SEMINARIO: DERECHO INFORMÁTICO

PROYECTO DE INVESTIGACION*: TÉCNICA LEGISLATIVA RESPECTO DEL DELITO DE PISHING.*

PROFESORES: **Dra. Olivera, Noemí.**

Abog. Liceda, Ernesto

ALUMNO: **VALDEZ BEDNARZ , DARA F.**

Nº de LEGAJO: **115433/7**

INDICE

INTRODUCCIÓN:

El presente trabajo tiene como objeto de investigación la *técnica legislativa* (entendiéndose a la misma como la actividad del legislador en la elaboración de las normas jurídicas), respecto del delito informático que recibe el nombre de PISHING.

Ello para verificar, primero, si actualmente existen tipos legales en los que se puedan incorporar este tipo de acción disvaliosa, y de ser así entonces investigar al respecto si se pudo lograr una regulación acabada y eficiente de tal figura delictiva, o si, por el contrario esto resulta insuficiente, de manera que debería llevarse a cabo otros recursos para lograr tal fin.

La tecnología informática y el enorme desarrollo de las telecomunicaciones, especialmente Internet, han planteado al sistema penal distintos desafíos y la necesidad de cambios en las normas. Es fácil advertir que el avance de la tecnología es más rápido que la adecuación del Derecho a este nuevo fenómeno.

Desde el sentido común parece evidente que el intento de aplicar las normas pensadas para la evidencia física a entornos digitales no puede arribar a buenos resultados.[1]

A partir de esto surge la problemática: ***¿Existe en la actualidad del ordenamiento jurídico argentino un tipo legal donde pueda quedar incorporado el delito informático de PISHING? De ser así, la técnica legislativa aplicada para dicho tipo legal ¿Resulta suficiente para regular todos los aspectos y consecuencias que conlleva el delito de PISHING?***

[1] *Marcos Salt, Profesor de Derecho Penal y Procesal (UBA) ,POLICIALES DELITOS INFORMÁTICOS: Los interrogantes que se están planteando en nuestros tribunales, Diario Clarín, en http://www.clarin.com/policiales/interrogantes-planteando-tribunales_0_859114225.html , consultado Julio de 2013.*

HIPÓTESIS:

Actualmente existe en el ordenamiento jurídico argentino la figura de fraude informático (que se incorpora al Código Penal por medio del Art. 173 inc. 16 según la ley nacional N° 26.388) que el legislador equipara a la estafa sólo a efectos de utilizar a esta figura como punto de partida y comparación[2], y siendo el PISHING una especie de estafa informática, cuenta con los elementos propios para quedar incorporado en la figura de fraude informático.

CAPITULO I : ¿QUE ES EL PISHING?

El término phishing proviene de la palabra inglesa "fishing" (pesca), haciendo alusión al intento de hacer que los usuarios "muerdan el anzuelo"[3].

Se trata de una técnica de captación ilícita de datos personales a través de correos electrónicos o páginas web que imitan la imagen o apariencia de una entidad bancaria (o cualquier otro tipo de empresa). Es uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial, ya que funciona por la confianza que los usuarios tienen depositada en las entidades de las que son clientes y, por desconocimiento o simplemente ante la incertidumbre, acceden a dichas páginas web piratas, donde el defraudador o delincuente informático, obtiene los datos personales o claves de acceso personales.

> "Distinguir un mensaje de phishing de otro legítimo puede no resultar fácil para un usuario que haya recibido un correo de tales características, especialmente cuando es efectivamente cliente de la entidad financiera de la que supuestamente proviene el mensaje.

[2] *Gustavo A. Arocena, LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL ARGENTINO – INTRODUCCIÓN A LA LEY NACIONAL N°26.388*

[3] *http://es.wikipedia.org/wiki/Phishing*

El campo De: del mensaje muestra una dirección de la compañía en cuestión. No obstante, es sencillo para el estafador modificar la dirección de origen que se muestra en cualquier cliente de correo.

El enlace que se muestra parece apuntar al sitio web original de la compañía, pero en realidad lleva a una página web fraudulenta, en la que se solicitarán datos de usuarios, contraseñas, etc.

Normalmente estos mensajes de correo electrónico presentan errores gramaticales o palabras cambiadas, que no son usuales en las comunicaciones de la entidad por la que se están intentando hacer pasar"[4].

I.1. CIRCUITO DE UN ATAQUE DE PISHING

Falsificación de un ente de confianza

⇩

Envío de mensajes por algún medio de propagación

⇩

Un porcentaje de usuarios confía en el mensaje y hace click

⇩

Los usuarios acceden a un sitio web falso e ingresan sus datos personales.

I.1.A. ACTO DE DISPOSICION PATRIMONIAL

Es la diferencia sustancial con el delito de estafa tradicional: la disposición patrimonial propia del delito de Pishing la comete el propio sujeto activo y no la víctima.

Ello porque la propia dinámica comisiva de dicho supone que no se pueda atender a los parámetros exigidos del engaño y error propios de la modalidad de estafa básica por ausencia de alteridad o relación interpersonal entre autor y víctima. La conducta se lleva a cabo mediante el empleo de "manipulación informática", perpetrando así la disposición patrimonial el sujeto activo, quien obtiene una "transferencia no consentida".

[4] *http://www.infospyware.com/articulos/que-es-el-phishing/*

I.1.B. CONCEPTOS DE ENGAÑO Y ERROR

Engaño: Consiste en una simulación o disimulación capaz de inducir a error a una o varias personas.

Maquinación dirigida a aparentar la existencia de una cosa que no es real o hacerla aparecer con características que no tiene (simulación= u ocultando aquellas que efectivamente posee (disimulación).

El engaño importa una conducta activa.

Error: Falso concepto que se tiene de un hecho o circunstancia. Para incurrir en error la persona debe ser capaz de ser engañada.

Tanto el engaño precedente o concurrente, como la producción de un error esencial que se relacionen directamente con el acto de disposición patrimonial, son esenciales para que ocurra el delito de estafa tradicional. Sin embargo éstos no son requisitos exigibles para la comisión del Pishing, en el cual están presentes la manipulación informática y la transferencia no consentida de activos patrimoniales.

I.1.C. CONSECUENCIAS

- Robo del dinero en la cuenta bancaria: Los daños causados por el phishing oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustanciales. Una vez que el pisher adquiere la información, puede usar esos datos personales para crear cuentas falsas utilizando el nombre de la víctima, gastar el crédito de la víctima, o incluso impedir a las víctimas acceder a sus propias cuentas.
- Uso indebido de la tarjeta de crédito.
- Estafa.
- Venta de los datos personales.
- Suplantación de identidad.

- Envío de publicidad.

I.1.D. OTRA MODALIDAD DE PISHING: WEB SPOOFING:

Suplantación de la página web de una conocida entidad financiera a la que se redirige al usuario desde el correo engañoso mediante un enlace o link.[5]

CAPITULO II: EL PRINCIPIO DE EQUIVALENCIA FUNCIONAL

> *"Es aquel que propone que nuevas situaciones planteadas por la incorporación de TICs a cuestiones jurídicas tengan la misma solución que la que se les daba cuando se resolvían en formato papel. Ha cumplido y cumple una función muy importante para el derecho, el permitir la utilización de las TICs y asignar a los actos mediados por ellas el valor jurídico derivado del cumplimiento de los preceptos formales tenidos en vista por el legislador inicial, ignorando las diferencias materiales de los soportes."*[6]

CAPITULO III: TÉNICA LEGISLATIVA DEL PISHING

Actualmente en Argentina existe- por la incorporación al Código Penal del inc. 16 del Art. 173 a través de la ley nacional N° 26.388- la *figura delictiva* ("que puede definirse como *el trozo más pequeño de texto legal que opera como condición necesaria de una pena*"[7]) de Fraude Informático:

> *ARTICULO 173.-" Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:*

[5] *http://web.ua.es/es/contratos-id/documentos/itipupdate2011/moya.pdf*
[6] *Ernesto Liceda, Límites de la equivalencia funcional (y de la comodidad de Legislador) en el Derecho Penal en http://www.39jaiio.org.ar/sites/default/files/39jaiio-sid-17.pdf*
[7] *Ernesto Liceda, Límites de la equivalencia funcional (y de la comodidad de Legislador) en el Derecho Penal, en http://www.39jaiio.org.ar/sites/default/files/39jaiio-sid-17.pdf*

16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. (Inciso incorporado por art. 9° de la Ley N° 26.388, B.O. 25/6/2008).

15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática. (Inciso incorporado por art. 1° de la Ley N° 25.930 B.O. 21/9/2004)."

Definido el delito de PISHING, se puede notar que, siendo una especie de estafa informática, tiene elementos propios que lo identifican y que sirven para incluirlo dentro de los artículos mencionados precedentemente. Sin embargo, al respecto surge el cuestionamiento de si resulta suficiente para su regulación incluirlo en la figura de fraude informático o, si por el contrario, sería necesaria la existencia de otra técnica legislativa (como puede ser una ley especial de Pishing) para abarcar todos y cada uno de los aspectos y consecuencias que conlleva tal figura antijurídica.

Por ejemplo, un aspecto del mismo que podría ser regulado más acabadamente serían las diferentes técnicas de obtención ilegítima de información personal. Así, en Argentina, el 19 de septiembre de 2011 fue presentado un proyecto para sancionar el Phishing , bajo el Nº de Expediente S-2257/11, Proyecto de Ley para tipificar el Phishing o Captación Ilegítima de Datos en el Senado de la Nación, con dicho objetivo.

III.1 LEGISLACIÓN COMPARADA

ESTADOS UNIDOS: El senador Patrick Leahy introdujo el Ley Anti-Phishing de 2005 el 1 de marzo de 2005. Esta ley federal de anti-phishing establecía que aquellos criminales que crearan páginas web falsas o enviaran spam a cuentas de correo electrónico con la intención de estafar a los usuarios podrían recibir una

multa de hasta $250,000 USD y penas de cárcel por un término de hasta cinco años.

Algunos estados tienen leyes que tratan las prácticas fraudulentas o engañosas o el robo de identidad y que también podría aplicarse a los delitos de phishing. [8]

CONVENIO DE BUDAPEST: También conocido como el Convenio sobre cibercriminalidad, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Japón y China.

El 23 de noviembre de 2001 se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004. A partir del 28 de octubre de 2010, 30 estados firmaron, ratificaron y se adhirieron a la Convención, mientras que otros 16 estados firmaron la Convención, pero no la ratificaron.

El 1 de marzo de 2006, el Protocolo Adicional a la Convención sobre Cibercrimen entró en vigor.

En su Título II "Delitos Informáticos", Artículo 8 establece:

> *"Fraude Informático: Las partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:*
>
> *a- la introducción, alteración, borrado o supresión de datos informáticos; b- cualquier interferencia en el funcionamiento de un sistema informático; con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona."*[9]

[8] *http://es.wikipedia.org/wiki/Phishing*

[9] CONVENIO SOBRE LA CIBERDELINCUENCIA, BUDAPEST.

CONCLUSIÓN

La actividad del legislador llevada a cabo en la elaboración de la norma que consagra y regula el delito de fraude informático no alcanza a abarcar todos los aspectos y consecuencias que conlleva el delito de PISHING, el cual se configura con la obtención ilícita de datos personales (usualmente el tipo de datos que se extrae de la víctima son códigos de tarjetas bancarias o de servicios financieros para estafarla y obtener información confidencial de forma fraudulenta),- puesto que si bien exige dolo directo por parte de quien lo comete, en cambio no exige que estén presentes otros elementos como el "engaño" o el "error", (requisitos esenciales para que se configure el delito de estafa Art. 172 C.P), a lo que se suma que el acto de disposición patrimonial no es realizado por la víctima de un engaño -como en la estafa común-,sino por el propio autor del delito, a través del sistema informático. Tampoco encuentran regulación otros aspectos del Pishing como ser las diferentes técnicas que se llevan a cabo para la comisión del mismo.

Con el avance de la Sociedad de la Información se ha ido incorporando en cada sistema jurídico un progresivo entramado de parches compuesto por nuevos institutos o sucedáneos electrónicos de otros originariamente previstos para su formalización en soporte papel.(9) Surgen así, nuevas figuras delictivas que pueden ser incorporadas a otras ya existentes o que por el contrario necesitan de una técnica legislativa que asegure una más acabada regulación de sus contenidos. Tal es el caso del PISHING: por un lado se observa su correcta inclusión en una figura delictiva como la es la del fraude informático, pero por otro lado se ven los esfuerzos proyectados en lograr una ley que lo aparte y lo eleve a la categoría de ser considerado un delito autónomo del fraude informático, y reconozca sus propias particularidades con el fin de penar a quienes lo cometan por cada uno de los medios utilizados para cometerlo.

BIBLIOGRAFÍA:

(1)- ***Marcos Salt, Profesor de Derecho Penal y Procesal (UBA) ,POLICIALES DELITOS INFORMÁTICOS: Los interrogantes que se están planteando en nuestros tribunales, Diario Clarín en*** *http://www.clarin.com/policiales/interrogantes-planteando-tribunales_0_859114225.html*

(2)- ***Gustavo A. Arocena, LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL ARGENTINO –INTRODUCCIÓN A LA LEY NACIONAL N°26.388***

(3)- *http://es.wikipedia.org/wiki/Phishing*

(4)- *http://www.infospyware.com/articulos/que-es-el-phishing/*

(5)-*http://web.ua.es/es/contratos-id/documentos/itipupdate2011/moya.pdf*

(6)- ***Ernesto Liceda, Límites de la equivalencia funcional (y de la comodidad de Legislador) en el Derecho Penal, en*** *http://www.39jaiio.org.ar/sites/default/files/39jaiio-sid-17.pdf*

(7)- ***Ernesto Liceda, Límites de la equivalencia funcional (y de la comodidad de Legislador) en el Derecho Penal, en*** *http://www.39jaiio.org.ar/sites/default/files/39jaiio-sid-17.pdf*

(8)- *http://es.wikipedia.org/wiki/Phishing*

(9)- CONVENIO SOBRE LA CIBERDELINCUENCIA, BUDAPEST, en *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF*