PHISHING E IMPUTACIÓN DE RESPONSABILIDAD EN EL ÁMBITO BANCARIO*

Mª Nieves Pacheco Jiménez**
Prof. Contratada Doctora
Centro de Estudios de Consumo
Universidad de Castilla - La Mancha

Fecha de Publicación: 4 de Octubre de 2017

1. INTRODUCCIÓN

No es la primera vez que CESCO analiza el fenómeno del "phishing", contando con varios estudios sobre la materia[1]. El presente trabajo es continuidad de ellos, pero podemos augurar que no será el último dada la preeminencia de esta modalidad de fraude en un contexto tecnológico cada vez más arraigado.

Recordemos que el *phishing* es una forma de abuso informático que utiliza *spam*, mensajes de correo electrónico o sitios web falsos, suplantando en este caso la identidad de la fuente fiable, en la mayoría de los casos empleando una razón

* Trabajo realizado en el marco de la Ayuda del Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia (Subprograma Estatal de Generación de Conocimiento) del Ministerio de Economía y Competitividad, otorgada al Grupo de investigación y Centro de investigación CESCO, Mantenimiento y consolidación de una estructura de investigación dedicada al Derecho de consumo, dirigido por el Prof. Ángel Carrasco Perera, de la UCLM, ref. DER2014-56016-P.

** ORCID 0000-0002-9062-2342

[1] LYCZKOWSKA, K.: "Responsabilidad cuasi objetiva del proveedor de servicios de pago por las transferencias fraudulentas", julio 2015, en *CESCO* (disponible en http://centrodeestudiosdeconsumo.com/index.php/por-tematica/responsabilidad-en-derecho-de-consumo/1600-responsabilidad-cuasi-objetiva-del-proveedor-de-servicios-de-pago-por-las-transferencias-fraudulentas-2).
PACHECO JIMÉNEZ, Mª N.: "Más allá del *phishing* en los ordenadores", octubre 2015, en *CESCO* (disponible en http://blog.uclm.es/cesco/files/2015/10/M%C3%A1s-all%C3%A1-del-phishing-en-los-ordenadores.pdf).

aparentemente importante para que el destinatario confiera sus datos personales, con la finalidad de adquirir la información confidencial sobre contraseñas de cuentas bancarias o cualquier otra información.

Una de las modalidades más peligrosas del phishing es el *pharming*[2]. Esta técnica consiste en modificar el sistema de resolución de nombres de dominio (DNS "Domain Name System" o Sistema de Nombres de Dominio), que se encarga de convertir una dirección tecleada de un sitio web oficial en el navegador a una dirección IP numérica, para conducir al usuario a una página web falsa, en apariencia idéntica a la web de confianza pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios. El fraude se produce a través de ejemplares de *malware* diseñados para modificar el sistema de resolución de nombres local ubicado en un fichero denominado HOSTS (usado por el sistema operativo para guardar la correspondencia entre dominios de Internet y direcciones IP)[3].

2. ACTUALIDAD DE LOS ATAQUES DE *PHISHING* BANCARIO

Los ataques de *phishing* son cada vez más avanzados en su utilización de técnicas de ingeniería social. No se puede negar que la calidad de los mensajes empleados es bastante alta: los sitios falsos, por lo general, se ven exactamente iguales que los originales. El objetivo no es otro que el usuario no sospeche que algo va mal cuando ingresa su nombre de usuario y contraseña[4].

Hace tan solo unos días, la compañía de ciberseguridad Panda Security alertaba de la existencia de una campaña de *phishing* que utilizaba la imagen de correos electrónicos corporativos de la entidad bancaria Bankia para introducir un troyano en los equipos de sus víctimas, afectando a cientos de compañías y particulares[5]. El procedimiento era el siguiente: los ciberdelincuentes envían falsos correos electrónicos imitando el diseño de Bankia, a través de los que informan en nombre de la entidad de la resolución de una supuesta incidencia en la cuenta bancaria del usuario; en el propio correo adjuntan un documento de texto (denominado "DocumentoSeguro.doc", para generar así confianza) con falsa información detallada del proceso; el documento en cuestión, al ser abierto habilitando el uso de macros y descargando una supuesta imagen en formato .png, ejecuta el troyano bancario TrickBot en el equipo. Una vez

[2] A diferencia de los "phishers", que utilizan los correos electrónicos para lograr sus objetivos, los "pharmers" obtienen las identidades a través de sitios web oficiales. (*Vid*. https://securelist.lat/threats/que-es-el-phishing/)

[3] *Vid*. http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/

[4] *Vid*. https://securelist.lat/threats/que-es-el-phishing/

[5] *Vid*. http://amp.lasexta.com/noticias/ciencia-tecnologia/detectada-campana-phishing-que-utiliza-imagen-bankia-robar-credenciales-bancarias_2017100759d8b8080cf29f7c62de2e06.html

instalado el *malwar*e en el sistema, su objetivo es robar credenciales bancarias de la víctima cuando esta acceda a determinadas páginas web como plataformas de pago, Bancos y sitios de compra y venta de criptomoneda.

Pero ya un mes antes, la Oficina de Seguridad del Internauta (OSI) informaba de haber detectado una campaña de correos fraudulentos suplantando al Banco Sabadell (llevaba como asunto el nombre de la entidad y un número entre paréntesis) con el fin de que el usuario facilitase sus credenciales de acceso bajo el pretexto de haberse percibido "una serie de errores en la información registrada de su cuenta". Si el usuario consideraba legítimo ese correo y accedía a "Activación clientes", se le abría una web con aspecto parecido al de la web oficial del Banco (aunque realmente era una página fraudulenta)[6].

Los expertos señalan que el 91% de los incidentes informáticos comienzan con un correo electrónico de *phishing*. De ahí que se recomiende extremar las medidas de seguridad en nuestros equipos y concienciarnos de la existencia y del *modus operandi* de esta modalidad de fraude. Para ello, la OSI[7] trabaja continuamente elaborando directrices para detectar correos de *phishing* y recomendaciones para evitar ser engañado (v. gr., no abrir correos de usuarios desconocidos o que no se hayan solicitado, eliminándolos directamente; no contestar en ningún caso a dichos correos; tener la máxima precaución al seguir enlaces sospechosos en correos, aunque sean de contactos conocidos, así como al descargar ficheros adjuntos de correos).

El estudio "Spam y phishing en el segundo trimestre de 2017", de la empresa Karpersky Lab[8], recoge que en ese período de 2017 el sistema *antiphishing* neutralizó 46.557.343 intentos de conducir a páginas de *phishing*. El ranking de la geografía de los ataques es el siguiente: Brasil (18,09%), China (12,85%), Australia (12,69%), Nueva Zelanda (12,06%), Azerbaiyán (11,48%), Canadá (11,28%), Catar (10,68%), Venezuela (10,56%), República de Sudáfrica (9,38%), Argentina (9,35%), Inglaterra (9,29%). Y en lo que a organizaciones atacadas respecta, el meritado informe observa que el 51,47% de las detecciones realizadas ocurrió en webs que mencionaban nombres de categorías financieras (v. gr., "Bancos", "sistemas de pago", "tiendas en línea").

[6] *Vid*. https://www.osi.es/es/actualidad/avisos/2017/09/detectado-nuevo-phishing-que-intenta-suplantar-al-banco-sabadell
[7] *Vid*. https://www.osi.es/es
Vid. https://www.osi.es/es/actualidad/blog/2016/05/24/el-phishing-version-grafica
[8] *Vid*. https://securelist.lat/spam-and-phishing-in-q2-2017/85433/

Atendiendo a este panorama, la OSI insiste en una serie de consejos para evitar el *phishing* bancario:

1. "Cierra todas las aplicaciones antes de acceder a la web del banco".
2. "Escribe directamente la URL de tu banco en el navegador, en lugar de llegar a ella a través de enlaces disponibles desde páginas de terceros o en correos electrónicos".
3. "No accedas al servicio de banca online de tu banco desde ordenadores públicos, no confiables o que estén conectados a redes wifi públicas".
4. "MUY IMPORTANTE**:** Ningún banco envía por correo electrónico solicitudes de datos personales de sus clientes. Si recibes un correo en este sentido, no facilites ningún dato y contacta inmediatamente con tu banco para informarles".

3. BREVE RECORRIDO JURISPRUDENCIAL POR LOS ATAQUES DE *PHISHING* BANCARIO

A pesar de los continuos y abundantes ataques de *phishing* en el ámbito bancario, su reflejo en los tribunales no es directamente proporcional. Además, los pronunciamientos jurisprudenciales sobre esta materia ya datan de varios años, lejos de aparecer en los últimos años de la mano de la proliferación de usuarios tecnológicos.

Llegados a este punto, he considerado conveniente reseñar algunas de las sentencias recaídas sobre litigios de *phishing* bancario.

A) SAP Valladolid 10 marzo 2010 (AC\2010\368)

- El caso gira en torno a la demanda del director financiero de una importante cadena comercial alimentaria contra Banco Santander Central Hispano S.A. por *phishing*: el cliente facilitó sus claves al recibir un correo electrónico con un enlace falso.

- Ambas partes debaten sobre la posible negligencia en que pudo incurrir el actor en la custodia de sus claves y la posible responsabilidad del Banco por no contar con medidas seguras para la protección de la modalidad de la banca online. Por un lado, "en cualquier sistema operativo (…) existen riesgos y lo determinante para atribuir responsabilidades será si en el utilizado se daban garantías suficientes, sin que pueda llegarse a la conclusión contraria por el mero hecho de que posteriormente se hayan mejorado los sistemas de seguridad, que es de lógica que se vayan modernizando y perfeccionando ante nuevas prácticas defraudatorias que hacen ineficaces los anteriores". Por otro, al director financiero, por su

cualificación, "hay que suponerle conocedor de las posibles conductas engañosas que se pueden producir en la red informática, pues como resulta de la prueba era usuario habitual de la red", "y conocedor, además, como reconoce al declarar en el juicio, de toda la operativa relativa a las finanzas y a la operativa bancaria a nivel general". "Por tanto, de manera razonable hay que considerarle versado en la existencia de algo como la banca online por ser un sistema que facilita toda la operativa comercial a la que no puede resultar ajeno una persona que alcanza en un grupo empresarial importante un alto rango o categoría profesional cual es la dirección financiera".

- "En la página web del banco se hacía la expresa advertencia de que jamás se facilitase información personal y financiera en respuesta a correos electrónicos o llamadas telefónicas y que tampoco se utilizasen enlaces incorporados en email o páginas web de terceros. Tal como resulta de la propia prueba pericial aportada por el actor lo que sucedió es que recibió un correo electrónico (phishing), con un enlace por medio del cual el actor facilitó sus claves incumpliendo una elemental medida de seguridad de la que estaba expresamente advertido pues aparecía en la pantalla auténtica del Banco". A ello hay que añadir que constaba una carta enviada por el Banco por correo ordinario advirtiendo de las oleadas de *phishing*.

- Se apreció negligencia en el actor por el uso del sistema "al haber omitido elementales medidas de seguridad de las que estaba expresamente advertido como cualquier usuario del sistema online de la entidad demandada".

- Pero también se apreció responsabilidad de la entidad demandada por haber autorizado y aceptado peticiones de transferencias por encima de los límites establecidos y fijados en el contrato multicanal suscrito con el actor. De ahí que se reconociese el derecho del actor "a ser reintegrado por la entidad bancaria de los excesos del límite máximo diario de disposición sobrepasando los 6.011 euros contractualmente pactados al haber incumplido la entidad demandada lo convenido en el contrato".

B) SAP Alicante 23 diciembre 2011 (JUR\2012\76634)

- El litigio versa sobre el acceso fraudulento a cuentas bancarias a través de Internet. Concretamente, el actor formula demanda contra la Cooperativa de Crédito Caja Rural Central por transferencias no ordenadas por el titular de la cuenta mediante el servicio de banca a distancia.

- A lo largo del proceso se pone de manifiesto que "hubo varios clientes que sufrieron el mal funcionamiento del servicio, aparte del actor, ya que desde sus cuentas se efectuaron transferencias no ordenadas por los titulares de las mismas; ello con independencia, además, de que la entidad demandada procedió a cambiar el sistema operativo con posterioridad a que se produjeras las irregularidades detectadas, añadiendo algunos requisitos adicionales a fin de garantizar una seguridad mayor a la que existía hasta la fecha".

- Examinadas las actuaciones, "la demandada no ha conseguido acreditar las afirmaciones vertidas en su contestación a la demanda, esto es, que había cumplido con la seguridad de los servicios prestados por Internet y que, por el contrario, había sido el actor quien no había cumplido con la diligencia en la custodia de su usuario y contraseña".

- En definitiva, se estima la procedencia de la responsabilidad de la entidad bancaria al no acreditar la falta de diligencia del cliente en la custodia del usuario y contraseña. Además de entenderse que el Banco tiene la obligación de proteger el sistema, deduciéndose de los diferentes indicios que no fue así (varios clientes del Banco sufrieron el mismo problema y se produjo un cambio del sistema informático después de las irregularidades).

C) SAP Asturias 18 septiembre 2012 (JUR\2012\369519)

- Se resuelve un caso de posible *phishing* en el seno de un contrato de servicios de pago (banca electrónica): la empresa ALMACLIP, S.L. formula demanda contra BANCO BILBAO VIZCAYA ARGENTARIA, S.A.

- Al haber abierto un correo de "BBVA.net", en apariencia fraudulento, el representante de la empresa lo puso en comunicación del Banco y le cambiaron las claves, siendo después del cambio cuando se producen las transferencias fraudulentas. Añade que le explicaron en la policía que "en el momento de abrir ese correo sin meter claves ni meter nada, ya te clonan la página". Por tanto, "la actuación, según se desprende del interrogatorio de la representante de ALMACLIP, no puede ser más ajena a cualquier tipo de negligencia".

- Es más, el director de la sucursal de la entidad demandada afirma que en "seguridad operativa" del Banco "se dan cuenta que hubo un fraude".

- En definitiva, en caso de operaciones de pago no autorizado, ante un supuesto de fraude cometido y sin que existiera actuación fraudulenta de la empresa

ALMACLIP, ni incumplimiento de las obligaciones de seguridad y notificación, deliberado o por negligencia grave, según lo que dispone el art. 31 de la Ley 16/2009, la obligación del Banco era "devolver de inmediato el importe de la operación no autorizada y, en su caso, restablecer en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada".

- "Se establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago (…) pues en este ámbito de la contratación electrónica, el prestador del servicio deberá reembolsar el importe de la sustracción a su cliente con el que tuviera contratado el servicio de pago electrónico en operaciones no autorizadas por éste". Añade esta sentencia que "quien resultó engañado o burlado no fue tanto el titular de la cuenta sino la entidad financiera y proveedora del servicio que tenía su custodia y los medios de seguridad para protegerla, por lo que es ésta quien debe responder".

D) SAP Madrid 4 mayo 2015 (JUR\2015\151311)

- Se resuelve un caso de *phishing* bancario por la realización de una serie de transferencias a través de la "Banca Internet" de CAJAMAR S.A., a favor de destinatarios absolutamente desconocidos para la demandante, mediante operaciones que nunca ordenó.

- Entre los días 21 al 26 de marzo de 2010 tuvieron lugar las referidas transferencias, siendo denunciado este hecho por la actora ante el Cuartel de la Guardia Civil de Las Rozas (Madrid); en la denuncia no reconoció que al realizar la transferencia le solicitaran diversos códigos y ella los introdujera en lo que parecía ser una página falsa de la propia entidad.

- Posteriormente, la demandante intentó dirigirse a la entidad bancaria para solucionar amistosamente el conflicto.

- En mayo de 2010, CAJAMAR envió una carta a la actora, comunicándole que la entidad había puesto en marcha un nuevo sistema de protección de determinadas operaciones contables, con objeto de reforzar la seguridad de sus operaciones, en el Servicio de Banca Electrónica.

- Tras la demanda de la actora, CAJAMAR contestó afirmando disponer de los medios de seguridad necesarios para garantizar el éxito de las operaciones bancarias a través de su oficina virtual y asegurando poseer varios niveles de seguridad

complementarios (en el primer nivel se ofrece a un cliente el código de seguridad y una contraseña; como segundo nivel, la banca electrónica de CAJAMAR dispone de una tarjeta de coordenadas). Por todo ello, la entidad bancaria consideraba que la actora había incurrido en una grave negligencia al facilitar la llave de su banca electrónica a un supuesto troyano.

- La entidad bancaria defendía haber actuado diligentemente, señalando que las medidas de seguridad y los filtros habilitados por CAJAMAR habían funcionado correctamente y que había sido la actora la que ha posibilitado el fraude, actuando con negligencia grave al introducir sus claves personales y las coordenadas de la tarjeta de claves en una página fraudulenta. Cuando se dio noticia de la actuación fraudulenta, la entidad bancaria bloqueó la cuenta de demandante y envió a las oficinas beneficiarias de las transferencias información sobre el posible fraude, aunque fue imposible la recuperación de las cantidades.

- Sin embargo, el testigo-perito entendió que en el caso concurrieron circunstancias que deberían haber alertado a CAJAMAR: (i) cambios abruptos en la cuenta de la demandante entre los días 21 y 26 de marzo, produciéndose 3 o 4 transferencias diarias, cuando, en 1 año y 2 meses que la actora era titular de la cuenta, tan solo realizó 2 transacciones; (ii) las 17 transferencias se realizaron a favor de dos personas "muleros", que es el procedimiento habitual, hecho que debería haber alertado al servicio de seguridad de la entidad demandada. Además, el Juzgador considera que la entidad bancaria reconoce que dispone de unas medidas de seguridad bajas porque las cambia poco tiempo después.

- Y debe añadirse que, a pesar de que en las Condiciones Particulares del Contrato (concretamente en el apartado de "Oficina Virtual"), se establecía expresamente que el límite de transferencias diario, en la utilización de la banca electrónica, no debía superar los 3.000 euros, CAJAMAR tampoco fue capaz de detectar que el día 23 de marzo de 2010 se ordenaron cinco transferencias bancarias, por importe de 3.590 euros, sobrepasando el límite impuesto por la propia entidad bancaria. Esta circunstancia debió alertar claramente a CAJAMAR.

- Es evidente la existencia de *phishing*, que "se origina con la suplantación de la identidad del Banco por parte del *phisher* con la finalidad de adquirir información confidencial sobre contraseñas de cuentas bancarias, tarjetas de crédito o cualquier otra información en relación con el Banco, que permita entrar en las cuentas de los usuarios en Internet de banca electrónica".

- En cuanto a las actuaciones de actora y demandada, la Sala entiende que no ha existido una conducta negligente por parte de la usuaria de banca electrónica; el sistema de seguridad bancario debería tener una forma de detectar que se han entregado todas las combinaciones posibles de la tarjeta de coordenadas. Por su parte, CAJAMAR no actuó diligentemente, en previsión del fraude con el nivel máximo de seguridad, ya que no detectó el *phishing* sufrido por la demandante, a pesar de que los *phishers* realizaron las conductas típicas y actuaron con el modus operandi característico en este tipo de fraudes informáticos.

- Se resuelve aplicando el artículo 31 de la Ley 16/2009, de Servicios de Pago, que "establece un sistema de responsabilidad cuasi objetiva de la entidad financiera, que prevé la responsabilidad del prestador de servicios a consumidores salvo que acrediten haber actuado con la diligencia exigible, toda vez que, en este tipo de operaciones se obliga al banco a reembolsar el importe de la sustracción al cliente, siempre que este no haya actuado con negligencia grave".

E) SAP Vizcaya 10 noviembre 2016 (AC\2016\2241)

- El supuesto del litigio puede resumirse así: Los actores tenían contratado con el Banco demandado el servicio de banca por Internet. A través de la línea online del Banco, sin que el mismo detectara ninguna anomalía, las operaciones que se realizaron no solo conllevaron retiradas de fondos de las cuentas de los actores, sino que también se transmitieron órdenes de ventas de valores y, tras recibir la cantidad, se transferían a cuentas de terceros. Se trata del típico fraude denominado *phishing*.

- En Primera Instancia se imputa responsabilidad a los actores derivada de su negligencia grave "por entregar las claves bancarias desconociendo que precisamente el fraude se comete a partir de que los estafadores se introducen en la línea del Banco y solicitan las claves, creando así la apariencia a los clientes de validez de la solicitud; el fraude denunciado se consuma a través de dicha mecánica, siendo que el propio Banco admite que fue un fraude no detectado". Es más, el propio Banco, en el informe que aporta en el procedimiento penal señala que "se llamó al cliente pero que no fue hallado"; lo que "viene a ratificar que los movimientos resultaron sospechosos, lo cual permite sostener la falta de diligencia que ante la sospecha no se bloquearan los movimientos (además de que no consta cual fue la conducta para hallar al cliente o a qué número telefónico se le llamó)".

- Al no probarse el error grave que se imputa a los actores y no quedando acreditado por el Banco que su sistema online fuera seguro y fiable, se solicita revocación de la sentencia ante la Audiencia Provincial.

- La Sala afirma que "dichas circunstancias vienen a contemplar un sistema bancario electrónico diseñado por la entidad demandada adoleciendo de seguridad, la oferta a los clientes para operar a través de dicha banca electrónica y que es un hecho conocido de que cada vez se impone más por las entidades bancarias a los clientes, eliminando los servicios en ventanilla, se publicita por ser seguro contener los filtros para detectar fraudes y operar de forma fiable siendo así que en cuanto se ha probado la mecánica de la facilidad para operar por terceros no autorizados a través de la banca electrónica de la demandada difícilmente podemos decir de que el Banco demandado no haya incurrido en negligencia grave de sus obligaciones, se han permitido efectuar operaciones bancarias (30 movimientos) sin superar ningún filtro cuando la legislación bancaria tiende precisamente a establecer que se efectúen y se establezcan diferentes controles por los Bancos en protección de los clientes, tendiendo a establecerse una responsabilidad cuasi objetiva de las entidades bancarias en cuanto deben soportar los riesgos de su actividad profesional en cuanto que se establece con el cliente una responsabilidad contractual del servicio de depósito, custodia y pagos de las cuentas del cliente".

- "En consecuencia con lo razonado no se comparte la valoración de prueba de la juzgadora debiendo ser revocada la sentencia y estimar la demanda si bien el Banco deberá devolver la cantidad de 59.327,18 euros, que es la cantidad que la parte apelante en esta segunda instanciasolicita, más los intereses legales desde el 21 de septiembre de 2006 en que se efectuó la primera reclamación frente al demandado".

F) SAP Valencia 25 enero 2017 (JUR\2017\146789)

- Sin tratarse de un caso de responsabilidad civil por *phishing* bancario, esta sentencia resulta interesante por el análisis que realiza de las figuras del *phishing* y del denominado "mulero".

- "*Phishing* es un término informático que denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común a través del correo electrónico, suplantando páginas web o utilizando llamadas telefónicas. Su objetivo son clientes de banco y servicios de pago en línea".

- "Actualmente empresas ficticias intentan reclutar tele trabajadores por medio de e-mails, chats, IRC y otros, ofreciéndoles no solo trabajar desde casa, sino también

otros jugosos beneficios, las personas que aceptan la oferta se involucran blanqueando el dinero obtenido a través del *phishing*, siendo conocido este método de captación en internet como *scam*. Para que una persona pueda darse de alta con esta clase de empresas debe rellenar un formulario en el que indicará, entre otros datos, su número de cuenta bancaria. Esto tiene la finalidad de ingresar en la cuenta del trabajador el dinero procedente de estafas realizadas por el método de *phishin*g. Una vez contratado el supuesto trabajador se convierte automáticamente en lo que se conoce vulgarmente como mulero. Con cada acto fraudulento de *phishing* el "mulero" recibe el cuantioso ingreso en su cuenta bancaria y la empresa le notifica del hecho. Una vez recibido este ingreso, se queda un porcentaje del total del dinero como comisión de trabajo y el resto lo reenvía a través de sistemas de envío de dinero".

- ¿Estos intermediarios o "muleros" son realmente responsables o pueden alegar que han sido engañados? En Derecho norteamericano se aduciría la "willful blindness" o "ignorancia deliberada", incorporando así el dolo eventual adecuado al necesario principio de culpabilidad.

- En nuestro ordenamiento jurídico, se aprecian dos tesis para catalogar la conducta del "mulero":

a) "Un delito de estafa informática del artículo 248.2 del Código Penal", basándose en la STS de 25 octubre 2012 cuando dice que "con carácter general, hechos (…) en lo que tienen de operación concertada, con una estratégica distribución de roles para lograr un acto de despojo patrimonial mediante un engaño, valiéndose de terceros para poder extraer esos fondos sin suscitar sospechas en la entidad bancaria y, una vez obtenidos aquéllos, colocarlos en un país que asegure la impunidad del desapoderamiento, presentan las características que son propias del delito de estafa informática al que se refiere el art. 248.2 del CP".

b) Encaje "en el art. 298 del CP, como una modalidad de receptación"; se entiende que "la colocación del dinero en países con los que no existen mecanismos jurídicos de cooperación judicial, forma parte ya de la fase de agotamiento del delito, de forma que la captación de estos puede llegar a producirse cuando ya la estafa se habría cometido. De ahí que estaríamos en presencia de una participación postdelictiva o postconsumativa, con un evidente contenido lucrativo, notas definitorias del delito de receptación".

4. CONSIDERACIONES FINALES

Ante los cada vez más habituales y perfeccionados casos de *phishing* bancario, los Bancos, en aras de prevenir la imputación de responsabilidades patrimoniales, deben tener muy presentes los lineamientos de la Ley de Servicios de Pago (Ley 16/2009, de 13 de noviembre)[9], a saber:

- Art. 29.1 LSP: "*Cuando el usuario de servicios de pago tenga conocimiento de que se ha producido una operación de pago no autorizada o ejecutada incorrectamente, deberá comunicar la misma sin tardanza injustificada al proveedor de servicios de pago, a fin de poder obtener rectificación de éste*".

- Art. 30 LSP: "*1. Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá a su proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico o cualquier otra deficiencia. 2. A los efectos de lo establecido en el apartado anterior, el registro por el proveedor de servicios de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste actuó de manera fraudulenta o incumplió deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 27*".

- Art. 31 LSP: "*Sin perjuicio de lo dispuesto en el artículo 29 de la presente Ley, y de las indemnizaciones por daños y perjuicios a las que pudiera haber lugar conforme a la normativa aplicable al contrato celebrado entre el ordenante y su proveedor de servicios de pago, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante le devolverá de inmediato el importe de la operación no autorizada y, en su caso, restablecerá en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada*".

Sin embargo, a pesar de la responsabilidad cuasi objetiva de las entidades bancarias *ex* art. 31 LSP, con su correspondiente inversión de la carga de la prueba (siendo el proveedor de servicios de pago quien deba demostrar que la operación fue autenticada y que no se vio afectada por fallos técnicos u otras deficiencias), el cliente también se responsabilizará de operaciones de pago no autorizadas en los supuestos del art. 32

[9] Sin olvidar su necesaria revisión –actualmente en ciernes- derivada de la Directiva europea 2015/2366/CE, sobre servicios de pago en el mercado interior (DSP II).

LSP: "*1. No obstante lo dispuesto en el artículo 31, el ordenante soportará, hasta un máximo de 150 euros, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado o sustraído. 2. El ordenante soportará el total de las pérdidas que afronte como consecuencia de operaciones de pago no autorizadas que sean fruto de su actuación fraudulenta o del incumplimiento, deliberado o por negligencia grave, de una o varias de sus obligaciones con arreglo al artículo 27*".

Pero deben hacerse dos salvedades que exoneran al ordenante *ex* art. 32.3 y 32.4 LSP: "*3. Salvo en caso de actuación fraudulenta, el ordenante no soportará consecuencia económica alguna por la utilización, con posterioridad a la notificación a que se refiere el artículo 27.b), de un instrumento de pago extraviado o sustraído. 4. Si el proveedor de servicios de pago no tiene disponibles medios adecuados para que pueda notificarse en todo momento el extravío o la sustracción de un instrumento de pago, según lo dispuesto en el artículo 28.1.c), el ordenante no será responsable de las consecuencias económicas que se deriven de la utilización de dicho instrumento de pago, salvo en caso de que haya actuado de manera fraudulenta*".