XLV ENCUENTRO DE INSTITUTOS DE DERECHO COMERCIAL DE LOS COLEGIOS DE ABOGADOS DE LA PROVINCIA DE LA PROVINCIA DE BUENOS AIRES.

Morón, Abril de 2007

TEMA: RESPONSABILIDAD BANCARIA. BANCA INFORMÁTICA. EL DOMINIO DE LAS PAGINAS WEB DE LOS BANCOS.

AUTOR: *DR. EDUARDO ANIBAL MARSALA*
INSTITUTO DE DERECHO COMERCIAL
"Dr. ANGEL M. MAZZETTI"
COLEGIO DE ABOGADOS DE LOMAS DE ZAMORA.

PONENCIA: La problemática de la forma de la adquisición de la titularidad de los dominios de las páginas web, puede implicar en algunos supuestos, un nuevo supuesto de responsabilidad bancaria, sin perjuicio, que resulta imprescindible una legislación adecuada al respecto.

I.- INTRODUCCION:

El avance de la tecnología informática, la globalización de las transacciones bancarias, su celeridad, la optimización de los servicios y la disminución de los costos, nos introducen en la problemática de la banca informática.

Estos beneficios no pueden obtenerse en desmedro de otro elemento fundamental al objeto-fin de la banca, esto es la "seguridad del sistema".

II.- EL DOMINIO DE LAS PAGINAS WEB

Los dominios de las páginas web, esto es a nombre de que titular –persona física o jurídica- se registra una pagina web, ya que las mismas se conceden a quien primero lo solicita, a cambio del pago de una tasa, sin tomar en cuenta ningún otro factor.

Esta sistematología, no tiene en cuenta varios factores, entre los que cabe mencionar:

1. No se respetan los nombres de las Sociedades regularmente inscriptas.
2. No se respetan los nombre comerciales, marcarios o de propiedad intelectual.
3. Tampoco, el de las personas físicas.

Lo cual, significa que en Internet no se tienen en cuenta otros registros.

Esta situación ha provocado la aparición de lo que se ha denominado "***ciberocupación"***, que constituye una metodología por la cual que muchos oportunistas hayan obtenido nombres de dominio que contienen o están relacionados con marcas famosas o nombres de personas conocidas con la única finalidad de negociarlos posteriormente con los titulares de dichas marcas o de quienes legítimamente tienen derecho al uso de un nombre de dominio a cambio de una contraprestación económica, lo que es aun peor, lo haga como un medio para efectuar fraudes o delitos informáticos.

De tal forma que al ser los nombres de dominio un registro autónomo, no se presentan conflictos entre diferentes nombres de dominio, sino –por el contrario- entre estos y nombres registrados en registros de otra naturaleza, y aún con los de uso publico y notorio.

Esta modalidad de actuación denominada ciberocupación, constituye un delito que debería ser rápidamente legislado, no solo en forma de sanciones punitivas, sino especialmente preventivas, atento al grave perjuicio que se puede ocasionar no ya solo al damnificado, sino a una comunidad de individuos que se pudieran conectar a esa página web, en la creencia que se encuentran haciéndolo a la perteneciente a la empresa determinada y no a una página que ha usurpado el nombre.

Ahora, Qué pasa cuando nos encontramos ante el supuesto de páginas de estas características con nombres de entidades financieras?.

III.- LA USURPACION DEL DOMINIO DE LAS PAGINAS WEB DE LOS BANCOS.

He aquí la primer aclaración: No nos encontramos ante un supuesto de laboratorio, sino ante una situación que se ha dado no solo en nuestro país, sino en todo el mundo.

Así, podemos citar el caso del Banco Río de la Plata S.A., es conocido masivamente y realiza incluso su marketing con el nombre de *"BANCO RIO"*. El banco utiliza el dominio: bancorio.com.ar y se encontró con un aviso en Internet, en el cual se ofrecían a la venta, los dominios: bancorio.com, bancorio.net y bancorio.org, en una evidente maniobra extorsiva.

Otro supuesto, se ha dado con el BBVA Banco Francés S.A. que es dueña de la marca "BANCO FRANCES", registrada en Argentina el 17/08/2000. El nombre de dominio "bancofrances.com" en disputa fue registrado por la entidad. Sin perjuicio de ello, con posterioridad el dominio (al igual que bancofrances.net) aparecen transferidos por medios informáticos a una tercera persona, aún cuando el banco continuaba utilizando el dominio que se encontraba en su servidor. La peligrosidad de la situación en este supuesto es extrema. El banco hoy en día, utiliza el dominio "bancofrances.com.ar".

Otros bancos perjudicados a lo largo del mundo han sido: Banex S.A., Banco de Chile, Banco de Bogotá, Banco Mercantil del Norte.

Ultimamente el Banco de Galicia, ha debido cambiar el dominio de su página web.

Los conflictos que se presentan en estos casos se resuelven ante la Organización Mundial de Propiedad Intelectual.

Pero, la resolución del conflicto puede llegar tarde, y haberse producido un perjuicio a consumidores bancarios.

Como antecedente vale citar la ley 34/2002 de España, en donde se exige una serie de requisitos, a los efectos de evitar la titularización de dominios a favor de aquellas personas que no tienen derecho al uso del nombre registrado marcariamente o de propiedad intelectual.

IV.- SUPUESTOS DE RESPONSABILIDAD DEL BANCO:

Entre los diferentes fraudes que se efectúan por Internet, se pueden mencionar:

SPAM: El correo masivo no deseado.

El SPAM puede definirse como el correo electrónico no solicitado, enviado de forma masiva a múltiples destinatarios. La finalidad del mismo es, generalmente, comercial: publicitar bienes o servicios, ofrecer productos, vender bases de datos, etc. Esta situación trae aparejada la consecuente molestia para los usuarios al descargar sus emails y encontrarse con una gran cantidad de correos electrónicos no deseados, lo que genera una gran pérdida de tiempo, a la vez que se incrementa el tráfico a través de las redes, congestionándolas

HOAX: Engaños.

Se trata de una "broma" o "engaño" . traducción literal del inglés ., generalmente es una falsa advertencia de virus, o de cualquier otro tipo de alerta o de cadena (incluso solidaria), distribuida por email, a través de la cual se pide que el usuario reenvíe a la mayor cantidad de conocidos. En definitiva, son historias inventadas que tienen la finalidad de captar el interés del destinatario. No se trata de un virus porque no cuentan con la capacidad de autoreproducirse.

PHISHING.

El Phishing tiene por finalidad engañar a los usuarios para conseguir datos confidenciales como ser, las claves de acceso a sus cuentas bancarias por Internet. Para ello, el estafador envía miles de correos electrónicos falsos que parecen provenir de sitios web de entidades financieras. A través del mismo se notifica al cliente la necesidad de que confirme información relacionada con su cuenta bancaria, alegando excusas de toda clase como, por ejemplo, modificaciones en el sistema de seguridad, avisos de cancelación de las cuentas si no se procede a la actualización y confirmación de los datos en un corto plazo de tiempo, personalización de cuentas, etc10.

Los mensajes suelen contener el logotipo de la entidad bancaria y demás signos distintivos para aumentar la confusión del cliente. El mensaje contiene un link a un sitio web, que en apariencia es el de la entidad de la cual es cliente, pero en realidad conduce a un sitio falso. Una vez que el usuario está en el sitio falso, le es requerido que ingrese su información personal sin saber que se transmitirá directamente al ciberdelincuente, quien la utilizará para transferir el dinero a su cuenta, realizar pagos, etc.

La fórmula del engaño: SPAM+HOAX=SCAM. La actitud de las entidades financieras frente a esta amenaza.

El método conocido como SCAM utiliza aspectos propios del SPAM, en cuanto al envío masivo de emails; y otros propios del HOAX, pretendiendo engañar o timar al cliente de una entidad bancaria para apoderarse de sus datos personales. Así, podemos definirlo como un fraude, que utiliza para su difusión las técnicas masivas del SPAM, y para perpetrar sus fines ilícitos, el abuso de la buena fe (tal como los HOAX) apoyándose en fallos o vulnerabilidades que se presentan en los programas utilizados para la navegación en Internet

Por este sistema fraudulento, el usuario recibe un correo del Banco idéntico o muy semejante al recibido usualmente, en donde se le especifica que se han aumentado las cuestiones de seguridad de la página web y se le solicita que ingrese a la página del banco para modificar su clave. El usuario por medio del vínculo que recibe en el propio mail, ingresa en la página, que es igual a la del Banco. Sin embargo no percibe, que en lugar de ingresar a “e-galicia.com.ar” -página oficial del Banco Galicia- ingresa a “i-galicia.com.ar” que corresponde a un dominio que fuera ocupado por un individuo que no tiene vinculación alguna con el Banco.

En los supuestos que se han presentado los Bancos se han logrado eximir de responsabilidad, atento al hecho que la página no era de propiedad del Banco.

Sin embargo, sostengo, que en algunos supuestos la situación puede no ser tan sencilla para las entidades bancarias.

De donde surge la responsabilidad del Banco en situaciones como esta?.

En los siguientes aspectos:

1. Para efectivizar el fraude, se requirió tener los mails de los clientes del Banco, a los efectos de remitirles el denominado *scam*.

   Por lo tanto, en este punto se modificar la carga probatoria, y debería ser el Banco quien deberá acreditar que no hubo dolo, culpa, negligencia o imprudencia en su deber de custodia de los mails de sus clientes, para evitar la responsabilidad.
2. También resulta necesario contar con un dominio obtenido por la metodología de la *ciberocupación* descripta.

   En este caso, también es el Banco el que cuenta con la tecnología de mayor avanzada para detectar la aparición de páginas con dominios que no le corresponde, y no solo iniciar las acciones legales correspondientes, sino alertar a sus

clientes en forma inmediata respecto de las páginas irregulares y de cual es página verdadera del Banco, en una política de marketing que no de lugar a dudas.

Sin perjuicio de lo expuesto, considero imprescindible el dictado de una legislación adecuada al respecto, que permita un cruzamiento previo con los diferentes registros existentes, como ser el de marcas, sociedades, propiedad intelectual, etc. Y que aumente los requisitos cuando el nombre elegido tenga alguna semejanza con nombres “públicos y notorios”.