BREVE RESEÑA SOBRE EL ACCESO A LA BANCA ELECTRÓNICA

Victor Pablo Conde Prada

INTRODUCCIÓN

Vamos a desarrollar en este articulo los problemas que se pueden plantear en caso de uso fraudulento de los servicios de Banca electrónica. No los vamos a desarrollar de manera exhaustiva, (lo que nos podría llevar cientos de páginas) sino que vamos a ofrecer una pincelada con relación a los problemas que se podrían plantear con relación al acceso de páginas web bancarias.

El principal problema que se deriva en ambos casos es el de la atipicidad. Nos encontramos ante ámbitos y actuaciones que, o bien no aparecen regulados por parte del ordenamiento jurídico, o bien la regulación es escasa y con normas de rango jerárquico "bajo". Y todo ello pese a que la importancia y el uso de la banca a distancia crece y seguirá creciendo en el futuro.

La seguridad aparece configurada como elemento principal, siendo necesario niveles mayores de seguridad, como codificación criptográfica de 128 bits, firmas digitales y procedimientos de autenticación específicos (autenticación basada en fichas o en tarjetas inteligentes, o contraseñas dinámicas).

La autenticación y la validación de la identidad es la principal preocupación pública en Internet, seguida de cerca por los ataques a la seguridad externa e interna, los piratas informáticos, los virus y la denegación del servicio. La seguridad de la red debe garantizar el control del acceso, la confidencialidad y la integridad de los datos, la autenticación, y la ausencia de rechazo.

Los bancos parecen utilizar la seguridad y la confianza como los medios principales para motivar a los clientes para que usen los servicios web que ofrecen, con la finalidad de retener mejor al cliente, a largo plazo.

LA BANCA A DISTANCIA

Actualmente la casi totalidad de bancos tienen páginas web que permiten realizar consultas de los productos bancarios que tiene contratado el cliente e incluso realizar operaciones

bancarias. También existen bancos que carecen de oficinas físicas y gestionan toda su actividad a través de internet. Esto a reportado para el sector bancario y para los clientes grandes ventajas, ya que ha permitido una notable reducción de costes, para los primeros y un mayor servicio para los segundos, al estar el banco operativo las veinticuatro horas del día. No obstante, estos servicios también generan numerosos inconvenientes.

En materia de banca a distancia conviene distinguir dos tipos de accesos por parte del cliente: el acceso a nivel informativo y el acceso a nivel operativo.

Acceso a nivel informativo

Se produce en aquellos casos en los que el Banco facilita al cliente una dirección web en la que, identificándose a través de una clave personal y secreta, va ha poder efectuar consultas sobre los productos que tiene contratados (consultas de saldos y movimientos, de operaciones efectuadas con la tarjeta, de fondos de inversión...)

La petición de claves se debería de realizar en direcciones web seguras del banco, es decir, aquellas direcciones que comienzan por https y que reúnen requisitos básicos de encriptación de datos. Los principales elementos en los que ha de basarse el sistema de seguridad de las entidades financieras son:

Establecimiento de un código de usuario y clave de acceso.

Comunicaciones de forma cifrada (criptografía simétrica criptografía asimétrica o de clave pública 128 bits).

Disponibilidad de un servidor seguro (https).

Certificado personal de firma electrónica o clave de firma (firma electrónica, firma electrónica avanzada y firma electrónica reconocida).

En estos casos el problema que plantearía un uso fraudulento de la clave de acceso afectaría solo al secreto bancario. Nos encontraríamos ante una vulneración del derecho de intimidad personal y de protección de datos de carácter personal. La responsabilidad que podríamos deducir de estos actos, sería, por un lado penal y por otro lado administrativa y contractual.

En el ámbito penal abría que hablar de un supuesto delito del artículo 197 del Código Penal, del que sería responsable el tercero que accede de forma fraudulenta a los datos pero en ningún caso podría desplazarse esa responsabilidad a la entidad bancaria.

La responsabilidad del banco sería administrativa, posible vulneración de las Ley de Protección de Datos de Carácter Personal (Ley 15/1999 de 13 de diciembre) y contractual siempre y cuando pudiéramos hablar de una negligencia en el deber del banco de proteger los datos del cliente.

El cliente tiene la obligación y el deber de custodiar la clave y de no facilitarla un tercero. Por tanto, el banco quedará exento de cualquier responsabilidad si se acreditase la

negligencia del cliente en la custodia de la clave. El problema se plantearía en aquellos casos en los que un tercero a través de procedimientos o programas informáticos consigue infiltrarse en el ordenador de un particular y obtener fraudulentamente las claves. En estos casos derivar toda la responsabilidad al cliente sería del todo incorrecto e inapropiado, pero tampoco podemos exonerarle de toda responsabilidad.

La entidad bancaria debe procurar que el acceso se realice a través de páginas web seguras de tal manera que si no se cumple este requisito u otros requisitos básicos de seguridad (enunciados de forma breve anteriormente), podría exigirse responsabilidad al banco.

Por su parte, el usuario debe acceder a través de ordenadores que sean seguros y fiables, y en este sentido, entendemos que el cliente debe asumir el riesgo derivado de acceder desde equipos de uso publico (cibercafes y similares) o desde equipos privados de riesgo, es decir, aquellos en los que se hayan instalado troyanos virus o programas similares, que permitan a un tercero acceder a los datos personales.

Correspondería a la entidad bancaria, para exonerarse de responsabilidad, la carga de probar que su dirección web es segura y al cliente probar que el equipo desde el que ha accedido es un equipo seguro. No obstante, nos encontramos ante una casuística variada, que podría ofrecer problemas.

Es usual en el clausulado de la mayoría de contratos de banca a distancia que el banco se exonere de responsabilidad en caso de interferencias, omisiones, desconexiones o averías en la red o en los sistemas telemáticos o informáticos. El banco no puede exonerarse completamente de responsabilidad y por tanto, entendemos que las cláusulas de este tipo podrían ser cláusulas abusivas que vulnerarían la Ley de Condiciones Generales de la Contratación (Ley 7/1998 de 13 de abril), o la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios, máxime cuando el Banco de España a través de su Servicio de Reclamaciones ha dejado establecido que “el uso de los nuevos canales de banca no puede conducir a la indefensión de la clientela” (Reclamación nº 3638/01).

Conviene hacer mención al Real Decreto 629/1993, de 3 de mayo, sobre normas de actuación en los mercados de valores y registros obligatorios (artículo 8) que impone la obligación a las entidades bancarias de llevar un registro de las operaciones efectuadas por vía telefónica o electrónica. En este caso, el banco sería responsable del mismo y de los perjuicios que se derivarían de su acceso fraudulento.

Acceso a nivel operativo

Básicamente la problemática sería igual que la examinada en el punto anterior, ya que el acceso a nivel operativo lleva incluido un acceso a nivel informativo, pero con la posibilidad de que el cliente pueda realizar operaciones bancarias mas o menos complejas (transferencias, contratación de tarjetas, compraventa de valores, warrants...).

La diferencia con el acceso a nivel informativo estribaría en el hecho de que puedan efectuarse operaciones, ya que ello añade una mayor complejidad en el sentido que los

perjuicios que pudieran plantearse, en un supuesto de uso fraudulento, ya no son solo de protección de datos, sino patrimoniales.

En la mayoría de entidades bancarias se diferencia el acceso informativo del acceso operativo exigiendo en esté ultimo caso una clave especifica denominada generalmente firma electrónica. La introducción de esta firma electrónica se equipara en el clausulado de la mayoría de contratos de banca a distancia a la firma manuscrita, produciendo por tanto análogos efectos jurídicos.

El cliente tiene la obligación de la custodia de la clave secreta de tal forma que no debe comunicar la misma a un tercero. Sería conveniente que la clave no coincidiera con fechas de nacimiento números de DNI etc... ya que son claves fácilmente deducibles. También tiene el cliente la obligación de acceso y realización de operaciones a través de equipos seguros. En caso de que el cliente sospeche que la clave operativa puede ser conocida por un tercero deberá comunicar está circunstancia al banco. El cliente responde de los perjuicios derivados en caso de que no se produzca tal comunicación. Efectuada esta el banco deberá dar de baja inmediatamente la clave operativa ya que si no la responsabilidad se desplaza a él.

La entidad bancaria tiene la obligación de que la página web sea una página segura, del registro de las operaciones efectuadas informaticamente y de establecer un canal de comunicación que permita al cliente poner de manifiesto de manera inmediata el posible uso o acceso fraudulento por un tercero a la clave de acceso.

En el supuesto de que un tercero acceda de manera fraudulenta a las claves operativas y realice operaciones que causen un perjuicio patrimonial al cliente cometerá un presunto delito de estafa informática (articulo 248.2 Código Penal).

Disponível em:< http://www.porticolegal.com/pa_articulo.php?ref=278 Acesso em.: 03 set. 2007.