Expediente Nº: E/06896/2016

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 denuncia presentada por D. ***B.B.B.***, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 01/12/2016, tuvo entrada en esta Agencia escrito de D. ***B.B.B.*** (en lo sucesivo el denunciante), en el que formula denuncia contra la entidad BANKIA, S.A. (en lo sucesivo BANKIA) por haber posibilitado el acceso por parte de terceros a la información relativa a su cuenta bancaria, cuyo código internacional de cuenta bancaria (IBAN) fue copiado por el propio denunciante desde la web de la entidad, a la que accedió mediante código de usuario y contraseña, e insertado posteriormente en un correo remitido por el mismo a la entidad en la que presta servicios como empleado en fecha 27/11/2015. El resultado de esta acción, según el denunciante, fue que utilizando el citado código IBAN desde el correo electrónico de 27/11/2015, simplemente clicando sobre el código, se podía acceder a todos los datos del denunciante.

Añade que, por este motivo, acudió a una sucursal de BANKIA, en la que se comprobó que podía accederse a sus datos utilizando el número de cuenta copiado. El mismo día realizó un escrito de reclamación, aunque parecía que el fallo había sido subsanado. Al no obtener ninguna respuesta por parte de BANKIA, en septiembre de 2016, reiteró la reclamación, la cual fue rechazada por la entidad argumentando que intentó reproducir la incidencia, sin que resultara posible acceder a la información del cliente.

Entre otra, con su denuncia anexa la siguiente documentación:

Copia del correo electrónico remitido desde la dirección ***C.C.C.***, a la dirección ***D.D.D.***, que incluía un número de IBAN, de fecha 27/11/2015, a las 9:47.
Escrito de reclamación presentado ante BANKIA en fecha 27/11/2015 por los hechos mencionados.
Copia de un correo electrónico remitido desde la dirección ***E.E.E.*** a atencionalcliente@bankia.com, de fecha 09/09/2016, en el que se reitera la reclamación al no haber obtenido respuesta.
Escrito de contestación de BANKIA, de fecha 08/11/2016, desestimando la reclamación al no poder reproducir la incidencia. Se indica que no se puede acceder a la información de clientes sin pasar por el proceso de autenticación.
Declaración del XXX de la compañía ***GRUPO PRILUX ILUMINACIÓN S.L.U.***, en la que manifiesta que, a las 9:47 horas del 27/11/2015, recibió un correo electrónico del denunciante en el que se adjuntaba un número de cuenta bancaria y al clicar se accedía a los datos personales del denunciante sin ningún proceso de autenticación.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos

procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

A. Con fecha 21/02/2017 se requiere información a BANKIA y, de la respuesta recibida en fecha 20/04/2017, se desprende:

1. El acceso a la Oficina Internet de Particulares de BANKIA se realiza mediante la autenticación del usuario a través de un código de usuario (generalmente el DNI/NIE) y una clave de acceso.

BANKIA manifiesta que previamente al acceso a través de la web, el cliente debe tener contratado el servicio de Oficina de Internet o del Servicio Multiacceso que permite utilizar la misma clave para la Oficina de Internet, la Oficina móvil, Cajeros…
BANKIA manifiesta que no es posible realizar sesiones simultáneas desde diferentes dispositivos o navegadores y solo es posible mantener una sesión única por cliente.

2. BANKIA manifiesta que el número de cuenta bancaria no corresponde a un código de usuario por lo que no es posible acceder a ninguna información utilizando dicho el número de cuenta, ni siquiera por un cliente autenticado y en el marco de una sesión activa, ya que únicamente se puede acceder a los movimientos de una cuenta bancaria utilizando los elementos activos en la Oficina de Internet que generan una dirección URL con un “ALIAS” que permite la navegación.

BANKIA manifiesta que, fuera de una sesión activa con autenticación del usuario, la URL accede únicamente a la pantalla que solicita la identificación del usuario.

3. Respecto de los accesos a la cuenta bancaria del denunciante en fecha 27/11/2015, BANKIA ha aportado fichero EXCEL e impresión de los accesos registrados en dicha fecha, que corresponden a la misma dirección IP y en horas comprendidas entre las 01:59:13 y las 09:55:41. Manifiestan al respecto que todos ellos se realizaron en el marco de una sesión con una autenticación previamente establecida.

4. En relación con las reclamaciones efectuadas por el denunciante, BANKIA manifiesta que, en fecha 27/11/2015, el cliente se persona en una sucursal informando de los hechos denunciados. Dicha sucursal contacta con el Departamento de Seguridad Informática notificando la incidencia y posteriormente el cliente envía un correo electrónico a la sucursal indicando que el fallo ha sido corregido.

BANKIA ha aportado copia del mencionado correo remitido el 27/11/2015 a las 13:54.
BANKIA ha aportado copia de las reclamaciones planteadas por el denunciante en relación a estos hechos, en fechas 27/11/2015 y el 09/09/2016, en la que indica que no ha recibido contestación. La entidad bancaria remite escrito de contestación, en fecha 08/11/2016, informando que es necesaria la autenticación del cliente para el acceso a cualquier dato y que la incidencia puesta de manifiesto no ha podido ser reproducida.
Con fecha 17/11/2016, el denunciante interpone nuevamente la reclamación siendo contestado por BANKIA en fecha 23/11/2016 en los mismos términos.
BANKIA manifiesta que tras recibirse la primera reclamación se intentó reproducir la incidencia concluyendo que no era posible acceder a la información de un cliente sin pasar previamente por el proceso se autenticación.

B. En el informe elaborado por BANKIA sobre la reclamación formulada por el denunciante se señala que el número de cuenta no es un código de usuario y que los hipervínculos que subyacen tras este número tiene el formato “***URL.1”, de modo que al insertar el número en un documento

de texto el hiperenlace no tiene la información relativa al número.

Con fecha 28/09/2017, por la Inspección de Datos se verifica que a través de la URL "***URL.1", sin incluir un valor en el campo "Alias", dicha URL redirige a la dirección "https://www.bankia.es/es/particulares/acceso-clientes", en la que se solicita la identificación y autenticación.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora 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 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

III

El artículo 9 de la LOPD establece:

"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 trascrito 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.

Los artículos 91 y 93 del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto

1720/2007, de 21 de diciembre, aplicables a todos los ficheros y tratamientos automatizados, establecen:

"Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio".

Este artículo desarrolla las previsiones que deberá establecer el responsable del fichero para garantizar que los usuarios con accesos a datos personales o recursos, por haber sido previamente autorizados, sólo puedan acceder a tales datos y recursos. Para ello es necesario que se implanten mecanismos de control para evitar que un usuario pueda acceder a datos o funcionalidades que no se correspondan con el tipo de acceso autorizado para el mismo, en función del perfil de usuario asignado.

"Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".

El artículo 5.2.b) del citado Reglamento define la autenticación como el procedimiento de comprobación de la identidad de un usuario; y el mismo artículo, letra h), se refiere a la identificación como el procedimiento de reconocimiento de la identidad de un usuario. Corresponde al responsable del fichero o tratamiento comprobar la existencia de la autorización exigida en el citado artículo 91, con un proceso de verificación de la identidad de la persona (autenticación) implantando un mecanismo que permita acceder a datos o recursos en función de la identificación ya autenticada. Cada identidad personal deberá estar asociada con un perfil de seguridad, roles y permisos concedidos por el responsable del fichero o tratamiento.

En definitiva, la entidad BANKIA está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias, y, entre ellas, las dirigidas a impedir el acceso no autorizado

por parte de terceros a los datos personales que constan en sus ficheros.

En el presente caso, se denuncia el acceso por parte un tercero a los datos personales del denunciante, cliente de BANKIA, a través del Área de Clientes habilitada por la misma para que puedan realizarse determinadas gestiones online, utilizando, según manifestó el denunciante, un hipervínculo generado al insertar en un correo electrónico el código IBAN de su cuenta bancaria.

Sin embargo, a la vista de las comprobaciones realizadas, ha quedado acreditado que el área de clientes habilitada a través de la web de BANKIA dispone de las medidas de seguridad establecidas en el Reglamento de desarrollo de la LOPD, incluido un procedimiento de acceso que requiere de un código de usuario y contraseña, distintos para cada cliente, conforme exige la normativa anteriormente reseñada, el cual no se compone con el número de cuenta bancaria.

Así, en este caso, no se advierte una inadecuada implantación de medidas de seguridad, en lo que se refiere al control de accesos y a la identificación/autenticación de los usuarios, por lo que no puede concluirse que BANKIA incumpliera la obligación de establecer las medidas de seguridad adecuadas para impedir de manera fidedigna el acceso a la información registrada en sus ficheros.

Además, no existe evidencia alguna sobre el acceso por un tercero a la información bancaria del denunciante. Según los registros que constan en el sistema de información de BANKIA, los accesos al área personal del denunciante realizados en la fecha señalada en la denuncia se realizaron, en todos los casos, utilizando el par usuario/contraseña correspondiente al mismo, y todos ellos desde la misma dirección IP.

No se trata del acceso por parte de un tercero no identificado ni autenticado que se aprovechara de vulnerabilidades del sistema de información, sino de accesos utilizando el código de usuario y contraseña del denunciante, es decir, por un cliente correctamente identificado frente al sistema de información de BANKIA.

Asimismo, se ha verificado que el hipervínculo que pudiera crearse a partir del número de cuenta conduce a la página en la que se solicita la identificación y autenticación del usuario.

Se ha de tener en cuenta que al Derecho Administrativo Sancionador, por su especialidad, le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad del principio de presunción de inocencia. La presunción de inocencia debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones.

En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *"que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio".* De acuerdo con este planteamiento, el artículo 137.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, vigente en el momento en que presuntamente tuvieron lugar los hechos denunciados, establece que "*Los procedimientos sancionadores respetarán la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario."*

En definitiva, la aplicación del principio de presunción de inocencia impide imputar una infracción administrativa cuando no se hayan obtenido evidencias o indicios de los que se derive la existencia de infracción.

En este sentido y para este caso, se reitera que no se han aportado indicios razonables que permitan establecer que se han producido los hechos denunciados, ya que no se han aportado evidencias ni indicios de los que pueda deducirse que se produjeron los hechos que denuncia, ni las actuaciones de investigación desarrolladas permiten variar dicha conclusión.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a BANKIA, S.A. y a D. ***B.B.B..***

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 Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora 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.

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