EL PHISHING COMO DELITO DE ESTAFA INFORMÁTICA. COMENTARIO A LA SAP DE VALENCIA 37/2017 DE 25 DE ENERO (REC. 1402/2016)

PHISING AS A CRIME OF COMPUTER FRAUD. COMMENT ON SAP VALENCIA 37/2017 OF JANUARY 25 (REC, 2402/2016)

Rev. Boliv. de Derecho Nº 25, enero 2018, ISSN: 2070-8157, pp. 650-659

Diego Eloy
GARCÍA GARCÍA

ARTÍCULO RECIBIDO: 30 de octubre de 2017
ARTÍCULO APROBADO: 15 de noviembre de 2017

RESUMEN: El "phishing" se revela como una modalidad de estafa informática cuyo objeto principal es obtener del usuario, entre otros, datos, claves o números de cuentas bancarias con la finalidad de obtener un beneficio económico ilícito utilizando para ello de forma fraudulenta y mediando engaño datos personales del usuario. Dicha modalidad delictiva ha ido evolucionando con el paso del tiempo adoptando diferentes perfiles, proliferando actualmente el denominado phishing bancario, el cual tiene como objetivo los clientes de Banco y servicios de pago en línea. La SAP de Valencia se hace eco de los últimos pronunciamientos jurisprudenciales para profundizar en los conceptos de "phishing", "mulero" y posible responsabilidad del mismo en la comisión del citado delito informático.

PALABRAS CLAVE: Phishing, mulero, datos personales, ignorancia deliberada.

ABSTRACT: "Phishing" is a modality of computer scam whose main purpose is to obtain from the user, among others, data, passwords or bank account numbers in order to obtain an illicit financial benefit by using it fraudulently and mediating scam user´s personal data. This criminal modality has evolved over time adopting different profiles, currently enabling the so-called banking phishing, which aims to bank customers and online payment services online. The sentence of AP reflected the last judgmental decisions to deepen in the concepts of "phishing", "mulero" and possible responsibility of the same in the commission of the mentioned computer crime.

KEY WORDS: Phishing, "mulero", personal data, wilful blindness.

SUMARIO.- I. EL CONCEPTO DE PHISHING Y SU CONSIDERACIÓN COMO DELITO DE ESTAFA INFORMÁTICA TIPIFICADO EN EL CÓDIGO PENAL.- II. RESPONSABILIDAD CUASI-OBJETIVA DE LA ENTIDAD BANCARIA PROVEEDORA DE SERVICIOS DE PAGO EN LÍNEA.- ESPECIAL REFERENCIA A LA LEY 16/2009. III. RESPONSABILIDAD PENAL DE LOS DENOMINADOS "MULEROS".- IV. CONCLUSIONES

SUPUESTO DE HECHO

En fecha 6 de mayo de 2016 el Juzgado de lo Penal nº 17 de Valencia dicta Sentencia por la cual condena al autor de un delito de estafa informática en grado de tentativa a cuatro meses de prisión e inhabilitación especial para el ejercicio del derecho de sufragio pasivo.

Del relato de los hechos se extrae que el acusado, con el propósito de obtener un beneficio económico ilícito, consiguió que le fueran transferidas a su cuenta bancaria sendas cantidades de dinero por importe de 300, 5 euros y 1.600 euros procedentes de varias cuentas de la víctima. Para lograrlo, manipuló u obtuvo sus claves de usuario y contraseña, ordenando así directamente éste o mediante la colaboración de terceras personas transferencias por los citados importes, las cuales fueron bloqueadas por la entidad bancaria y el dinero recuperado.

Contra la sentencia dictada en primera instancia se alza el recurrente en apelación aduciendo como motivos de apelación falta de motivación de la sentencia, error en la apreciación de la prueba, infracción de precepto penal y dilaciones indebidas, los cuales son desestimados por la Sección 2ª de la Audiencia Provincial de Valencia en una sentencia de 25 de enero de 2017, a excepción de las dilaciones indebidas como circunstancia modificativa de la responsabilidad criminal. El resto de motivos son desestimados sobre la base de que a la vista del relato de los hechos y la prueba practicada, el acusado cometió un delito de estafa informática del artículo 248.2 a) del Código Penal, ya sea por su propia actuación o valiéndose de terceras personas, los denominados "muleros", encargados de recibir parte de las transferencias para posteriormente entregarlas al "phisher" o autor del delito de contenido informático.

• Diego Eloy García García
Colegiado ejerciente del Ilustre Colegio de Abogados de Valencia. Junior en Deloitte Abogados S.L.P Fiscal-Legal. Graduado en Administración de Empresas y Derecho por la Universidad de Valencia. Secretario de comunicación del IDIBE.

DOCTRINA JURISPRUDENCIAL

La sentencia de la Audiencia Provincial de Valencia de 25 de enero de 2017 tiene especial importancia porque analiza dos aspectos clave:

-En primer lugar, profundiza en el concepto de phishing a través de la recopilación y análisis de pronunciamientos de otras Audiencias provinciales y del Alto Tribunal, no solo refiriéndose al phishing con carácter general sino concretamente hace hincapié en el phishing bancario como modalidad de estafa informática contenida en el artículo 248.2 a) del Código penal consistente en la utilización de técnicas de sustracción o robo de datos personales de contenido económico, como pueden ser las credenciales de acceso a los servicios de pago en línea o tarjetas de crédito mediante la suplantación de páginas web, a través del correo electrónico o por medio de la utilización de servicios de pago, teniendo como principales víctimas los usuarios de servicios de pago en línea.

-En segundo lugar, analiza en base a qué conducta delictiva y modalidad de actuación o colaboración puede exigírsele responsabilidad penal a los muleros, concluyendo que "hay que estar al caso concreto", pues hay teorías divergentes entre sí que consideran que puede exigírseles responsabilidad penal como colaboradores en el delito de estafa, como autores de un delito de receptación o del delito de prevención de blanqueo de capitales.

COMENTARIO

I. EL CONCEPTO DE PHISHING Y SU CONSIDERACIÓN COMO DELITO DE ESTAFA TIPIFICADA

El término "phishing" ha sido analizado en los últimos años por los distintos órganos jurisprudenciales habida cuenta la incidencia que dicha conducta delictiva sobre la manipulación de los datos personales, y más concretamente, la modalidad de phishing bancario, la cual se ha ido extendiendo y adoptando formas cada vez más difíciles de detectar.

El Tribunal Supremo desde hace años ha analizado éste delito de estafa informática, así destaca la sentencia de 2 de diciembre de 2014 (RJ 845, 2014) relativamente reciente en la que el Alto Tribunal encuadra estas conductas de phishing bancario en el artículo 248.2 a) del Código Penal y explica cómo suele actuar el autor de este tipo de delitos de estafa informática.

La conducta básica que encarna este tipo de delitos consiste en el envío de emails fraudulentos desde direcciones supuestamente de entidades bancarias a la dirección de correo electrónico de la víctima, reclamando datos personales

de contenido económico, como regla general datos de acceso a las cuentas (usuario y contraseña) que la víctima o víctimas tengan abiertas en la entidad o mediante enlaces a una web casi idéntica o muy similar a la de la entidad bancaria, produciendo así engaño en los usuarios con la finalidad de obtener un beneficio económico ilícito mediante la realización de transferencias a la cuenta del autor o autores del delito.

Destaca también la SAP de Vizcaya de 10 de noviembre de 2016 (RJ 429, 2016), en la cual dicho órgano jurisdiccional concreta que en el "phishing bancario" es habitual que "el internauta reciba un correo en el que se la informe de que debe verificar sus cuentas, seguido por un enlace que parece la página Web oficial de la entidad bancaria."

La sentencia objeto de análisis de la Audiencia Provincial de Valencia de 25 de enero de 2017 (RJ 37/2017) profundiza en los conceptos de phishing y mulero, trata de configurar la responsabilidad del mulero y además analiza un caso en el que Bankia S.A como proveedora de servicios de pago en línea consigue bloquear las transferencias realizadas por el autor del delito, desplegando así la requerida diligencia y no generándose responsabilidad civil contractual por haber adoptado la entidad bancaria las medidas necesarias tendentes a la evitación del delito.

El phishing en sí consiste según la Audiencia "en enviar una oferta de trabajo a una cuenta de correo electrónico de un usuario para que desde su propio domicilio pueda acceder a otras cuentas corrientes de personas desconocidas, cuyos datos ha dado voluntariamente el usuario que recibió el correo, obteniendo ingresos propios de la actividad económica legal que se dice realizada en España (…) Ese dinero obtenido, que habitualmente proviene de la sustracción a la cuenta bancaria de otra persona a la que se ha tenido acceso, llega a una cuenta que un individuo o sociedad tiene en lugar de imposible identificación o localización."

La Audiencia a continuación se pronuncia sobre el denominado phishing bancario como técnica de ingeniería social caracterizada *por* intentar obtener información confidencial, consistente en datos personales del usuario, de forma fraudulenta, como pueden ser contraseñas o información sobre tarjetas de crédito u otra información bancaria a través de una técnica consistente en suplantar páginas web o enviar correos electrónicos aparentemente oficiales haciéndose pasar por empresas o entidades de confianza (normalmente Bancos) y solicitando la aportación de datos relativos al usuario y contraseña de acceso a servicios de pago en línea, pues el principal objetivo del autor o autores de estos delitos son los usuarios de servicios de pago en línea.

II. RESPONSABILIDAD CUASI-OBJETIVA DE LA ENTIDAD BANCARIA PROVEEDORA DE SERVICIOS DE PAGO EN LÍNEA.

El Alto Tribunal, en la sentencia anteriormente mencionada instaura un sistema de cuasi-responsabilidad civil objetiva de las entidades bancarias sobre la base de una falta de diligencia del Banco por no contar con medidas de protección suficientes del servicio de banca online, descartándose así un pretendido deber de autoprotección de la víctima salvo que se trate de "un engaño burdo o fácilmente perceptible que hubiera podido ser evitado por cualquier sujeto pasivo con una mínima reacción defensiva".

Por tanto, el Tribunal Supremo considera que como regla general no se le puede exigir a la víctima del delito mecanismos de autoprotección en orden a evitar la comisión del hecho delictivo, pues por la propia complejidad de las conductas delictivas que configuran este delito de estafa informática es muy difícil que la víctima pueda darse cuenta y en consecuencia evitar que se consumen dichas conductas delictivas, sino que es la entidad bancaria la que debe adoptar los mecanismos de precaución necesarios para evitar dichas conductas delictivas.

En el mismo sentido se pronuncia la SAP de Asturias de 18 de septiembre de 2012 (JUR\2012\369519), la cual considera que existe un sistema de responsabilidad cuasi-objetiva de la entidad bancaria pues es ésta como proveedora de dichos servicios de pago en línea quien debe asegurar la custodia de las claves de acceso y proporcionar los medios de seguridad necesarios para protegerla, y quien en caso de consumarse la conducta delictiva sin haber adoptado los medios necesarios para evitar que se produjera la estafa informática quien deberá "restablecer en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haber efectuado la operación de pago no autorizada", tal y como dispone el artículo 31 de la Ley 16/2009.

Por tanto, la realización de este tipo de conductas da lugar a la exigencia de dos tipos de responsabilidades:

En primer lugar, una responsabilidad penal consecuencia de la comisión de un delito de estafa informática del 248 del CP, el cual se exigirá a título de autor o autores a quien o a quienes hayan desplegado la conducta delictiva tendente a la utilización de métodos de sustracción de datos personales mediante robo de claves de acceso a los servicios de pago en línea con la finalidad de obtener un beneficio patrimonial ilícito mediante la generación de engaño en la víctima o víctimas. También nos referiremos posteriormente a aquellas conductas tendentes a posibilidad la materialización del delito, denominados muleros.

En segundo lugar, una responsabilidad civil cuasi-objetiva derivada de la falta de diligencia de la entidad bancaria en orden a adoptar las medidas necesarias para evitar las disposiciones económicas en favor del autor o autores del delito, sobre la base de la existencia de una relación contractual entre la entidad bancaria proveedora de servicios de pago en línea y el usuario víctima del delito, responsabilidad amparada en la Ley 16/2009 de Servicios de Pago.

De nuevo en este punto resulta de especial relevancia la SAP de Vizcaya de 10 noviembre de 2016 responsabilidad exigible a la entidad bancaria prestadora de servicios, la Audiencia considera que el phishing como "modalidad fraudulenta de movimientos de cuenta es una práctica extendida, por lo que, exige por ello que la entidad bancaria o crediticia deba adoptar las medidas de seguridad específicas, siguiendo las recomendaciones existentes, o que puedan practicar otras entidades."

Si bien en primera instancia el Juzgado de 1ª Instancia nº 9 de Bilbao desestimó la demanda interpuesta por la parte demandante sobre la base de la existencia de negligencia grave de los actores por no haber custodiado las claves de acceso a la cuenta. Sin embargo, en segunda instancia la Audiencia entiende que el Banco no fue capaz de demostrar que su sistema contaba con los medios necesarios para garantizar la seguridad de las transferencias efectuadas en línea, no quedando acreditado que el sistema online del Banco fuera seguro y fiable.

Quedaron probadas las múltiples transferencias que se realizaron desde la cuenta de los actores sin que la entidad bancaria adoptara las precauciones necesarias ni sospechara de las mismas, por lo que debiendo el Banco soportar los riesgos de su actividad profesional, se estima el recurso de apelación interpuesto por la parte actora y se condena a la demandada a devolver el importe de las transferencias efectuadas de forma fraudulenta de conformidad con lo dispuesto en el artículo 31 de la Ley 16/2009 de servicios de pago.

La sentencia de la AP de Valencia objeto de análisis acoge un supuesto hecho novedoso, pues a diferencia de otras en las que los tribunales se han referido a la aplicación de la Ley 16/2009, la entidad bancaria proveedora de los servicios de pago en línea, consiguió bloquear las transferencias indebidas y recuperar los montantes de dinero de dichas transferencias, las cuales fueron devueltas al usuario de los servicios de pago, siendo condenado el autor por un delito de estafa informática del 248 del Código Penal en grado de tentativa y no exigiéndose por tanto responsabilidad civil contractual a la entidad bancaria sobre la base de no haber adoptado las precauciones necesarias para evitar las transferencias indebidas, pues las misma fueron bloqueadas por Bankia.

En la mayoría de las ocasiones en que han tenido lugar dichas conductas delictivas, los tribunales se han remitido a lo dispuesto en los artículos 31 y 32 de la Ley de Servicios de Pago, instaurando un sistema de cuasi responsabilidad cuasi-objetiva:

El artículo 31 contempla la responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas, estableciéndose una obligación de pago para el proveedor de servicios de pago del ordenando, quien deberá devolver de inmediato el importe de la operación no autorizada y restablecerá en la cuenta de pago el estado que habría existido en caso de no haberse efectuado dicha operación de pago no autorizada.

Por tanto, la responsabilidad contractual corre a cargo del proveedor de los servicios de pago en línea con la salvedad contemplada en el artículo 32 de la citada Ley: pues el usuario soportará hasta un máximo de 150 euros las pérdidas derivadas de operaciones de pago no autorizadas cuando el instrumento de pago haya sido extraviado o sustraído.

Solo responderá el usuario ordenante y en consecuencia soportará el total de las pérdidas cuando "sean fruto de su actuación fraudulenta o del incumplimiento deliberado o por negligencia grave, de una o varias de sus obligaciones."

De modo que, habiéndose intentado la consumación del delito de estafa informática se condena al acusado como autor del delito de estafa informática en grado de tentativa y no cabe exigir responsabilidad civil contractual a la entidad bancaria por haber adoptado las precauciones necesarias en orden a evitar la materialización de las transferencias fraudulentas, habiendo sido bloqueadas por el Banco, habiendo actuado diligentemente.

III. RESPONSABILIDAD PENAL DE LOS DENOMINADOS "MULEROS"

Tal y como menciona la Audiencia provincial de Valencia en la citada sentencia, el autor o autores del delito se sirven a su vez de otras personas que colaboran consciente o inconscientemente en al blanqueo de dinero obtenido a través del phishing reclutando así a personas mediante la denominada captación en internet como scam.

Estos trabajadores conocidos como "muleros", los cuales son contratados por una supuesta empresa, reciben ingresos procedentes del phishing, quedándose un porcentaje del total del dinero como comisión de trabajo y reenviando el resto a la supuesta empresa que les contrató, lo que posibilita el blanqueo de capitales.

Con respecto a los muleros, ha suscitado una importante polémica la atribución o no de responsabilidad criminal por colaborar en la comisión del hecho delictivo:

Parte de la doctrina considera que la conducta de los muleros se encuadra dentro del delito de estafa informática en su condición de cooperados necesarios en la comisión del hecho delictivo.

Sin embargo, hay otros autores doctrinales que consideran que la conducta de los muleros se encuadraría más en el delito de receptación como ocultación o encubrimiento de los efectos del delito, tratando de evitar así las sospechas de la entidad bancaria, y que la captación de éstos en ocasiones puede producirse una vez ya se ha consumado el delito, por lo que para algunos autores tendría más cabida en el delito de receptación que no en el delito de estafa informática.

Y finalmente, otros autores doctrinales consideran que dichas conductas se encuadrarían en el delito de blanqueo de capitales.

La Audiencia Provincial acoge el concepto de "ignorancia deliberada" para apreciar la existencia del dolo eventual en la conducta de los muleros, aspecto que justifica la atribución de responsabilidad criminal a estos colaboradores.

IV. CONCLUSIONES

El presente trabajo ha pretendido analizar cómo se pronuncia en la actualidad la jurisprudencia acerca del phishing bancario a través del análisis de la SAP de 25 de enero de 2017.

Se ha escogido esta sentencia por ser una novedad en algunos de los aspectos que envuelven el phishing y por contemplar un supuesto en el que la entidad bancaria proveedora de los servicios de pago en línea actuó diligentemente y evitó la consumación del delito, evitando así incurrir en un supuesto de responsabilidad civil contemplado en la Ley 16/2009 de servicios de pago.

Como conclusión, podemos destacar que el phishing como modalidad de estafa informática ha ido adoptando perfiles cada vez más complejos, existiendo una mayor dificultad para detectar la sustracción de datos personales y requiriendo mecanismos cada vez más sofisticados a implementar por parte de las entidades bancarias para evitar que como consecuencia de la sustracción de datos personales se ordenen transferencias indebidas, siendo deber de la entidad bancaria desplegar la debida diligencia en orden a evitar la consumación del delito.

Como consecuencia de ello, es inviable exigir al usuario ordenante que adopte mecanismos de autoprotección, pues es harto difícil que la víctima pueda darse

cuenta de que el correo electrónico o la página web a la que redirecciona el correo electrónico no sean las de la entidad bancaria proveedora de servicios en línea, pues cada vez son más sofisticados los mecanismos utilizados por los phishers para sustraer mediante engaño las claves de la cuenta online de los usuarios, salvo que exista una falta de diligencia del usuario en orden a la custodia de las claves de acceso al servicio de pago electrónico

Es a la entidad bancaria a quien corresponde desplegar distintas estrategias o acciones tendentes a prevenir la sustracción de los datos personales de contenido económico del ordenante, como por ejemplo avisar de que no se facilitase información personal y financiera en respuesta a correos electrónicos ni tampoco utilizar enlaces integrados en un email o acceder a páginas web de terceros, advertir de oleadas de phishing y sobre todo implementar mecanismos que bloqueen las transferencias cuando puedan existir indicios de que las mismas puedan haberse realizado de forma fraudulenta. En caso contrario, las entidades bancarias a la luz de la Ley 16/2009 de servicios de pago se exponen a que se les exija una responsabilidad civil cuasi-objetiva y deban de reintegrar el importe de las transferencias indebidas al usuario de los servicios de pago

Por último, con respecto a la cada vez más habitual utilización de los denominados muleros para evitar dejar rastro de las transferencias indebidas, como bien expone la sentencia de la AP de Valencia habrá que estar al caso concreto, pues aunque en ocasiones la contratación de los mismos pueda ser posterior a la comisión del delito de estafa informática y no ser partícipes del mismo pues éste ya se consumó previamente, sí podría exigírseles responsabilidad penal por un delito de receptación u ocultación de efectos o instrumentos del delito o de un delito de prevención de blanqueo de capitales.