La captación ilegítima de datos confidenciales como delito informático en Argentina.

Lic. Cristian Borghello[1]; Abog. Marcelo G. I. Temperini[2]

Abstract Español. La actividad conocida como phishing, se encuentra en pleno auge en América Latina, donde representa un área en constante crecimiento. Técnicas de engaño, desde las más simples y clásicas hasta las más complejas y creativas, son diaramente ejecutadas y modificadas, buscando localizar vectores de ataque que posean un mayor porcentaje de éxito en las víctimas. Este trabajo se propone desarrollar las raíces del phishing, explicando su clasificación, su funcionamiento, sus distintas etapas y su mutación a lo largo del tiempo. Desde la óptica jurídica, se realizará un análisis crítico sobre su regulación legal en Argentina y en el derecho comparado, finalizando la investigación con la propuesta de un tipo penal que sancione la captación u obtención ilegítima de datos confidenciales, así como de otras actividades relacionadas al proceso.

Abstract en Inglés: The activity known as phishing, is booming in Latin America, which represents an increasing area. Deception techniques, from simple and classic to the most complex and creative, are executed and amended every day, seeking to locate attack vectors that have a higher success rate on the victims. This work aims to develop the roots of phishing, explaining its classification, its operations, its various stages and its mutation over time. From a legal viewpoint, there will be a critical analysis of its legal regulation in Argentina and in comparative law, ending the investigation with a new proposal to punish the unlawful acquisition or obtaining of confidential data and other related activities process.

Keywords: delitos informáticos, captación ilegítima de datos, información, confidencialidad, seguridad de la información, phishing.

[1] Licencido (UTN) en Sistemas y certificado internacional en seguridad de la información. Creador y Director de los sitios Segu-Info –www.segu-info.com.ar– y Segu-Kids –www.segu-kids.org– especializados en Seguridad de la Información Seguridad para la familia. Contacto: info@segu-info.com.ar

[2] Abogado (UNL) especializado en Derecho Informático. Director de la Red Iberoamericana de Derecho Informático – elderechoinformatico.com. Analista de Seguridad y Director de AsegurarTe – Consultora en Seguridad de la Información Contacto: temperinimarcelo@gmail.com

Introducción

Las actividades informáticas delictivas están en pleno auge en América Latina, donde representan un área en contínuo crecimiento.Un importante abanico de técnicas, desde las más simples y clásicas hasta las más complejas y creativas, son diaramente ejecutadas y modificadas, buscando localizar vectores de ataque que posean un mayor porcentaje de éxito en las víctimas. Estas actividades, impulsadas tanto por el incremento de la tasa de usuarios conectados a Internet, así como por el aumento en la utilización del sistema financiero en línea, brindan cada vez mayor cantidad de potenciales víctimas para los delincuentes informáticos dedicados a la recolección ilegítima de información privada.

En este sentido, la inmensa cantidad y diversidad de tipos de engaños existentes, son directamente proporcionales al grado de inventiva e imaginación del delincuente, así como también al nivel de inocencia / ingenuidad / ignorancia de la víctima. Sin embargo, es posible establecer un denominador común entre todos ellos: el uso de la tecnología como herramienta para llevar adelante los engaños y fraudes (en el sentido común del vocablo). En este trabajo se desarrollará particularmente el caso del "phishing", uno de los flagelos de mayor impacto y crecimiento de la era de la información, analizando sus etapas, sus raíces, su regulación legal y finalmente, realizar una propuesta tendiente a su mitigación.

La expansión del Derecho Penal

Partiendo de la concepción de la "Sociedad de Riesgo" del sociólogo Ulrich Beck, la actualidad está marcada por un avance o expansión del derecho penal hacia ramas o acciones que antes no se encontraban reguladas. Dentro de esas acciones, la ciberdelincuencia encuentra un lugar importante, junto a otros temas en crecimiento, como la protección del medio ambiente. Sucede que algunas de las acciones clásicas, combinadas con las variadas posibilidades que ofrecen las nuevas tecnologías, dan lugar a acciones más dañosas y masivas (exponencialmente) que antes.

Sumado a ello, los delitos informáticos siguen siendo un desafío trasnacional, toda vez que su comisión es posible en cualquier instante, desde cualquier lugar del mundo, y aquellos países que no avanzan en la materia, se convierten rápidamente en *paraísos jurídicos – penales* para el accionar de los delincuentes. El derecho penal moderno, sin reducir su función de protección de los bienes jurídicos clásicos (la vida, el patrimonio, etc.) se expande haciéndose cargo de nuevas acciones delictuosas que no encuentran efectiva contención por otras fases menos extremas del derecho (rama civil o administrativa). Según el autor Andrés Saravia, *"hay cambio de rumbo del Derecho Penal, el cual no es ya aquel que reaccionaba frente al hecho lesivo, sino que ahora, dentro de un ámbito más a lo general, se expresa a través de la gestión de riesgos"*.

Phishing: Primera etapa

La primera cita a la palabra "phishing" se puede encontrar en el popular grupo de noticias de ***hacking alt.2600*** en enero de 1996, cuando varios delincuentes obtuvieron datos y contraseñas de usuarios de AOL (***America On Line***). Este vocablo "phishing" fue acuñado por ser la contracción de ***"Password Harvesting Fishing"***, literalmente "cosecha y pesca de contraseñas", donde se destaca que en su propio nombre no se menciona el método ni el objetivo para el cual esos datos son recolectados.

En 1997, esta técnica ya era ampliamente conocida y utilizada para obtener datos y comercializarlos en el mercado negro. En todos los casos analizados, se hace referencia al uso de técnicas de ingeniería social, donde se engaña y manipula psicológicamente a la víctima para que revele datos que no brindaría en circunstancias normales (***lure***). En estos casos, el engaño se efectúa a través del uso de cualquier medio de comunicación tecnológico como el teléfono, fax, correo electrónico, chat, SMS, etc. Más allá de lo expuesto, cabe aclarar que la dificultad en la conceptualización de esta técnica, viene relacionado a que su práctica y caracterización ha ido mutando constantemente.

Atento a ello, y en la búsqueda de encontrar una clasificación que permita mejorar la comprensión de estos delitos, se pueden distinguir dos fases perfectamente diferenciadas.

La primera fase consta de la obtención de información confidencial o sensible del usuario a través de las distintas técnicas. En este caso el delincuente toma contacto con la víctima a través de cualquier medio de comunicación y, con un componente de ingeniería social, engaña al usuario para que entregue voluntariamente la información solicitada (nombres de usuario, contraseña, números de cuenta, PIN, tarjetas de crédito, etc.).

La forma más tradicional de llevar adelante esta etapa es realizar el envío masivo de correo electrónico no deseado -spam- a miles o millones de direcciones previamente recolectadas para lograr, posteriormente, que el usuario ingrese a un sitio web similar al de una entidad de confianza y coloque allí la información necesaria para concretar la segunda etapa. Si bien una importante cantidad de casos busca obtener los datos financieros de la víctima (para concretar futuras estafas), vale destacar que esta primera fase no debe considerarse como asociada o vinculada exclusivamente al fraude informático, error muy común en el ámbito de los delitos informáticos.

Esta etapa inicial de captación ilegítima de datos, puede ser utilizada para obtener cualquier tipo de información de utilidad para el delincuente, tales como datos de autenticación (***login***), datos de una cuenta de red social, blog, cuenta bancaria o casilla de correo, incluso hasta información mas puntual, como los secretos industriales de una empresa, que son obtenidos por el delincuente mediante trampas (engaños/***lure***) especialmente diseñadas para esos fines.

En esta fase también es común la utilización de técnicas específicamente tecnológicas como los programas dañinos (***malware***) y la explotación de debilidades en el sistema operativo y aplicaciones instaladas por el usuario (vulnerabilidades o ***bugs***) pero, al margen de la metodología aplicada, el objetivo sigue siendo la obtención de información de la víctima.

En un análisis realizado durante 2011 por Segu-Info, se consultó sobre las entidades de las cuales es más común recibir correos electrónicos falsos. En este caso los sitios bancarios/financieros alcanzaron el primer puesto, seguidos muy de cerca por el phishing de redes sociales, los *webmail* y los sitios de compra/venta/subasta de productos.

Phishing: Segunda etapa

Concluida la primera etapa de captación de los datos del usuario, se procede a una segunda etapa, donde el delincuente se encuentra con un espectro de posibilidades diversas. Si bien como mencionamos, las estadísticas demuestran que tradicionalmente aquí el delincuente comienza a utilizar los datos obtenidos para obtener beneficios económicos perjudicando el patrimonio de la víctima, con el tiempo la actividad se ha ido desprendiendo de esta finalidad casi exclusiva, existiendo en la actualidad un crecimiento de las otras opciones que se pueden realizar con los datos captados. Aquí presentamos un listado de las opciones mencionadas:

- Venta de la información obtenida a otros delincuentes en el mercado negro. En este caso la información cotiza de acuerdo al grado de plenitud y exactitud (no es lo mismo una base de datos con el nombre de usuario y contraseña que aquella que además contiene el número de tarjeta de crédito y su PIN). Esta actividad no se encuentra tipificada actualmente en Argentina.
- Extracción directa de dinero de las cuentas obtenidas. Esta actividad si se encuentra tipificada en Argentina (art. 173 inc. 16 CP) y es la calificada como “fraude informático”. A su vez, reviste diferentes opciones:
  - Realización de transferencias de manera directa por el delincuente a cuentas propias (poco frecuente por su posibilidad de rastreo).
  - Utilización de “mulas”, aquellas personas que, de forma inocente y generalmente sin conocimiento, facilitan su cuenta bancaria para realizar movimientos de dinero obtenido de transacciones fraudulentas. Este tipo de acción, calificado como “lavado de dinero”, generalmente se realiza a través de la captación de víctimas con ofertas de trabajos sencillos y demasiado bien remunerados (“trabaje 2 hs desde su casa y gane $5.800”).
- Adquisición de bienes o servicios a través de canales virtuales que no soliciten la presencia del titular o de su documentación. En este tipo de fraude es común la compra de crédito para líneas de teléfono móvil. Esta actividad si se encuentra tipificada en Argentina (art. 173 inc. 16 CP).
- Ejecución de una “broma” a la víctima, donde se establecen comunicaciones o se generan perfiles falsos en su nombre. Esta actividad es muy común en los jóvenes y es generalmente llevada a cabo en las redes sociales y chats. No se encuentra tipificada en Argentina (aunque podría existir el delito de injurias para casos graves).

- Suplantación de identidad de la víctima, provocando un daño patrimonial -estafas- o personal -injuria, daños a la reputación, lesión al honor- en nombre de la víctima. Esta actividad no se encuentra tipificada en Argentina, excepto para casos de estafa, que opera como delito autónomo.
- Publicación de la información obtenida en Internet. En ocasiones, el delincuente se limita a captar ilegítimamente los datos para posteriormente "colgarlos" en la red, a sabiendas que su difusión generará consecuencias en los medios y en la opinión pública sobre la empresa u organismo encargado de la seguridad de esos datos.
- Colección personal. Pueden existir casos donde el sujeto que capto la información, decida no utilizarla en ninguna de las alternativas descriptas, limitándose a recolectarlas de manera privada sin posterior uso.

En orden a lo desarrollado sobre la primera y segunda etapa de esta actividad, nos encontramos ya en condiciones de poder desarrollar un concepto sobre que debemos considerar como phishing. De acuerdo a nuestra posición, debe considerarse "phishing" a la práctica de la obtención ilegítima de datos confidenciales, independientemente de la opción que se busque realizar en una segunda etapa con esos datos. Es decir, consideramos que el phishing existe de manera plena y completa dentro de la primera fase ya explicada, independientemente de la actividad posterior que realice el delincuente. Definida la clasificación de las etapas, se hace imprescindible el análisis profundo de los motivos del robo de información y el debate sobre la necesidad de tipificación de la captura ilegítima de datos confidenciales, concebida como acto preparatorio raíz de diferentes tipos de problemas.

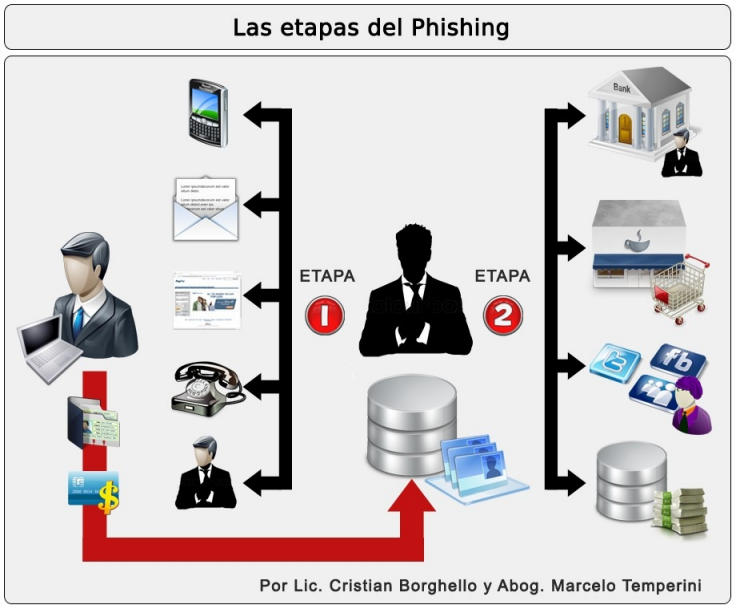

Imagen 1 – Diferenciación de etapas en la actividad del *Phishing*

Ganancias de los ciberdelincuentes

Hasta aquí se han analizado los métodos para obtener la información sensible destacando que uno de los principales objetivos (pero no el único) del delincuente es el beneficio económico a través de la utilización de los datos robados.

Según un estudio realizado a principios de 2011 por la empresa de seguridad Panda, *"El mercado negro del cibercrimen funciona como cualquier otro tipo de negocio y cuenta con todos los ingredientes que un comprador necesita para confiar en el vendedor. Por ejemplo, existe la competencia y la ley de la oferta y la demanda que los obliga a ajustar los precios y a ofrecer descuentos por volumen"*.

En este mundo *undeground* de internet se puede conseguir una tarjeta de crédito sin garantía de saldo por U$S 2 -y U$S 80 con garantías-; máquinas duplicadoras de tarjetas físicas de U$S 200 a U$S 1.000; el servicio de blanqueo de dinero a cambio de comisiones que pueden ir desde el 10 hasta 40% del total de la operación; alquiler de redes para el envío de spam a través de sistemas infectados (*botnet*), desde U$S 15.

Con respecto al phishing, durante enero de 2012, Segu-Info públicó el primer informe con estadísticas de América Latina y datos sobre la cantidad de casos, países y entidades afectadas, las técnicas de propagación utilizadas y el dinero recaudado por los delincuentes:

- Los datos de una tarjeta de crédito clásica pueden ser vendidos a un promedio de U$S 10 y aumentar de acuerdo al tipo de tarjeta (*gold*, *platinum*, *black*, etc.).
- Los montos extraídos de las cuentas afectadas generalmente no son demasiado altos y se evita el vaciado de la cuenta, de forma de minimizar la probabilidad de que la víctima se percate y efectúe la denuncia, o bien que en caso de darse cuenta, el costo y desgaste de los trámites sean mayor al dinero efectivamente robado. Los montos están en el rango de U$S 30 a U$S 400.
- El 12,6% de los usuarios que reciben un correo fraudulento, ingresan al sitio falso y brindan sus datos personales al delincuente.
- Considerando (en forma optimista) que el delincuente sólo roba U$S 30 de cada cuenta obtenida, estaría logrando al menos U$S 4.770 en 10 días "de trabajo" (U$S 174.105 anuales).

Al margen de que siempre se afecta al usuario, las empresas y organizaciones también sufren daños y pierden dinero cada vez que su imagen es relacionada a un caso de phishing. Sobre este aspecto, un estudio realizado por LACNIC sobre el panorama del ciberdelito en América Latina señala que *"las pérdidas totales para los bancos de Latinoamérica al afrontar los costos del phishing serían de 93.000 millones de dólares estadounidenses por año"*.

Sin embargo, un estudio publicado por INTECO destaca que, *"a pesar de las perdidas económicas de los afectados, no se produce un abandono masivo de los servicios de banca ni compra online"*. En este aspecto, es importante señalar que las entidades bancarias, al no ver afectadas sus actividades (merma en la utilización de los servicios), prácticamente no realizan ningún tipo de acción proactiva ni de prevención de casos de phishing, más allá de las escasos notas de prensa publicadas

en sus sitios web informando al usuario sobre los riesgos de no proteger sus datos personales o del escaso seguimiento realizado en casos de que un cliente se vea afectado.

Otro aspecto a señalar es que la cantidad de dinero "perdido" generalmente está asegurado (a expensas del cliente) y por lo tanto, la entidad no pierde desde el punto de vista económico, desalentándose así las acciones proactivas por combatir estos delitos.

Cuando un cliente es estafado (en el sentido que se le realizó un perjuicio patrimonial por un tercero), la entidad afectada puede actuar de diferentes maneras ya que no existe un procedimiento normado para dar respuesta al cliente. La entidad puede optar por ignorar el caso, investigarlo, dejar pasar el tiempo con trámites burocráticos a costa del cliente (y que finalmente costarán más que la estafa en sí misma), pagar una indemnización, devolver el dinero perdido por el cliente o simplemente rechazar el pedido culpando al usuario de su "excesiva confianza al utilizar internet".

Explotar las vulnerabilidades del usuario

En un gran porcentaje de los casos, el éxito de los engaños consiste en aprovecharse de la ignorancia de los usuarios sobre las técnicas utilizadas por los delincuentes. El informe de INTECO, confirma que el término phishing es conocido por sólo el 41,2% de los usuarios de internet españoles.

En el estudio de phishing de Segu-Info se consultó a los usuarios si creían saber reconocer un caso de phishing y el 68% de los consultados dijo conocer positivamente un correo que pretende engañarlo para robar sus datos sensibles. Sin embargo, luego el informe prueba que el usuario desconoce que el mensaje puede ser creado de forma apócrifa falseando ciertos campos del correo (*spoofing*), haciéndolo parecer verdadero. Esta situación genera una falsa sensación de seguridad en los usuarios porque efectivamente ellos "creen" que pueden identificar un caso de phishing, lo que los vuelve más propensos a caer en la trampa cuando el correo recibido esté correctamente manipulado y sus autores hayan puesto mayor esfuerzo en hacerlo pasar por verdadero.

A las luces de la cantidad de casos de phishing que aparecen cada día y de la cantidad de clientes afectados, se destaca la necesidad de implementar mayor cantidad de controles proactivos por parte de las organizaciones y entidades afectadas, así como la realización de campañas de concientización orientadas a que los usuarios comprendan el riesgo que existe en el uso inadecuado de los medios electrónicos y en las actividades que realizan con sus cuentas a través de dichos medios.

Responsabilidad compartida

En relación al análisis de las distintas responsabilidades que incumben a cada parte involucrada en este tipo de actividades, surgen al menos tres que se detallan a continuación:

- El delincuente, como agente activo, que con distintos ardides planea y ejecuta la acción. Pueden existir otros agentes intermedios que colaboren en la ejecución pero se puede incluir a todos ellos en el mismo grupo delictivo.
- El servicio, prestado por una empresa u organización cuya imagen es tomada por el delincuente para llevar adelante la acción fraudulenta (se produce aquí un caso de robo de identidad a la empresa u organismo utilizado para engañar al usuario).
- El cliente o usuario afectado, como actor pasivo del delito.

En cuanto al primer ítem, desde hace tiempo los delincuentes se han comenzado a agrupar en organizaciones delictivas (crimen organizado) y jerárquicas que les permite aprovechar la experiencia y técnica de cada una de las partes involucradas. En este sentido, el FBI ha tipificado al menos diez "profesiones o especializaciones" relacionadas con el cibercrimen: programadores, distribuidores, expertos, investigadores, defraudadores, proveedores de *hosting*, vendedores, muleros, blanqueadores y líderes. Una vez comprendida la acción criminal del agente activo, cabe preguntarse ¿existe responsabilidad por parte del cliente, por creer en el ardid o engaño? ¿cuál es la responsabilidad de la entidad que presta un servicio, por no actuar parar prevenir la posible acción delictiva? Acción que es conocida, previsible y practicada en forma masiva en todo el mundo.

La respuesta a estas preguntas no es sencilla y para contestarla INTECO entrevistó a distintos expertos que, si bien no coincidían en algunos detalles, acuerdan que existe responsabilidad compartida: *"Tratándose de un fenómeno basado en la ingeniería social, el usuario ha de asumir cierta responsabilidad en este tema, manteniendo un comportamiento prudente y seguro a la hora de usar dichos servicios"*.

BankersOnline, un popular sitio de gurús bancarios, sostiene que *"La negligencia del consumidor no reduce sus derechos porque las reglas deberían estar hechas para alentarlos y protegerlos"*. Para reforzar esta idea, en uno de los primeros fallos internacionales sobre esta discusión, un banco de la India fue condenado a pagar todos los gastos y pérdidas que afectaron a su cliente, aun cuando el cliente había procedido con negligencia. Así mismo, otro banco de EE.UU. fue encontrado responsable por las pérdidas que sufrió un cliente a través de un caso de phishing, porque *"el banco no cumplía con las medidas de seguridad adecuadas de acuerdo con los estándares de la industria"*.

Los problemas en la tipificación argentina

En Argentina, normalmente se considera que el phishing fue tipificado en junio de 2008, a través del art. art. 9 de la Ley Nº 26.388. Ello es así teniendo en consideración lo explicado precedentemente, entre las diferencias conceptuales sobre su calificación. En este sentido, en el presente se considera que la tipificación vigente en nuestro país no es la adecuada para combatir este tipo de delitos, por los motivos que se detallan a continuación.

Se debe comenzar por analizar el artículo mencionado sobre Delitos Informáticos, aunque para comprender su redacción, es necesario establecer el contexto de los

demás artículos que referencia, particularmente el texto del art. 172 y 173[3] del Código Penal Argentino:

> ***Art. 9º*** *- Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente:*
>
> ***Inciso 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.*

De acuerdo a los artículos citados, el phishing estaría regulado en Argentina en el inciso 16 del art. 173, por lo tanto, sería un tipo especial de la estafa clásica del art. 172. Siendo así, es menester consultar la doctrina clásica penal del delito de estafa, para así saber cuando quedará configurado el tipo. Citando la impecable explicación del destacado penalista Edgardo Donna, quien afirma que: "*En la estafa el bien jurídico no es, como podría pensarse, la "buena fe en el tráfico" o la "lealtad en las operaciones" sino el patrimonio. El ardid y engaño previstos en el tipo como formas de comisión constituyen simplemente los medios con los que se produce el daño patrimonial del sujeto pasivo, de modo que el quebrantamiento de la buena fe es el modus operandi que va a determinar la lesión jurídica patrimonial, pero no el objeto de la tutela, ni directa ni indirectamente. Si la buena fe fuese el bien jurídico amparado, la consumación del delito debería producirse con la sola realización del engaño, sin necesidad de que ocasione perjuicio patrimonial alguno, solución que resulta inaceptable desde el punto de vista legal"*.

En relación a lo expuesto, se precisa que para la configuración del delito de estafa y por lo tanto, del tipo especial del inc. 16 para "phishing", debe existir primero el ardid o engaño y luego un perjuicio patrimonial consecuencia de dicho engaño.

Estamos aquí ante el gran inconveniente que tiene la actual tipificación argentina, dado que la mayoría de las conductas consideradas como delictuosas, no reúnen estos requisitos. Sólo se configuraría el tipo especial de estafa del art. 173 inc. 16 para el caso de que el delincuente, no sólo realice el ardid o engaño para capturar los datos de la víctima, sino que además posteriormente realice alguna transferencia bancaria o adquisición de bienes o servicios a nombre de la víctima, provocándole allí el perjuicio patrimonial exigido para cualquier estafa, y perfeccionándose recién en ese instante el tipo penal.

En la descripción realizada sobre el funcionamiento del phishing, se ha señalado la proliferación de personas dedicadas exclusivamente a la captación ilegítima de datos confidenciales (phishing propiamente dicho según el concepto defendido en este trabajo), pero que luego optan por otras alternativas diferentes a la estafa tradicional a la víctima. Es decir, la mayoría de los casos de phishing, actualmente no son delito en Argentina, puesto que según la estrategia jurídica utilizada por el legislador, se exigen

---

[3] Art. 172.- Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negación o valiéndose de cualquier otro ardid o engaño.
Art. 173.- Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece: Inc. 1º. El que defraudare a otro en la substancia, calidad o cantidad de las cosas que el entregue en virtud de contrato o de un título obligatorio...

los elementos típicos de la estafa, y por consiguiente, se necesita que exista perjuicio patrimonial para que exista delito.

Entonces, ¿Qué utilidad tiene el actual inciso? Concretamente lo que se encuentra tipificado en el inc. 16 del art. 173 es la estafa o fraude informático (una de las posibles alternativas en la segunda etapa analizada previamente). Es valioso destacar la jurisprudencia por caso de fraude informático, una causa[4] de agosto de 2010 en donde se procesó a dos personas como coautores del delito de defraudación previsto en el art. 173 inc. 16 del Código Penal. Se les imputó *"haber llevado a cabo maniobras de fraude mediante la técnica de manipulación informática conocida por "phishing" -página paralela-, por la que obtuvieran los datos necesarios –código de transferencia y número de tarjeta de crédito-para poder operar en las cuentas bancarias"*. En palabras del juez, *"Que no se hayan verificado en el caso, todos los pasos del procedimiento del "Phishing" como alega especialmente la asistencia técnica de G. o que no se haya determinado de qué computadora se realizaron las transferencias, no altera de momento los graves indicios cargosos"*. Como se afirmaba anteriormente, en el caso fue posible la imputación y condena del delito, por haberse producido el perjuicio patrimonial a la víctima (dos transferencias, de $ 780 y $ 770).

Alterar el normal funcionamiento.

Los inconvenientes en la tipificación argentina no cesan en lo ya desarrollado. Repasando nuevamente el inciso 16 del artículo 173, se observa que su aspecto objetivo exige que la defraudación se realice *"mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos",* destacando de manera positiva el hecho que el legislador adoptó una técnica legislativa amplia para incluir cualquier tipo de técnica de manipulación informática, sin señalar alguna en particular.

El problema mencionado surge de su detalle, que exige que exista una *"alteración del normal funcionamiento"***.** Esto significa que, por ejemplo, para que exista delito el delincuente debe realizar una acción como ingresar al sitio web oficial de una entidad, modificar su código de manera que el sistema, cada vez que un usuario intente acceder, envíe sus datos a una base de datos alternativa, que posteriormente utilizaría para producir el perjuicio patrimonial (o no, según lo ya explicado en la sección anterior).

Esto es un problema (grave) considerando que, en la actualidad en ningún caso el delincuente altera el normal funcionamiento del sistema original, sino que elabora su propio sistema, engañando al usuario para que crea que se trata del original, y es allí donde realiza la captura de datos. Es decir, es más fácil y menos riesgoso para el delincuente, construir un sistema propio con fines de engañar al usuario, que *crackear* el verdadero sistema de la empresa u organización.

[4] CN Apelaciones en lo Criminal y Correccional de la Capital Federal, Sala VI, "G., R. y otro s/procesamiento" (Causa Nº 39779) 3/8/2010

En base a la suma de los dos inconvenientes desarrollados, es que se fundamenta la opinión sobre que en la actualidad, en Argentina no se encuentra debidamente sancionada la práctica de phishing.

Derecho Comparado

En relación a la tipificación del phishing en diferentes países, nuevamente se debe utilizar la clasificación realizada inicialmente en la presente investigación. En ese sentido, en general se puede encontrar una buena cantidad de países que poseen regulación sobre el fraude informático (como anteriormente se explicó el caso argentino). Entre las legislaciones más modernas se puede citar la Ley sobre Crímenes y Delitos de Alta Tecnología de República Dominicana, norma especial a destacar por la seriedad en el tratamiento de los delitos informáticos, donde incluso se regula aspectos de derecho procesal penal para combatir el cibercrimen. En el texto de la misma, se encuentran los artículos 14 y 15 donde se regula la obtención ilícita de fondos[5], así como su transferencia electrónica y la estafa informática[6].

Dentro de la segunda clasificación, sobre el phishing propiamente dicho, se encuentran países que más allá de la clásica tipificación del fraude informático, incorporan la tipificación de la captación ilegítima de datos. En esta postura se puede citar legislaciones también actuales como Colombia[7], en cuyo art. 269F sanciona a quien *"sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes"*. En el artículo siguiente (art. 269G), la misma norma sanciona a quien *"con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes"*.

Regulaciones más precisas en esta segunda tendencia, las podemos localizar dentro de los EE.UU., como por ejemplo en New York, en cuya *Anti-phishing Act*[8] se

5 Ley No. 53-07. Rep. Dom. Art. 14.- Obtención Ilícita de Fondos. El hecho de obtener fondos, créditos o valores a través del constreñimiento del usuario legítimo de un servicio financiero informático, electrónico, telemático o de telecomunicaciones, se sancionará con la pena de tres a diez años de prisión y multa de cien a quinientas veces el salario mínimo.
Transferencias Electrónica de Fondos. La realización de transferencias electrónicas de fondos a través de la utilización ilícita de códigos de acceso o de cualquier otro mecanismo similar, se castigará con la pena de uno a cinco años de prisión y multa de dos a doscientas veces el salario mínimo.

6 Ley No. 53-07. Rep. Dom. Art. 15.- Estafa. La estafa realizada a través del empleo de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con la pena de tres meses a siete años de prisión y multa de diez a quinientas veces el salario mínimo.

7 Ley 1273 de 2009. Diario Oficial No. 47.223 de 5 de enero de 2009. Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html [28/02/2012]

8 New York General Business - Article 26 - § 390-B. Inc. 3. It is unlawful for any person, by means of a web page, electronic message, or other use of the internet to solicit, request or collect identifying information by deceptively representing himself or herself, either directly

sanciona a cualquier persona que, a través de medios electrónicos, solicite, requiera o colecte información personal para representar de manera engañosa, a una empresa u organismo del gobierno, sin contar con su autorización. Similar redacción posee el Código de Illinois[9], donde "*It is unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing himself, herself, or itself to be a business without the authority or approval of the business*". Entre sus diferencias se puede observar la inclusión de las personas físicas como sujeto pasivo del delito, así como la ampliación en los verbos, al incluir a "cualquier acción que induzca a una persona a proveer su identificación personal".

Convenio de Cibercriminalidad de Budapest

El Convenio de Cibercriminalidad de Budapest[10], fue adoptado por el Comité de Ministros del Consejo de Europa en el año 2001, como proyecto destinado a armonizar las legislaciones de los estados miembros (47 miembros y 8 observadores al día de la fecha) y abierta a otros países como Australia, Japón, Canadá, Sudáfrica y los EE.UU. Este acuerdo internacional tiende a regular todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional), tratando con carácter prioritario la construcción de una política penal de cooperación internacional contra la ciberdelincuencia.

Actualmente varios países (entre ellos Argentina) están en vías de adhesión y por lo tanto deben tener en consideración sus lineamientos, dado que desde la fecha de aprobación se computa un plazo donde el nuevo país miembro debe adecuarse a dicho instrumento. En cuanto al derecho penal, la modificación de la Ley Nº 26.388 fue pensada teniendo en vistas este Convenio, de manera que buena parte se encuentra ya regulado, aunque las modificaciones más importantes serían en materia procesal penal de y acción real contra el cibercrimen (como por ejemplo, disponiendo de Centro de Atención 24x7 para incidentes y delitos informáticos).

Entre algunos de los aspectos a adecuar en materia de derecho penal material, se encuentra el tema tópico de esta investigación. En relación al mismo se destaca el art. 6 del Convenio, que expresa:

> ***Artículo 6. Abuso de equipos e instrumentos técnicos***
>
> *1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:*

---

or by implication, to be a business or a governmental entity and doing so without the authority or approval of such business or such governmental entity.
http://law.onecle.com/new-york/general-business/GBS0390-B_390-B.html [28/02/2012]

9 Illinois Compiled Statutes 740 ILCS 7 Anti-phishing Act. Section 10.
http://law.onecle.com/illinois/740ilcs7/10.html [28/02/2012]

10 Council of Europe. "Convenio de Cibercriminalidad de Budapest". Budapest, 23 de noviembre de 2001.
http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF [08/03/2012]

a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición

1. de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados

2. de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5; y

b. la posesión de alguno de los elementos descritos en los parágrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal.

Como se puede observar, es menester que el país interesado, tenga penalmente sancionada las acciones descriptas: *"producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de hacking, cracking, interceptación ilícita de datos o denegación de servicios"*. En el segundo párrafo (inc. 2 del art. 6), se completa el esquema exigiendo la tipificación de la "*obtención para su utilización... de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5…."*. Las infracciones citadas de los artículos 2 a 5 del Convenio, ya encuentran regulación en el sistema penal argentino[11].

Es decir, acertadamente el Convenio propone la tipificación de la captación u obtención ilegítima de datos confidenciales, así como las actividades relacionadas en estos procesos.

Conclusiones

Que, como se ha desarrollado a lo largo de la presente investigación, se hace evidente la necesidad de combatir el phishing en Argentina, a la luz que es una de las actividades delictivas de mayor crecimiento y fundado en que estas acciones son el primer eslabón en la cadena de gran parte de los delitos informáticos.

Que, siguiendo esa línea de trabajo, se propone la punición de las actividades relacionadas a la captura ilegítima de información, por considerarse que ello sería atacar un aspecto medular del cibercrimen, toda vez que tender hacia su mitigación

[11] Art. 2. Acceso ilegítimo (hacking): tipificado en el art. 153 bis; Art. 3. Interceptación ilícita: tipificado en el art. 153 2do párrafo; Art. 4. Atentado contra la integridad de los datos (cracking): tipificado en el art. 183 2do párrafo (daño informático); Art. 5. Atentado contra la integridad de un sistema (denegación de servicio): tipificado en el art. 197 (interrupción de comunicaciones).

sería tomar una medida de importantes consecuencias en la disminución de otros delitos informáticos de mayor complejidad.

Que, si bien se destaca la necesidad de contar con una legislación actualizada e idónea para combatir los delitos informáticos, su sanción legislativa no es suficiente. Argentina necesita de manera urgente contar con un avance en materia procesal, a fin de instrumentar los mecanismos que permitan obtener los medios probatorios necesarios para condenar a los responsables en este tipo de delitos.

Que, de la misma manera, se hace necesaria la cooperación con otros países, puesto que la transnacionalidad de los delitos informáticos, obliga a tomar medidas de acción con cierto nivel de coordinación para tener éxito.

Que, a través de la nueva legislación se debe buscar dar cumplimiento a las exigencias aún no satisfechas en materia de Derecho Penal Material (Capítulo II) del Convenio de Budapest, artículo 6, inc. a y b.

Por todo lo expuesto, y convencidos que más allá de la utilidad de los análisis y diagnósticos, se debe avanzar hacia la realización de propuestas útiles para intentar brindar herramientas en el combate contra la ciberdelincuencia, se propone la siguiente la siguiente tipificación[12]:

ARTICULO 157 ter. - Será reprimido con prisión de un (1) mes a dos (2) años o multa de pesos diez mil a pesos cien mil el que:

1. Mediante cualquier forma de ardid o engaño, indebidamente obtuviere o captare datos personales, financieros o confidenciales

2. Con fines ilícitos, diseñare, programare, desarrollare, vendiere, ejecutare, facilitare o enviare un dispositivo, sistema o programa informático, destinados a la indebida obtención o captura de datos personales, financieros o confidenciales.

12 Presentado ante el Honorable Congreso de la Nación. Ingresado en fecha 09/09/2011, Expediente Nro. 2257/11
http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=2257/11&nro_comision=&tConsulta=1 [03/03/2012]

Referencias bibliográficas

DONNA, Edgardo y FUENTE, Esteban Javier. "Aspectos generales del tipo penal de estafa". Revista Latinoamericana de Derecho. Año I, núm. 1, enero-junio de 2004, pp. 39-92.

STUTZ, Michael, *"AOL: A Cracker's Paradise?"*. Wired News. 29 de enero de 1998. http://www.wired.com/science/discoveries/news/1998/01/9932 [03/03/2012]

GUNTER, Ollmann, "Phishing Guide: Understanding and Preventing Phishing Attacks". 10 de julio de 2006. http://www.technicalinfo.net/papers/Phishing.html [03/03/2012]

SEGU-INFO. BORGHELLO, Cristian. "Estadísticas de Phishing". Abril de 2011. http://www.segu-info.com.ar/articulos/109-estadisticas-phishing.htm [03/03/2012]

SEGU-INFO. BORGHELLO, Cristian. "Los números de un año de Phishing". Enero de 2012. http://www.segu-info.com.ar/articulos/117-numeros-phishing.htm [03/03/2012]

PANDA SECURITY. "Mercado negro del cibercrimen". Enero de 2011. http://prensa.pandasecurity.com/wp-content/uploads/2011/01/Mercado-Negro-del-Cybercrimen.pdf [02/03/2012]

MSNBC. "Know your rights on bank account fraud". Agosto de 2005. http://www.msnbc.msn.com/id/8915217/ns/technology_and_science-security/t/know-your-rights-bank-account-fraud [04/03/2012]

PALAZZI, P., "Los Delitos Informáticos en el Código Penal – Análisis de la ley 26.388", Abeledo Perrot, (2009)

TOO STEP. "Phishing Frauds--Should banks be made responsible?". Febrero de 2011.

MY BANK TRACKER. *"Who Really Owns Customers' Banking Information?"*. Agosto de 2011. http://www.mybanktracker.com/bank-news/2011/08/05/bank-vs-customer-who-is-responsible/ [04/03/2012]

SARAVIA, Andrés. "Comentarios sobre la expansión del derecho penal. La Vinculación Con La Figura Del Phishing.". 2010.

LACNIC. Proyecto Amparo. "Panorama del ciberdelito en Latinoamérica". Julio de 2011. http://www.proyectoamparo.net/files/LACNIC-PanoramCiberd-VsFinal-20110701.pdf [03/03/2012]

INTECO. "Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing". Octubre de 2007. http://www.inteco.es/file/rmqBMNKZwCoOKzEyqx15mg [03/03/2012]

FBI. "An orthodox report on organized Cyber Crime". Octubre de 2010. http://ezinearticles.com/?An-Orthodox-Report-On-Organized-Cyber-Crime&id=5236455 [08/03/2012]

INFOBAE. "Bajo análisis la adhesión de la Argentina al Convenio Europeo del Ciberdelito". http://www.infobae.com/notas/541142-Bajo-analisis-la-adhesion-de-la-Argentina-al-Convenio-Europeo-del-Ciberdelito.html [12/03/2012]

SILVA SÁNCHEZ, Jesús María, La Expansión del Derecho Penal, 2001, Editorial Civitas, p 136.