el que manifiesta que los nuevos programas informáticos SEPA de BANKIA, relativos a la utilización del código IBAN en las transacciones nacionales entre cuentas corrientes, suponen una invasión en los sistemas operativos de los usuarios. Los programas informáticos que a este respecto ofrece BANKIA –que son para generar recibos, nóminas y transferencias bancarias- necesitan modificar distintos archivos de los sistemas operativos de los ordenadores. Al ser los mencionados programas susceptibles de alojar información personal dentro de los ficheros de los sistemas operativos, la información personal y privada de los usuarios podría estar expuesta a virus y demás situaciones no deseadas. En definitiva, la denunciante considera que el citado programa podría poner en peligro la confidencialidad de los datos bancarios e identificativos de los usuarios.

SEGUNDO: Tras la recepción de la denuncia, la Subdirección General de Inspección de Datos realizó actuaciones encaminadas al esclarecimiento de los hechos teniendo conocimiento de los siguientes extremos que constan en el Informe de Actuaciones Previas de Inspección que se reproduce:

<<ANTECEDENTES

*Con fecha de 30 de mayo de 2014 tiene entrada en esta Agencia un escrito de **C.P.XXXX** en el que declara que como consecuencia de la aplicación de las normas SEPA (básicamente utilización del código IBAN en las transacciones nacionales entre cuentas corrientes, de ahorro, etc.) se ha procedido a modificar el programa informático de generación de recibos, nómina, transferencias, etc (no on-line) resultando que al instalarlo en los computadores personales de los usuarios, se procede a modifica distintos archivos de los sistemas operativos y si no se modifican el aplicativo no funciona o no funciona correctamente (esto ha sido probado en cuatro ordenadores, entre pc y portátiles).*

Con ello entienden que los nuevos programas de SEPA de Bankia resultan invasivos en los sistemas operativos de los usuarios y por ello pueden ser susceptibles de alojar información personal dentro de los ficheros de los sistemas operativos y por

consiguiente estar la información personal y privada expuesta a virus, troyanos y demás situaciones no deseadas.

Solicitan a la agencia que haga los esfuerzos a través de una consulta, previa denuncia para modificar el programa de aplicación SEPA, en el sentido que la regla general o única es que no fuera invasivo, de tal forma que se pudiera aplicar sin modificar ficheros de los sistemas operativos e incluso que fuera operativo en linuxs, Ubuntu, etc y sobre todo que funcione de forma independiente en memorias extraíbles o discos duros externos a fin de garantizar la confidencialidad de los datos bancarios e identificativos de los usuarios y sin dejar rastros dentro de los sistemas operativos.

ACTUACIONES PREVIAS

Con fecha 30 de enero de 2015 se solicita a Bankia lo siguiente:

“Como consecuencia de la aplicación de las normas SEPA, se ha procedido a modificar el programa informático de generación de recibos, nóminas, transferencias, etc (no on-line) resultando que al instalarlo en los computadores personales de los usuarios se procede a modificar distintos archivos de los sistemas operativos y si no se modifican el aplicativo no funciona correctamente”

Con ello el denunciante entiende que los nuevos programas SEPA de Bankia resultan invasivos en los sistemas operativos de los usuarios y por ello pueden ser susceptibles de alojar información personal dentro de los ficheros de los sistemas operativos y por consiguiente estar la información personal y privada expuesta a virus, troyanos y demás situaciones no deseadas.

Se solicita información y documentación que aclare lo manifestado por el denunciante”.

De la información aportada se desprende lo siguiente:

En el caso de Bankia, existen dos opciones para que los clientes que realizan operaciones de pago al amparo de la normativa SEPA generen los ficheros necesarios para que Bankia realice dichas operaciones de pago.

1. Descarga de un programa para instalar en el PC del cliente a nivel local

Existen actualmente en el mercado multitud de programas que los clientes pueden comprar en cualquier tienda especializada. Cada programa genera un fichero informático, que contiene la información de las órdenes de pago según la estructura que precisan las Entidades Bancarias para realizar dichas ordenes al amparo de la normativa SEPA. Esta estructura viene determinada por la normativa interbancaria correspondiente aplicable según la orden de pago de que se trate. Posteriormente, una vez generado el fichero el cliente lo envía a su Entidad Bancaria por el conducto que haya pactado con ésta (acudiendo a la oficina, por oficina internet...).

En el caso de Bankia, los clientes pueden o bien usar uno de los programas existentes en el mercado o bien descargarse gratuitamente el programa "Generador de ficheros Bankia" (que es una versión comercial con la única modificación de contener un directorio de oficinas de Bankia, disponible para descarga tanto en bankia.es como en la OIE).

Con este programa los clientes pueden generar en local las remesas masivas: Nóminas, Recibos, Anticipos de crédito, Pago a Proveedores, Confirming y Consulta de ficheros N43, con los datos de proveedores, empleados.... responsabilidad del cliente.

En cuanto a las especificaciones técnicas del programa, este instala en el PC del cliente las librerías necesarias para su funcionamiento en el sistema operativo, como cualquier otro programa que se quiera instalar (Word, Contaplus, un editor de texto, etc.). Es una mecánica de uso común en la distribución de software, estando controlado el sistema de instalación por Windows.

Por otro lado, efectivamente estos programas (los de Bankia y los de cualquier otra entidad o cualquier otro existente en el mercado) que sean considerados "locales", funcionan con una base de datos para almacenar los datos que el propio cliente/usuario introduce.

Esta base de datos es la estándar del mercado MS Access, cifrada bajo la propia tecnología de Microsoft y protegida con contraseña, lo cual reduce drásticamente la posibilidad de robo de datos, al estar estos cifrados. Aportan las DLL y OCX que utiliza el generador local de Bankia.

Por otro lado, manifiestan que el cliente cuando se instala la aplicación de "Módulos Locales", cuando encuentra una dll o OCX (necesarias para la instalación) existente en el equipo, pregunta al usuario si desea actualizar dicha librería, por lo tanto en todo momento el cliente tiene la información y la autorización para actualizar o no la instalación del Software. Hay que resaltar que la no actualización o instalación de alguna librería implica en el mal funcionamiento de la aplicación ya que todas son necesarias para la correcta ejecución.

Adicionalmente se pone por parte de Bankia a disposición de los usuarios unas guías rápidas, tanto para recibos, nóminas, etc, que guían al usuario en la instalación, configuración, del programa y en la creación y exportación del fichero. Adjuntan copia de las guías rápidas, que se encuentran disponibles para descarga en los enlaces:

- Desde la propia Oficina Internet Empresas (O.I.E.), en la opción de Ficheros del menú principal, pestaña de Software/Utilidades, una vez haya accedido.
Desde el espacio DEMO de Oficina Internet Empresas (O.I.E.), accediendo por el portal de Bankia Empresas (empresas.bankia.es/DemoOIE) en la opción. Programas que aparece a la derecha en el espacio DEMO.
- Desde aquí mismo pulsando sobre el enlace: Descargar programa Generador de Ficheros Bankia v.I (con ayudas) (Se incluyen en el fichero de descarga los manuales de ayuda disponibles)

Una vez el cliente ha completado los datos que le solicita el programa, genera el fichero y remite la información a Bankia (o a cualquier otra Entidad Financiera) a través de la OIE (que en estos casos solo funciona como "canuto" de envío), que dispone de las medidas de seguridad oportunas, o llevando el fichero a una oficina (en un CD, usb...). Aportan impresión de las pantallas existentes en la OIE para el envío de esta información.

2. Remisión de la información a través de la Oficina de Internet Empresas

Manifiestan que la operativa más común entre sus clientes es la remisión de los datos a la Entidad a través de la opción Cobros y Pagos de la OIE, que no requiere instalación a nivel local en el equipo del usuario y la información necesaria para realizar las órdenes de pago permanece en los servidores Bankia.

Este generador web integrado en Oficina Internet Empresas (OIE) (Opcidn: ficheros) permite ampliar el límite de registros hasta 2.000 y no supone la instalación de un programa en local en el PC del cliente. Aportan impresión de pantallas de la versión demo de la OIE donde se puede ver la funcionalidad.

Independientemente de lo anterior, Bankia entiende que la responsabilidad de "blindar" los equipos de los usuarios contra virus, hackers y troyanos no corresponde a Bankia S.A., sino que cada sistema es responsabilidad de su propietario. Afirmar lo contrario supondría, por ejemplo, denunciar a Microsoft porque su programa WORD instala librerías en el sistema operativo, y si entra un virus puede robar datos de carácter personal almacenados.>>

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 artículo 9.1 de la LOPD, bajo el epígrafe "seguridad de los datos", se refiere a la obligación que incumbe al responsable del fichero, y, en su caso, al encargado de tratamiento, de "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".

El precepto añade a continuación:

"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 tratamientos, 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 Real Decreto 1720/2007, por el que se aprueba el Reglamento de Desarrollo

de la LOPD (RLOPD) dedica el Título VIII, artículos 79 a 114, a las medidas de seguridad en el tratamiento de los datos.

II

La denuncia que nos ocupa plantea la posibilidad de que se vean sometidos a *“virus, troyanos y demás situaciones no deseadas”* los datos bancarios e identificativos de los usuarios como consecuencia de la instalación del programa informático de BANKIA, que ha sido modificado a raíz de la aplicación de las normas SEPA y que se usa para la generación de recibos, nóminas, transferencias etc.

La Inspección de Datos de la AEPD dirigió un requerimiento informativo a BANKIA y de su respuesta y se concluye lo siguiente:

BANKIA ofrece dos opciones para que los clientes que efectúen operaciones de pago a través de la entidad, al amparo de la normativa SEPA, generen los ficheros necesarios para que la entidad financiera lleve a cabo las operaciones:

Una posibilidad es remitir los datos a la entidad denunciada a través de la opción cobros y pagos de la Oficina Internet Empresas (OIE), lo que no requiere instalar un programa en el PC del cliente.

La segunda opción es descargar un programa que se instala en el PC del cliente a nivel local. La denunciada indica que los clientes pueden usar tanto alguno de los numerosos programas que se comercializan en el mercado como descargar gratuitamente el programa “Generador de ficheros de BANKIA”, que no es sino una versión comercial con la especialidad de incluir un directorio de las oficinas de la entidad financiera.

En relación con este programa precisa que instala en el PC del cliente, al igual que cualquier otro programa que se quiera instalar, las librerías necesarias para su funcionamiento en el sistema operativo. Y que tanto el programa de BANKIA como cualquier otro que exista en el mercado funcionan con una base de datos para almacenar los que el propio cliente/usuario introduce. Base de datos que es la estándar en el mercado MS Access, que está cifrada por la tecnología Microsoft y protegida con contraseña.

Sin perjuicio de lo anterior, la entidad advierte que es responsabilidad del usuario propietario de un equipo informático y no de BANKIA “blindar” estos equipos frente a virus, hackers o troyanos.

A la luz de la respuesta ofrecida al requerimiento informativo de la AEPD por la entidad denunciada y de la documentación aportada con ella, se concluye que el programa de BANKIA para llevar a cabo operaciones de pago al amparo de la normativa SEPA tiene las mismas garantías de seguridad que cualquiera otro que se comercializa actualmente por lo que no existen indicios de que el citado programa vulnere la normativa de protección de datos. Por otra parte, como se recoge en el artículo 9 de la LOPD, el cliente de BANKIA que sea responsable de un fichero con datos personales tiene la obligación de adoptar las medidas que garanticen la seguridad de los datos objeto de tratamiento. Las consideraciones expuestas conducen al archivo de las actuaciones de investigación practicadas.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

- 1. PROCEDER AL ARCHIVO** de las presentes actuaciones.
- 2. NOTIFICAR** la presente Resolución a **BANKIA, S.A.** y a **C.P.XXXX**.

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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos