Matías Salvi

Leg: VABG37117

Trabajo Final de Graduación

Carrera: Abogacía

“*El Phishing en la Argentina*”

Universidad Siglo XXI

INTRODUCCIÓN

De las distintas herramientas soporte de aquellas modalidades delictivas conocidas dentro del ámbito de los delitos informáticos, el tema de enfoque del presente trabajo de investigación será el "phishing" o suplantación de identidad. El "phishing" es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como "phisher", se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

El trabajo aquí encarado, se encamina a analizar los distintos problemas que giran en torno a conceptualización del "phishing", las distintas modalidades de comisión delictiva que presenta, la pregunta respecto a si todas ellas logran ser abarcadas por la normativa vigente. Por ello, será de gran utilidad profundizar en las lagunas normativas que trae aparejadas, tanto en su ámbito de aplicación de la ley penal, como en la cuestión de la competencia material y territorial. Añadiéndose un interrogante a ser resuelto: ¿Se debe tipificar penalmente la conducta de la obtención de datos personales?

Palabras clave: Phishing, Phisher, Origen, Estafa, Fraude, Delito, Mulas, Bancos, Internet, Antivirus, Antiphishing.

ABSTRACT

In relation to the different support tools of those known criminal modalities within the scope of cybercrime, the focus of this research work will be "phishing" or identity theft. Phishing is a computer term that calls a model of computer abuse and that is committed through the use of a type of social engineering, characterized by fraudulently acquiring confidential information (such as a password, detailed information about credit cards or other information). Bank information). The cybercriminal, known as phisher, is posing as a trusted person or company in an apparent official electronic communication, usually an email or an instant messaging system or even using phone calls.

The present work has focused analyzing the different problems that revolve around the conceptualization of "phishing", the different forms of criminal commission that it presents, if all of them, can be covered by the current regulations. Therefore, it will be very useful to deepen the regulatory gaps that come with it, both in its scope of application of criminal law, and in the question of material and territorial jurisdiction. It also, will delve into the ways, which, it can be fought or prevented.

Keywords: Phishing, Phisher, Origin, Scam, Fraud, Crime, Mules, Banks, Internet, Antivirus, Antiphishing.

INDICE

INTRODUCCIÓN Y MARCO METODOLÓGICO

INTRODUCCIÓN

En la actualidad, el desarrollo en materia informática, se ha visto en un crecimiento exponencial, que parece no tener límite en su avance. Cualquier actividad que se imagine resulta ligada de algún modo al campo informático, esto es, computarizado. No es posible colocar al hombre fuera de los alcances tecnológicos, pues cualquier actividad que se piense, se halla ligada de manera intrínseca con la tecnología, cualquiera que sea. De este modo, resulta que todo lo que rodea al ser humano se asocia en mayor o menor medida con la propia informática. Bastaría pensar en dispositivos electrónicos, como teléfonos celulares, tablets, Smart Tv´s, computadoras portátiles, por mencionar algunos, los cuales, en los tiempos que corren, casi no queda persona alguna que no posea uno de ellos.

La tecnología informática, la misma que conecta a millones de personas en todo el mundo, las cuales se sirven de ella para sus diversas tareas habituales, no sólo ha logrado ser un valioso elemento que ha venido a facilitar y simplificar la vida de las personas, sino que además con su llegada, ha resultado, puesta en las manos equivocadas, convertirse en un elemento o herramienta de extremo peligro por permitir la comisión de diversos delitos, los que hoy se conocen como ciberdelitos o delitos informáticos.

A pesar de considerarse que no existe una enunciación propia del delito informático, se encuentran diferentes concepciones al respecto, ello gracias a la dedicación y aporte de distintos especialistas en la materia, que se han volcado en su investigación y análisis. La propia denominación requiere puntualizar en un tema de manera más específica, entendiendo a los delitos como acciones típicas, contempladas en textos jurídicos penales, Para lograr esa clara concepción, primeramente, se debería asignar la expresión delitos informáticos en el propio Código Penal.

En la legislación argentina, la llegada y promulgación de la Ley N° 26.388, buscó cubrir el vacío legal que la tecnología informática ocasionaba, lo cual se logró, aunque no por completo como se pensaba. Si bien lo que busca la ley penal es castigar aquellas conductas que resulten contrarias al ordenamiento jurídico, la Ley N° 26.388 dejó

entrever que hay conductas que aún, siendo antijurídicas y reprochables, no consiguen ser tipificadas, debido al modo de comisión de las mismas. Es que el delito busca su modo de perfeccionamiento, intentando aventajarse a la normativa vigente. Un caso de ello podría ser el delito conocido como "phishing", el cual se vuelve el tema central de este trabajo. Para ello será necesario analizar las clases conocidas de esta modalidad delictiva, vistas desde el objeto que persigue, como desde sus modos de comisión. De gran utilidad resulta hacer hincapié en el marco legal que el derecho penal argentino le brinda como cobertura a este tipo de modalidad delictiva.

Luego de todo lo referido, la pregunta central que abre la cuestión de análisis del presente trabajo, es ¿debería estar tipificado como delito la obtención de datos personales en nuestro ordenamiento? Considerando que dicha conducta, como génesis del "phishing" no se encuentra actualmente tipificada en la Argentina.

MARCO METODOLÓGICO

Tipo de estudio o investigación:

Se siguió el tipo de estudio principalmente cualitativo. Entendiendo que este tipo de estudio apunta a describir el objeto de estudio, visto desde sus rasgos generales, siendo necesaria la comprobación de una hipótesis. Con la realización del presente trabajo, se intenta analizar la problemática que gira en torno al "phishing" como canal o medio hacia la concreción y comisión de delitos informáticos y cómo éstos conectan con la legislación argentina, sirviendo de apoyo analizar los antecedentes que ayudaron al impulso de la Ley N° 26.388 de Delitos Informáticos, promulgada en junio del año 2.008 y lo que sucede en la actualidad respecto del delito informático cometido bajo la modalidad conocida como "phishing".

Estrategia metodológica:

En el presente trabajo se ha optado por seguir el método conocido como cualitativo, ya que se analiza a la Ley 26.388 desde su promulgación hasta la actualidad, luego de manera más específica, en el momento en que se toma como objeto de estudio al delito de "phishing" y las "lagunas normativas" que pueden presentarse, como en el caso de la determinación de la competencia en materia territorial.

Fuentes utilizadas:

Primarias: Tales como bibliografía ligada a la temática a abordar y jurisprudencia, vista desde fallos dictados a partir de la promulgación de la ley de Delitos Informáticos.

Secundarias: La doctrina, de derecho interno y derecho comparado.

Delimitación temporal/nivel de análisis del estudio:

El estudio se centra temporo-espacialmente, en distintos momentos. Primero se retrotrae a comienzos del siglo XXI, al realizarse un análisis de los antecedentes legislativos que sirvieron como punto de partida para la posterior acogida de la regulación normativa del cyber delito. Posteriormente, el tiempo nos coloca en los días de la entrada en vigencia de la Ley N° 26.388 de Delitos Informáticos en el año 2008 y hasta la fecha actual.

Respecto al análisis de estudio, la investigación se centra en el análisis de legislación, doctrina y jurisprudencia argentinas. Asimismo, se añade el análisis de legislación internacional de derecho comparado, los cuales fueron fuente inspiradora para la recepción en la legislación nacional de la tipificación de los delitos informáticos.

PRESENTACION DEL PROBLEMA DE INVESTIGACION

El punto central respecto del problema de investigación del tema que nos convoca, se funda en el avance exponencial y acelerado de la tecnología informática y su impacto en la sociedad, pero de manera particular nos adentraremos en una modalidad delictiva muy particular, conocida como “PHISHING”. Tal vez, por ser una manera bastante sencilla para expertos informáticos de acceder a datos confidenciales que el común de las personas, sin percatarse deja expuestos y tan accesibles, con la posterior y consecuente obtención de esos datos, los cuales luego servirán de resorte para cometer delitos tales como fraude y estafas, entre otros. Todo ello, lleva a la necesidad de adaptar la legislación vigente, con el fin de volverla más abarcativa, máxime en aquellas áreas donde las herramientas de la informática actúan como facilitadoras del delito.

Quizás lo que más requiere de atención, sea la propia conducta humana frente a los medios tecnológicos de los cuales se sirve, ello en razón de que es por medio del engaño del que se vale el delincuente ante el desconocimiento de su víctima, lo que sirve como el prefecto escenario para lograr su cometido. Es entonces cuando debe entrar en juego la tarea de la prevención del delito, posible únicamente brindando la correcta información a la población.

La Ley N° 26.388 contiene de manera generalizada la tipificación de distintos delitos informáticos, pero no lo hace de manera específica en delitos vinculados con el “phishing”, presentándose así, cierta vaguedad. Por ello, será necesario comenzar a analizar en profundidad, en los siguientes capítulos, esta vaguedad que se piensa, se halla presente en la ley vigente.

CAPÍTULO I:
EL PHISHING EN ARGENTINA

1.1. Concepto y etapas del "Phishing":

En los tiempos que corren no resulta extraño haber oído terminologías como "Hacking", "Spyware", "Malware", "Grooming", "Precking", "Cyberbullying", o "Phishing", y aunque estos nombres resulten llamativos por lo novedosos que se oyen, hoy se sabe que los mismos no refieren a otra cosa, sino a las nuevas modalidades delictivas, cometidas a través de la informática. De las múltiples y variadas clases de delitos informáticos que se conocen a la fecha, nos ocuparemos de manera exclusiva y particular en analizar el llamado "PHISHING". En primer lugar, explicaremos un poco de qué hablamos cuando hablamos de "phishing". El mismo se encuentra en pleno auge en América Latina, donde representa un área en constante crecimiento.

Técnicas de engaño, desde las más simples hasta las más complejas y creativas, son ejecutadas y modificadas a diario, buscando localizar puntos de ataque que permitan un mayor grado de éxito en las víctimas. Este tipo de actividad, tanto por el incremento de usuarios conectados a internet, así como también 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. (ANZIT, TATO, & PROFUMO, 2010, pág. 13).

Resumiendo, para tener un concepto correcto y acabado de la palabra "phishing" diremos, según lo que propone Davara Rodríguez (2002), que esta palabra no se refiere a otra cosa más que "al robo de datos que distintas personas poseen en sus sistemas informáticos" (p.47). Este robo al que se hace mención, puede ser llevado a cabo de las maneras más insólitas e ingeniosas por parte de quienes se ocupan de su comisión, que en muchas ocasiones mejoran y perfeccionan sus técnicas de engaño para conseguir su cometido.

Ahora bien, siguiendo a Téllez Valdez, en su obra sobre delitos informáticos[1], es provechoso, para la investigación desarrollada, analizar el modo en que el autor nos presenta en su trabajo las distintas etapas del "phishing", a saber:

[1] TELLEZ VALDEZ, Julio – Derecho Informático (2009) 4° Ed – Mac Graw Hill

ETAPA 1:

La primera etapa es definida por Telles Valdés como "*fase inicial de extracción ilegítima de datos*". Esta etapa consiste en obtener datos confidenciales del usuario mediante diferentes técnicas. En esta etapa, el sujeto activo toma contacto con la víctima a través de cualquier medio de comunicación y, con un componente de ingeniería social, logra engañar al usuario para que entregue de manera voluntaria la información solicitada (nombre de usuario, contraseña, número de cuenta bancaria, datos de tarjeta de crédito, etc.).

La modalidad más conocida para impulsar esta etapa es realizando un envío masivo de correos electrónicos conocidos como *"no deseados",* o *"SPAM"*, a un importante número de direcciones de correo electrónico que en una etapa previa fueran recolectadas, posteriormente el usuario ingresa a un sitio web equivalente al de la entidad de confianza y colocará allí aquella información necesaria con la cual se dará inicio a la segunda etapa de esta modalidad delictiva.

ETAPA 2:

Una vez cumplida la primera etapa, Telles Valdes explica que lo que seguirá será disponer de la información obtenida por parte del usuario víctima. Es en este momento cuando el delincuente cuenta con múltiples opciones de uso respecto a tales datos obtenidos. La finalidad más común de esta recolección de datos que realiza el sujeto activo, es la de ser utilizada con el propósito de obtener un beneficio económico, lo cual, para ser llevado a cabo, deberá afectar el patrimonio del sujeto pasivo. Pero veamos cuáles son algunas de las múltiples posibilidades que nos acerca Telles Valdes, respecto de lo que el delincuente podrá tener a su disposición, a saber:

VENTA DE DATOS: La misma se realizará a otros delincuentes en el mercado clandestino. En este caso la información se valora según el grado de integridad y exactitud, ya que no tendrá el mismo valor una simple base de datos con nombres de

usuario y contraseña, que aquella que además contenga datos de tarjetas de crédito y código PIN. Este tipo de actividad aún no se halla legislada en nuestro país.

EXTRACCIÓN DIRECTA DE PATRIMONIO DE CUENTAS ADQUIRIDAS: Este tipo de modalidad se encuentra tipificada en nuestro país en el Art. 173 inc. 16 del Código Penal y se la conoce como "Fraude informático". Con la incorporación de esta figura en el inciso 16, se podría inferir que la misma logra abarcar de manera amplia, aunque en abstracto, los supuestos en que se configura el phishing.

EJECUCIÓN DE TRANSFERENCIAS BANCARIAS DE FORMA DIRECTA: En este caso, el delincuente realizará la transferencia directa de una suma de dinero desde la cuenta de la víctima a sus propias cuentas, lo cual no es muy frecuente en razón de la facilidad en la posibilidad de rastreo.

MANEJO DE "MULAS": Son aquellas personas que, de forma honesta y obrando de buena fe y por desconocimiento, suministran su cuenta bancaria para realizar movimientos de dinero, obtenido de transacciones fraudulentas. A esta modalidad se la conoce como "lavado de dinero", la cual se realiza comúnmente a través de la atracción de víctimas con ofertas de trabajos fáciles y con altas remuneraciones.

ADQUISICIÓN DE BIENES DE CONSUMO O SERVICIOS A TRAVÉS DE CANALES VIRTUALES: En estos casos y para tal fin no se requiere de la presencia del titular de la tarjeta o de documentación del mismo. En este tipo de estafas es común la compra de crédito para líneas telefónicas móviles. Este tipo de delito se encuentra tipificado en el Art. 173 inc. 16 de nuestro Código Penal Argentino.

REALIZACIÓN DE "BROMA" A LA VÍCTIMA: Consiste en crear perfiles falsos en nombre de la víctima, como también comunicaciones. Una actividad muy común entre los grupos más jóvenes y llevada a cabo a través de las redes sociales. Si bien en los casos más graves tales "bromas" pueden incurrir en el delito de injurias graves -que sí contempla el Código Penal Argentino- en el resto las mismas no encuentran asidero legal, por no hallarse tipificadas.

SUSTITUCIÓN DE IDENTIDAD: En este caso, lo que se buscará generar es un daño patrimonial en la víctima, como las estafas, así también un daño de índole personal, como las injurias o la lesión al honor personal. Esta es otra actividad que en la actualidad no se halla tipificada en derecho argentino, a excepción de los casos de estafa, que actúa como delito independiente. Esta figura, a diferencia de la del Art. 173 inc. 16, puede afectar distintos bienes jurídicos, pues el fin que puede perseguir la sustitución de identidad podría tener múltiples propósitos que, hasta no hallarse cumplidos, no podrán conocerse su alcance y finalidad real, esto es, aquello que se quiere lograr con tal sustitución.

DIVULGACIÓN DE INFORMACIÓN ADQUIRIDA POR INTERNET: Se da cuando el sujeto activo se dedica a captar de manera ilegítima la información, para luego "colgarla" en la llamada red de redes, a sabiendas de que su posterior propagación generará reacciones en los medios y en la opinión generalizada sobre el organismo encargado de la seguridad de ese tipo de datos.

COMPILACIÓN PERSONAL: Pueden existir algunos casos, donde el delincuente que captó la información, resuelva no utilizarla en ninguna de las alternativas mencionadas, limitándose a recolectarlas de manera privada. Ello no configura delito alguno para el ordenamiento jurídico argentino (TELLEZ VALDEZ, 2009).

Con este análisis realizado, de las etapas requeridas en el "phishing", comenzamos a adentrarnos en el que será el tema central de este trabajo: las figuras derivadas del "phishing" que caen en una laguna normativa o vacío legal en nuestro Derecho Interno, pues pudimos apreciar que, de las citadas se destacan tres figuras no contempladas por la ley penal argentina, como es el caso de la venta de datos; la sustitución de identidad y la compilación personal; debiendo desde ahora, intentar concluir y justificar por qué tales figuras penales podrían y deberían incorporarse a nuestro ordenamiento.

1.2. El problema de la tipificación en nuestro país

Hasta este punto y luego de todo lo expuesto, nos encontramos ante un gran inconveniente, que es el de la actual tipificación argentina, ello en razón de que algunas de las conductas de las que se vale el "phishing" para lograr su objetivo, que son consideradas como delictuosas, no reúnen del todo estos requisitos, como se pudo observar, en el caso de la sustitución de identidad o la compilación personal, vistas en el punto anterior. Todo ello nos lleva a realizarnos la pregunta acerca de, si los actos preparatorios mencionados deberían o no estar tipificados en nuestro ordenamiento.

A modo de excepción, se puede afirmar que se configuraría el tipo especial de estafa del Art. 173 inc. 16 del C.P. para el caso en que el delincuente no sólo realice el ardid o engaño para obtener datos sensibles de la víctima, sino que además realice alguna transferencia bancaria o adquisición de bienes o servicios a nombre de la víctima, generando entonces el perjuicio patrimonial que requiere cualquier modalidad de estafa y perfeccionándose recién -en ese momento puntual- el tipo penal.

Merece un análisis considerable el importante número de personas que se dedican a la obtención de datos confidenciales de manera ilegítima, pero luego se puede optar por otras alternativas diferentes a la estafa tradicional a la víctima. La mayoría de los casos de phishing actualmente no son delito en la Argentina, debido a que, de acuerdo a la estrategia jurídica utilizada por el legislador, se exigen elementos típicos de la estafa y como consecuencia es menester que exista perjuicio patrimonial para que exista delito. Será tal vez por ello que surge la pregunta más importante a analizar: ¿Qué tan abarcativo y provechoso resulta el actual inciso 16 del Art 173, respecto a la estafa o fraude informático? Según la mayoría de los juristas especializados en la temática, resultaría realizador si se lograse tipificar a todas las conductas antes mencionadas, dentro de la propia ley penal actual y, así evitar la insatisfacción y vacío, no sólo desde el punto de vista jurídico normativo, sino que además para quienes como víctimas debieran soportar tales figuras hasta ahora no contempladas por la ley.

Vale analizar lo que sucede al momento en que el juzgador debe realizar la correcta calificación de los delitos derivados del "phishing", como sucede con aquellas maniobras ilícitas de similar tenor -englobadas en el concepto de "fraude informático". Aquí se está en presencia de lo que conoce como *laguna normativa*. Ello en razón de la duda que se presenta en cuanto a la calificación legal a escoger: ¿se estaría frente a hechos como constitutivos del delito de hurto, o bien como constitutivos del delito de estafa?

Tal como sostiene Sebastián Bisquert – Fiscal de Instrucción en la Provincia de Buenos Aires- en su análisis sobre esta temática, propone lo siguiente:

"*exponer en primer término una concreta maniobra de "phishing" y a partir de ello, desarrollar los distintos argumentos que llevarían a encuadrar jurídicamente el accionar del imputado en la figura de hurto o en la de estafa.- Supongamos la existencia de un imputado, que mediante "phishing" obtiene el número y la clave de una tarjeta y con dichos datos celebra una compra por internet. Una "máquina" registrará la compra y en base a dicho registro se efectuará el envío de la mercadería adquirida -si así lo requiere el agente* (BISQUERT, 2006).

Siguiendo siempre en este análisis, lo que propone Bisquert, que se considera sumamente útil y pertinente, es *observar los dos extremos opuestos*, en cuanto a la calificación y el modo de sostener aquella argumentación que llevará a defender dicha calificación. Así, los que se inclinan por encuadrar el hecho antes descripto en la figura de hurto, sostienen que no se configura una estafa, ya que se cae un elemento clave para la comisión de este delito: el engaño. Simplemente porque no se puede engañar a una máquina, la cual *no es una persona que, en base a un engaño y en virtud del mismo pueda efectuar una disposición patrimonial perjudicial*. Del mismo modo que no podría mediar una defraudación, sino que aquí se está simplemente ante un hurto, descartando por completo el robo, pues el autor se habrá apoderado ilegítimamente de una cosa ajena, sin mediar la violencia que requeriría el robo.

Bisquert, en un acertado y sostenido argumento, refiere que para la comisión del delito de estafa se requiere de "*la verificación concreta de la trilogía "ardid-error-disposición patrimonial voluntaria"* (BISQUERT, 2006). Con dicha trilogía sí se podría encuadrar en la figura que prevé el art. 172 del Código de Fondo. Incluso obteniendo el beneficio indebido propio de la estafa, si falta el error y el ardid que lleve a tal error, no habrá estafa.

Existirá un desmedro patrimonial, pero no existirá la disposición voluntaria originada en un error que se ha ocasionado al efecto. Ello es lo que sucedería con la modalidad del "phishing".

Ahora bien, analicemos el argumento de aquellos que se apoyan en que el caso traído a análisis encuadra en una defraudación. Sabido es, que en los casos en que se obtenga un desplazamiento patrimonial indebido apoyados por el uso de un medio informático, se estará en presencia de la infracción que prescribe el Art. 172 del Código Penal.

El Fiscal Bisquert al respecto, sugiere que "*quien pretenda fundar tal postura deberá recurrir a una moderna concepción del tipo de estafa"* (BISQUERT, 2006). Vale tener presente que, como se explicó anteriormente, ninguna "máquina" es capaz de realizar un acto de disposición patrimonial por sí sola, ya que son las máquinas quienes están para servir a las personas humanas, siendo tan sólo instrumentos programados al servicio del hombre. Y es este hombre el que dispone la entrega de un bien o la prestación de un determinado servicio, a cambio de la contraprestación correspondiente al consumidor.

Algunos doctrinarios, sostienen que los dispositivos mecánicos o electrónicos ejecutan, al activarse, una voluntad dispositiva de la que en ningún momento se independizan. Así las cosas, cuando un consumidor o usuario accede a una máquina para obtener un bien o un servicio, entabla una relación con una persona física o jurídica, que valiéndose del referido medio, entrega el bien o suministra el servicio.

Otro argumento que menciona Bisquert y que resulta útil para corroborar la relación de un usuario con una persona física y no con una máquina, se da en el siguiente ejemplo: en que la máquina no registra una compra realizada por el usuario pero, aun así, realiza el descuento correspondiente de la tarjeta de crédito de este usuario, sin enviar la mercadería que se compró. Nuevamente, no se le puede imputar el engaño a la máquina, sino el titular de esta máquina, que la programó u ordenó su programación, quien cometerá el delito de estafa.

Ante la falta de un antecedente relacionado a casos concretos de "phishing"; se cuenta con jurisprudencia relativa a los genéricamente llamados "fraudes informáticos", entre

los cuales podemos incluir al "phishing" como uno de ellos. El problema sigue siendo que en este tipo de hechos no se cuenta con la posibilidad de inducir a error a persona alguna que la lleve a efectuar una disposición patrimonial perjudicial.

Al respecto, en la causa nº 162 del Tribunal Oral en lo Criminal y Correccional nº 24, de fecha 19 de julio de 1995 se arribó a lo siguiente. En este caso se juzgó a una empleada bancaria que, valiéndose de la alteración del número de cuenta de su propia tarjeta de débito, el cual reemplazó por el de otra persona que era clienta del banco, realizó una extracción de quinientos pesos a su favor. Frente a este caso el Tribunal consideró que tal conducta no se podía configurar como estafa, a menos que se incurriera en analogía, algo absolutamente prohibido para el derecho penal argentino. A consideración del Tribunal, no existió provocación de error alguno en la víctima, capaz de conducir a una disposición patrimonial perjudicial. Mejor dicho, la encartada se valió de sus conocimientos y se aprovechó de su puesto estratégico en la entidad bancaria, logrando con ello, alterar el sistema informático para finalmente hacerse del dinero de la víctima, todo ello debidamente tipificado en la figura penal de hurto[2].

A modo de cierre en esta cuestión, el Dr. Bisquert concluye de manera acertada, en que *"... La cuestión y las dificultades planteadas ya han sido recogidas por el legislador. En el Anteproyecto de Ley de Delitos Informáticos -sometido a consulta pública por la Secretaría de Comunicaciones por resolución nº 476/2001 del 21.11.2001- se propone una solución, consistente en considerar al delito de fraude informático como un tipo autónomo y no como una figura especial de defraudación..."* (BISQUERT, 2006). Seguido a ello y, al exponer los motivos que dan fundamento a esta solución, el fiscal lo sintetiza de la siguiente manera:

"...Se ha pensado el delito de fraude informático como un tipo autónomo y no como una figura especial de las previstas en los arts. 172 y 173 del Código Penal. En este sentido, se entendió que, en el fraude informático, la conducta disvaliosa del autor está signada por la conjunción de dos elementos típicos ausentes en los tipos tradicionales de fraude previstos en Código: el ánimo de lucro y el perjuicio patrimonial fruto de una transferencia patrimonial no consentida sin que medie engaño ni voluntad

[2] Tribunal Oral en lo Criminal y Correccional nº 24 – Causa N° 162 – Buenos Aires - 19 de julio de 1995

humana viciada. El ánimo de lucro es el elemento subjetivo del tipo que distingue el fraude informático de las figuras de acceso ilegítimo informático y daño informático en los casos en que la comisión de las conductas descriptas en estos tipos trae aparejado un perjuicio patrimonial. El medio comisivo del delito de fraude informático consiste en la manipulación o despliegue de cualquier artificio semejante sobre un sistema o dato informático. Se ha optado por definir la conducta que caracteriza este delito como una "manipulación" o "artificio tecnológico semejante" en el entendimiento de que dichos términos comprenden tanto la acción de supresión, modificación, adulteración o ingreso de información falsa en un sistema o dato informático. El hecho se agrava cuando el fraude informático recae en alguna Administración Pública Nacional o Provincial, o entidad financiera...." (BISQUERT, S. – 2006).

Luego de este análisis, no queda duda alguna de que el legislador toma en consideración a las dificultades que se plantean al encuadrar los distintos fraudes informáticos, entendiendo que resulta necesario crear nuevos tipos penales, ello atento a la imposibilidad de brindar una solución jurídica acorde, tomando en cuenta a las clásicas figuras penales que precisan adaptarse. Entre las adaptaciones que se consideran precisas realizar encontramos la incorporación de la figura de obtención de datos personales como modalidad delictiva. Pero para volver esto una realidad, primeramente, debemos formularnos las circunstancias y los casos en que la misma quede encuadrada como delito.

1.3. La cuestión de la competencia territorial

Para lograr comprender con mayor claridad la problemática que trae aparejada la modalidad de "phishing" en nuestra actual legislación, será de gran importancia analizar lo que sucede desde el punto de vista procesal al respecto.

Uno de los grandes interrogantes que se presentan en delitos cometidos mediante la modalidad de phishing, tiene que ver con la determinación de la competencia territorial, esto es, conocer qué juez será el que entienda en la causa. Por tal motivo, la Corte Suprema de Justicia de la Nación resolvió dos contiendas negativas de competencia entre la Justicia nacional y la Justicia local en causas que investigaban delitos cometidos mediante el uso de Internet[3].

El primer caso traído a conocimiento, tuvo su origen a raíz de la investigación de un delito de defraudación, cometido mediante la modalidad de phishing, a través del cual, personas no identificadas, haciéndose de claves bancarias de una persona, realizaron una transferencia de dinero hacia una cuenta cuya titularidad recaía en el encartado.

El titular del Juzgado Nacional en lo Criminal de Instrucción N° 24 se declaró incompetente para entender en este caso, por lo que decidió remitir la causa al Juzgado de Garantías N° 2 de Lomas de Zamora, fundamentando su decisión en el hecho de que la cuenta bancaria desde la cual se realizó la transferencia pertenecía a una sucursal con domicilio en Monte Grande, Provincia de Buenos Aires En tanto que el juez de Lomas de Zamora también negó tener competencia, alegando que la operación de phishing había sido llevada a cabo desde Canadá, en tanto que la disposición patrimonial había ocurrido fuera de su jurisdicción.

[3] Corte Suprema de Justicia de la Nación, "Pavón, Cristian Sebastián s/estafa", Comp. CCC 66074/2014, 29 de noviembre de 2016, y "Piccadaci, José Guillermo s/estafa", Comp. CCC 60569/2015, 20 de diciembre de 2016.

El segundo caso aquí analizado, tuvo lugar por una denuncia, ante la venta fraudulenta de pasajes a través de una red social, delito realizado por medio del ingreso no autorizado a sistemas informáticos de agencias de turismo, ello logrado desde una dirección IP extranjera.

La titular del tribunal a cargo de esta investigación, el Juzgado Nacional en lo Criminal de Instrucción N° 25, se declaró incompetente y a favor de la justicia local de Río Gallegos. Tal decisión fue tomada considerando que la localidad de Río Gallegos era el lugar del hecho denunciado, ya que el dinero obtenido del hecho ilícito fue depositado en la caja de ahorros de una entidad bancaria con domicilio en dicha localidad; asimismo la magistrada consideró que el titular de la cuenta realizó dos extracciones también en esa ciudad. Seguidamente, la juez a cargo del Juzgado de Instrucción N° 1 de Río Gallegos también se consideró incompetente. En su caso, entendió que el juzgado nacional había actuado de modo prematuro, pues se desconocía el lugar físico concreto desde donde se realizaron los depósitos, como también en qué momento se produjo el perjuicio económico.

Estos dos casos fueron remitidos ante la Corte Suprema de Justicia. En ambos casos, el Procurador General entendió que correspondía tomar intervención a la justicia local, ello fundado en la cuestión del principio de economía procesal y en los distintos lugares en los cuales hubo actos con relevancia típica. Además, consideró que aún se desconocían muchos hechos y que los delitos probablemente habrían sido realizados a través de conexiones simuladas en el extranjero. Concluyó entonces que correspondía que los jueces locales continuaran con la investigación, apoyándose en los hechos ciertos que sí ocurrieron en su ámbito territorial.

Siguiendo el razonamiento y fundamentos del Procurador General, la Corte Suprema de Justicia resolvió que debían seguir entendiendo en las causas los juzgados locales; situación que plantea un nuevo interrogante para quienes defienden la Teoría Mixta o de Ubicuidad, la cual sostiene que, "*tanto el comportamiento como el resultado, integran el supuesto de hecho previsto por la norma secundaria y que, como consecuencia de ello, ambos tienen la misma relevancia jurídica y resultan suficientes para determinar la ley penal aplicable".* Con ello aparece una discrepancia notoria al momento de determinar la

competencia territorial y material, ello al analizar los pronunciamientos ut-supra mencionados, emanados de la Corte Suprema de Justicia de la Nación, discordantes con lo que plantea la Teoría Mixta. Entonces, si nos inclinamos por defender dicha teoría, deberemos ineludiblemente tomar como relevantes a los actos preparatorios que nos llevarán -a posteriori- a la consumación del delito mantenido en la inteligencia de su autor.

Por el contrario, si se opta por sostener y focalizar en los decisorios de la CSJN, resultará de interés y relevancia, no tanto los actos preparatorios, que harán al *iter criminis,* sino el lugar donde se lleve a cabo la consumación del hecho, es decir donde realmente se produzca el perjuicio económico a la víctima.

CAPÍTULO II:

LEY N° 26.388

2.1. Análisis de la Ley N° 26.388 de delitos informáticos:

La Ley 26.388, denominada "de delitos informáticos", sancionada en junio de 2008 y, desde entonces en vigencia en la Argentina, ha logrado incorporar las figuras típicas a diversos artículos del Código Penal de la Nación. Adiciona a las nuevas tecnologías como medios de comisión de distintos tipos, previstos en el Código Penal.

Los artículos incorporados son:

a) Tenencia con fines de distribución por Internet; u otros medios electrónicos de pornografía infantil.
b) La violación, apoderamiento y desvío de comunicación electrónica;
c) Intercepción o captación de comunicaciones electrónicas o telecomunicaciones;
d) Interrupción de las comunicaciones electrónicas;
e) El acceso ilegítimo a sistemas informáticos;
f) Publicación de una comunicación electrónica. –
g) Acceso a un banco de datos personales;
h) Revelación de información registrada en un banco de datos personales;
i) Daño informático y distribución de virus;
j) Inserción de datos falsos en un archivo de datos personales;
k) Fraude informático;
l) Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP). Las penas que establece son: a) prisión; b) inhabilitación (cuando el delito lo comete un funcionario público o el depositario de objetos destinados a servir de prueba); c) multa.[4]-

De esta manera, con la sanción de la presente ley, la República Argentina se agrega a la lista de países que cuentan con regulación legal en estos aspectos puntuales.

[4] Ley N° 26.388 – Modificatoria - CODIGO PENAL DE LA NACION ARGENTINA – 04 de junio de 2008

De los artículos contenidos en la ley de estudio, vale destacar dos de ellos, los cuales se enfocan de manera más específica en la estafa informática y los cuales se vinculan con la modalidad de comisión delictiva que define al "phishing":

ARTICULO 8 - Sustitúyase el artículo 157 bis del Código Penal, por el siguiente:

"Artículo 157 Bis. - Será reprimido con la pena de prisión de un mes a dos años el que:

1.- A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro, información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años."[5]

La comisión de esta figura penal sólo admite dolo y reprime a aquel que ingrese a un banco de datos personales sin autorización ni permiso alguno; o a quien revelare secretos o archivos registrados en ese banco de datos y al que las modifique por cualquier medio. La pena se ve agravada si el sujeto activo es un funcionario público.

Esta figura está íntimamente relacionada con la protección de datos personales establecidos en la Ley N° 25.326, que incorporó las figuras del acceso ilegítimo a un banco de datos y revelación ilegítima de información.

El bien jurídico aquí protegido es la privacidad. La conducta siempre de tipo dolosa acepta la tentativa.

El criterio guarda similitud con la violación del correo electrónico, pero hace referencia a los datos personales, protege la intimidad o el secreto de una base de datos privada y cerrada y cualquier violación a ella es considerada delito. También reprime a quien participa de la información allí registrada a terceros, pero en este caso se detiene la

[5] Art. 8 - Ley N° 26.388 – Modificatoria - CODIGO PENAL DE LA NACION ARGENTINA – 04 de junio de 2008

norma en que la prohibición de esa revelación se encuentre establecida por ley: *"...cuyo secreto estuviere obligado a preservar por disposición de la ley..."* Esto hará que surja la pregunta: ¿si no está establecida por ley, la revelación de la información guardada en una base de datos no será considerada delito? Considerando la redacción del artículo de análisis, si la revelación de la información guardada en base de datos no está prohibida por ley, entonces tal revelación no será delito.

Pablo Palazzi, explica que en el caso de este artículo sucede lo siguiente:

"*la norma no hace referencia a que los datos sean falsos sino a datos, por ende, poco importa que éstos datos sean falsos o verdaderos. La protección que el legislador otorga al banco de datos podrá extenderse tanto al responsable de los datos como a su titular (...) La norma se refiere a insertar datos, pero no aclara cuales pueden ser. El resultado típico requerirá que el archivo se modifique, ya sea agregándose nuevos asientos o borrando los existentes.*" (PALAZZI, 2009, pág. 24 y 25)

El sujeto activo será cualquier persona que ingrese indebidamente a una base de datos sin autorización, y el sujeto pasivo no será simplemente el dueño o titular de esa base de datos, sino también quien tenga la responsabilidad de proteger y resguardar la base de datos.

c) ESTAFA INFORMÁTICA - FRAUDE INFORMÁTICO

ARTICULO 9 - 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."[6]

[6] Art. 9 – inc. 16 - Ley 26.388 Modificatoria - CODIGO PENAL DE LA NACION ARGENTINA – 04 de junio de 2008

Nos encontramos con una nueva figura del delito de estafa establecido en el Código Penal Argentino. Previamente, el 21 de setiembre de 2004, la Ley N° 25.930 incorporó la defraudación mediante el uso de tarjetas de crédito o débito.

La incorporación del delito de defraudación informática en nuestro Código, llevó a los legisladores a diversos debates. Este tipo de debates se dividía en dos grandes sectores, en un sector se encontraban quienes consideraban que se debía encuadrar a la apropiación de bienes informáticos en la figura de defraudación, mediante la utilización de medios informáticos y en otro sector opuesto, se encontraban aquellos que consideraban que tal apropiación debería ser hurto a través de medios informáticos.

Finalmente; y pese al debate generado entre los propios legisladores, se ha incorporado la figura de fraude informático dentro del artículo 173 del Código Penal, algo concebido en gran medida gracias al aporte y precedente recibido de diferentes países europeos, como España, Italia, Alemania e Inglaterra y también de los Estados Unidos.

Intentando definir la defraudación informática nos estamos refiriendo a una nueva modalidad de estafa, la cual *se logra mediante la manipulación de cualquier sistema informático que afecte al patrimonio y/o a la propiedad*.

Lucero y Kohen en su obra “Delitos Informáticos” acotan "…*nos inclinamos por pensar que el bien jurídico protegido es el patrimonio, ya que la conducta lesiva se afecta holísticamente el patrimonio del damnificado y no un componente de la propiedad de dicho sujeto pasivo, como podría ser el caso de los delitos de hurto o robo...*" (LUCERO & KOHEN, 2010, pág. 43)

Coincide Palazzi en este sentido, proponiendo que "*como todo delito contra el patrimonio, esta nueva modalidad de estafa requiere que exista perjuicio patrimonial*…" (PALAZZI, 2009, pág. 29)

No resulta común ver que una estafa informática haya sido cometida por personas sin conocimiento alguno en informática, justamente porque se requiere de conocimientos específicos para poder manipular los sistemas o una transmisión de datos, utilizando

cualquier tipo de ardid que lleve a la víctima a cometer un error y que ese error lo lleve a un perjuicio económico que a su vez beneficie económicamente al autor del delito. Ardid, engaño y beneficio económico son los pilares fundamentales e imprescindibles en la configuración del delito de estafa y sus variantes.

Distintos autores mencionan múltiples formas de fraude informático, tales como la alteración de registros informáticos; el uso no autorizado de tarjetas de crédito; la utilización de claves falsas; la sustracción de datos personales para utilizarlos en la web para efectuar compras on line; el “phishing”; el "caballo de Troya"; las "técnicas del salami", entre otros

Vale mencionar entre los delitos enumerados ut supra, al Robo de Identidad, ya que este delito está creciendo exponencialmente y por medio de éste han sido estafadas una gran cantidad de personas, producto del robo o sustracción de su identidad, todo ello siendo posible a través de la utilización ilegal de sus datos personales. Estos datos por lo general son facilitados por los propios damnificados mediante engaños, falsas encuestas, llamados telefónicos que simulan ser del banco en que se posee cuenta para verificar datos, mismo sistema utilizado por correo electrónico; también mediante sorteos simulados en comercios o en la vía pública, o también a partir del hurto o robo de documentos y tarjetas de crédito, cupones de sorteos, y cualquier credencial que contenga datos propios. En la mayoría de los casos, el damnificado tomará conocimiento del robo de su identidad una vez que reciba intimaciones de cancelación de deudas crediticias, o emplazamientos pre judiciales, emitidos por entidades financieras. Y en casos más graves resultan pedidos de detención, los cuales suceden cuando la víctima realiza alguna operación bancaria en persona, o cuando desea salir del país por algún motivo.

El robo de identidad, visto del modo en que se analiza no es el típico delito informático. Inicialmente el robo de identidad iba de la mano del denominado “phishing”, a través del cual se engañaba a la víctima para que "verifique" sus datos personales, tales como bancarios o de sus propias cuentas de correo electrónico, generalmente mediante mensajes falsos enviados por correo electrónico, en los que se le solicitaba al usuario que actualice sus datos personales, para ello debiendo ingresar su nombre de usuario y

contraseña. Con esa información, el hacker se hace de información verídica, con la cual inicia su raid delictivo a través por ejemplo de realización de compras online.

A partir de la sanción de la Ley de Delitos Informáticos y hasta la fecha, se ha incrementado exponencialmente el uso de las redes sociales, así es el caso de Facebook, Instagram o Twitter, siendo poco frecuente que alguna persona no posea una de estas cuentas. Cualquiera puede generar su perfil personal y allí compartir con quien desee información propia y ajena, de toda índole. Esta modalidad de estafa o fraude informático analizada, resulta ser un delito de tipo doloso, de acción pública, que admite la tentativa.

Si bien este capítulo permite destacar el avance logrado con la sanción de la Ley N° 26.388 en materia de delitos informáticos, aún la misma no logra contener y contemplar la totalidad de posibles modos comisivos mediante la técnica del "phishing", así es el caso de la compilación de datos personales, la cual no se halla debidamente tipificada penalmente, ergo no se la castiga como a una conducta antijurídica. Es en este punto, donde el legislador deberá situarse y determinar si dicha compilación puede ser configurada finalmente como una conducta delictiva, pero para ello sucede algo que se antepone como una barrera de difícil traspaso: poder conocerse la finalidad de la compilación de datos que realiza el sujeto activo. Este último punto es, para algunos juristas, el motivo que se plantea como la mayor barrera a traspasar, pues como se ha analizado en conclusiones categóricas de doctrinarios entendidos en la materia penal, como Eugenio Zaffaroni, en aquellos casos -como lo es el de la compilación de datos personales- se piensa la idea de un delito de peligro abstracto, el cual es definido por Ossorio como "*aquel que no requiere para configurarse, que se produzca un peligro concreto respecto del bien jurídico protegido, siendo suficiente que se presenten los hechos que la ley presume abstractamente como creando un peligro respecto de ese bien jurídico"* (OSSORIO, 1999)[7].

Por lo expuesto precedentemente y, considerando que nuestro Derecho Penal tilda la acogida de esta teoría como inconstitucional, toda vez que con ella el legislador determina

[7] OSSORIO, Manuel – Diccionario de Ciencias Jurídicas, Políticas y Sociales (1999) – 2° Ed - Heliasta

que tal acción resulta típica, por considerar que dicho comportamiento posee la cualidad de ser tenido como peligroso, prescindiendo de la necesidad, al momento de la subsunción, de comprobar si tal conducta ocasionó o no en el caso concreto algún peligro efectivo para el valor que la norma tutelada. Dicho de otro modo, sería como castigar una conducta, aunque la misma no termine configurándose en delito propiamente consumado, no por los lineamientos seguidos en el delito en tentativa, sino por no poder preverse cuál será el resultado final de la conducta, o qué querrá conseguir el autor como resultado. Es decir, se lo juzga *"ex ante"*, resultando ello insostenible en toda acusación por devenir en abstracto. De allí que los doctrinarios consideran al delito de peligro abstracto como inconstitucional, por juzgar de antemano una determinada conducta no consumada.

Así las cosas, entendiendo la cuestión que se suscita entorno al delito de peligro abstracto, si se tipificare penalmente en nuestro ordenamiento a la compilación de datos personales, el legislador debería dejar definido de manera precisa y taxativa cuál deberá ser la conducta descripta y acabada, susceptible de castigo, permitiéndonos pensar que, tal vez, habiendo considerado este punto de inflexión, la compilación de datos personales no haya sido tipificada al momento de la creación de la Ley N° 26.388, como sí ocurrió en países como Colombia.

CAPITULO III
DERECHO COMPARADO Y
LA SITUACIÓN EN ARGENTINA

3.1. Análisis del Derecho comparado:

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada en materia de delitos informáticos, más aún en lo que respecta al "phishing". A continuación, se presenta un breve análisis de los principales países que cuentan con legislación en materia de "phishing".

Punto de atención especial, merece el análisis de lo que ocurre en Estados Unidos, con la denominada "Anti Phishing Act" del Estado de New York, la cual sanciona penalmente a cualquier persona que, valiéndose de medios electrónicos, solicite, requiera o colecte información personal para representar de manera engañosa a una empresa u organismo del gobierno, sin la debida autorización para ello. En igual sentido, se pronuncia el Código de Illinois, con la particularidad que la normativa vigente en New York, aparece identificada la persona física como sujeto pasivo del delito, al tiempo que se incluye la situación en que cualquier persona se vea inducida a proporcionar datos sensibles.[8]

Alemania, por su parte cuenta desde el año 1986 con la "Ley contra la Criminalidad Económica", que contempla el castigo de delitos como espionaje de datos con pena de tres años de prisión y multa; la estafa informática, cuya pena de prisión es de cinco años; la alteración de datos, con una pena de prisión de dos años o multa; y el sabotaje informático, que contempla una pena de prisión de tres años, todas estas figuras admiten a tentativa. Claramente estas figuras penales están vinculadas de manera directa con el "phishing" como vía o camino de soporte para cometer tales delitos, por ello la importancia de traerlos a conocimiento[9]. En mismo sentido se conduce Austria, la cual cuenta con regulación legal respecto de delitos cometidos bajo la modalidad de phishing

En el Reino Unido de Gran Bretaña, rige la "Computer Misuse Act" (Ley de Abusos Informáticos). Esta ley castiga incluso la tentativa de los delitos informáticos, de hecho,

[8] New York General Business – Art. 26 – N° 390-B. Inc. 3

[9] Gesetz gegen Wirtschaftskriminalität – Art. 200a, 263a; 303a

en uno de sus apartados, que específica la modificación de datos, previamente obtenidos sin autorización, pone en manifiesto al "phishing", ya que por medio de esta modalidad es posible lograr tal modificación no autorizada de datos[10].

.

Holanda, en cambio, cuenta con regulación legal desde el 1º de marzo de 1993, fecha en que entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el "hacking", el "phishing", el "preacking"[11]. Francia en cambio, desde enero de 1988, dictó la ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil euros por la intromisión fraudulenta que suprima o modifique datos[12].

En materia de estafas electrónicas, el *nuevo Código Penal de España,* en su artículo 248, sólo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito, lo cual se haya emparentado con la modalidad del "phishing". Mediante la Ley N° 27.309, promulgada el 15 de julio de 2000 y publicada el 17 de julio de 2000, en España se incorporaron los delitos informáticos al Código Penal, enfocándose con mayor énfasis en el sabotaje informático, el acceso ilegal a bases de datos privadas, la sustracción de identidad y la estafa cometida desde la suplantación de identidad (phishing)[13].

Vale mencionar de modo más específico lo que ocurre con la "Ley sobre Crímenes y Delitos de Alta Tecnología" de República Dominicana, en la cual se ha tratado la temática de los delitos informáticos de manera precisa. Dicha ley reglamenta aspectos de derecho procesal penal para combatir el cibercrimen. Es oportuno mencionar los artículos 14 y 15 de la presente ley, en los que se regula la obtención ilícita de fondos[14], como también su transferencia electrónica y la estafa informática[15].

---

[10] Computer Misuse Act (Act 2014) – Ch.18 – United Kingdom of Great Britain.

[11] Computer misdaden wet (1993) – Nederland.

[12] Loi 88/19 Sur la fraude informatique (1988) - République Française.

[13] Ley N° 27.309 de delitos informáticos (17/07/200) Art.248 – España.

[14] Ley N° 53-07. Art 14 Rep. Dominicana – Obtención Ilícita de Fondos.

[15] Ley N° 53-07. Art 15. Rep Dominicana – Estafa

En la segunda clasificación sobre phishing, aparecen países que más allá de la tipificación de fraude informático. Es en este caso que se analiza, donde podemos avizorar la tipificación que nos resulta de mayor interés poder llegar a incorporar en nuestro país. Así entonces, en el caso de Colombia, introducen la tipificación de la captación ilegítima de datos[16], cuya legislación vigente expresa que:

" 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 (Art. 269 F – Ley 1.273).

En Argentina, la normativa vigente incluye la ciber criminalidad en su Código Penal en forma desconcentrada, como en los casos de algunos países europeos, es decir, incluyendo los distintos tipos legales en los diversos títulos del libro segundo, conforme los variados bienes jurídicos a tutelar, pero se agota antes de lograr la incorporación de la obtención de datos personales.

La reforma del Código Penal para incorporar aquellas modalidades delictivas vinculadas con la informática se traduce en una suerte de "paliativo" o "remedio", con la entrada en vigencia de la, ya analizada, Ley N° 26.388, sancionada el 4 de junio de 2008.

Como enuncia Gustavo Arocena en su análisis, *"en principio, no puede predicarse ya la existencia de un único bien jurídico amparado por los nuevos delitos informáticos; antes bien, lo resguardado mediante cada una de estas figuras será el común objeto jurídico designado por el título del código que alberga una u otra descripción típica"* (AROCENA, 2011).

El Estado con la Ley 26.388, les ha brindado a aquellas situaciones jurídicas antes desprotegidas un respeto acorde a los nuevos tiempos y circunstancias, reconociendo también la influencia y alcance real de la tecnología en este nuevo ordenamiento legal.

[16] Ley N° 1273- Art.269F – Año 2009. Colombia.

Sin perjuicio de reconocer que aún existen falencias de tipo técnico, o algunas mejoras que pudo haberse aprovechado incorporándolas a la propia ley, lo cierto es que en adelante será tarea de mayores investigaciones, al igual que de avances doctrinarios y jurisprudenciales que se vayan suscitando, tanto en el derecho local, como en el derecho comparado.

Luego de las cuestiones minuciosamente desarrolladas, es preciso realizar un análisis adicional, que no se vincula al estudio de las normas de derecho penal material sancionadas por la Ley 26.388, sino a las referidas al derecho procesal penal "vinculado" con aquellas disposiciones. Y es que no resulta suficiente profundizar sólo en la tipificación —por más perfecta y acabada que sea— de las distintas hipótesis de ciberdelito, a la hora de perseguir y castigar esta modalidad de delito. Del mismo modo no alcanza con una imprescindible adecuación de las estructuras y las herramientas de su Parte General en Derecho Penal. Previo a ello, y como nos propone Arocena en su análisis sobre delitos informáticos, resulta imprescindible la creación de estructuras procedimentales destinadas a la elaboración y acreditación de la hipótesis fáctica a subsumir en las nuevas figuras delictivas que se instituyen.

Si con la determinación exacta de los ilícitos comprendidos en el ámbito de la criminalidad informática, el *derecho penal realizador* no cuenta o no obtiene los instrumentos de comprobación judicial idóneos para la acreditación de tales delitos, se podría acabar arribando a la violación del *Principio de Racionalidad Penal Legislativa*, según el cual, el legislador sólo debe sancionar leyes que prevean delitos *apriorísticamente susceptibles de acreditación fáctica* en un debido proceso penal. Por el contrario, y como se expuso en el capítulo que antecede, si al momento de la sanción de una ley penal, el legislador prescindiera de considerar la acreditación fáctica de una conducta, enfocándose en el resultado peligroso que posiblemente o no pudiera cumplirse, caería en las vicisitudes que plantea el *delito de peligro abstracto*, constitucionalmente reprobable.

CAPÍTULO IV:
LA TEORIA DEL DELITO
EN MATERIA DE CIBERCRIMINALIDAD

4.1. La Teoría del Delito y su encuadre en la cibercriminalidad:

Ante todo, vale destacar en este trabajo a la Teoría del Delito, toda vez que, por medio de dicha teoría y sus componentes, se podrá comprender mejor de qué manera la misma se ajusta y abarca también al delito informático.

De acuerdo a lo que propone Bacigalupo sobre a la Teoría del Delito, el autor señala que:

"Es una teoría de la aplicación de la ley penal y, como tal, procura instituir un orden para el planteamiento y la resolución de los problemas que envuelven la aplicación de la ley penal. La misma desempeña una doble función mediadora, por un lado, entre la norma y la solución del caso concreto; y por otro lado, una intervención entre la norma y los hechos que son objeto del juicio" (BACIGALUPO, 2014)

Con esta afirmación de Bacigalupo, lo que se sugiere es que resulta necesario lograr evidenciar que determinado sujeto se comporta del modo que se prevé en la ley, que su conducta no se halla autorizada de acuerdo al contexto en que la misma tiene lugar y, finalmente, que el autor de tal conducta reunía las características requeridas para reprocharle su accionar. Pero ¿cómo esta descripción que elabora Bacigalupo, tiene asidero en nuestro tema de investigación ("phishing")?

En base a la Teoría del Delito, se propone hacer hincapié en aquellos aspectos considerados como de mayor relevancia, respecto a la modalidad de "phishing" en el marco la cibercriminalidad, a saber:

4.1.1. PRINCIPIO DE LEGALIDAD:

Este principio exige la preexistencia de un régimen jurídico que ponga en evidencia la descripción de la conducta penal y de la pena que le cabe por dicha conducta, la cual se

hallaba prevista como criminal, logrando así responsabilizar al sujeto como autor del delito.

Siguiendo al Principio de Legalidad y conforme lo dispone el ordenamiento jurídico penal argentino, si bien el mismo ha logrado regular y tipificar determinadas conductas que encuadran en lo que se conoce como "delito informático", la modalidad de "phishing" se logra plasmar como herramienta conducente de delitos tales como hurto, estafa, injurias y defraudación, entre otros.

4.1.2. EL PRINCIPIO DE RESERVA PENAL:

Según Núñez, este Principio reconoce como condiciones de su existencia las subsiguientes: "*a) la determinación legal de los hechos punibles; b) la determinación legal de las penas correspondientes; c) La prohibición de la analogía; d) La irretroactividad de la ley penal"* (NUÑEZ, R – Ob. Cit. P. 83).

Este principio, considerado una garantía individual incluso a priori del propio derecho penal, no se refiere a otra cosa sino a la facultad de actuar del hombre dentro de lo permitido, sin que su conducta pueda acarrear sanción alguna. Por ello es una garantía del sujeto ante el mismo órgano de legislación penal y no es exclusiva de los organismos de persecución.

Así pues, Nuñez considera que el Principio de Reserva cumple una función de doble amparo, pues en un sentido, restringe la libertad de punir, mientras que, al mismo tiempo, restringe la libertad de prohibir. Es así que, en materia informática, este principio reviste gran importancia, pues el elemento nomotético, el cual es el software que, por su naturaleza jurídica, de carácter intangible, no logra encuadrar en la esfera de protección penal común, siendo precisa una protección especial cuando las acciones criminales se realizan mediante la ejecución de medios informáticos.

4.1.3. ACCION U OMISION EN EL PHISHING:

Respecto a lograr definir si los delitos informáticos son delitos de acción u omisión, en el caso del phishing, la gran mayoría considera que estos delitos, cometidos mediante sistemas informáticos, son delitos de acción (positiva), que se ejecutan mediante un hacer. La estafa o la defraudación informática (phishing), requiere para su consumación de una conducta, una acción positiva, cuya intención y finalidad sea generar un resultado negativo (desobedecer un mandato imperativo) sobre los bienes jurídicos transgredidos. Por ello nuestra legislación en consonancia con la Doctrina, consideran en su mayoría que los delitos informáticos requieren de una ejecución, de un hacer para su comisión, es decir que en el caso del phishing se lo considera una modalidad delictiva que requiere de acción por parte del sujeto activo.

De este modo, podemos avizorar el papel fundamental que juega la Teoría del Delito, respecto de los delitos informáticos, específicamente cometidos bajo la modalidad de "phishing"; entendiendo como síntesis que, en estos -como en todo delito- se requiere a priori, de un sujeto determinado, es decir un autor de una determinada conducta; que dicho autor viole con su conducta una prohibición prevista y castigada por la ley penal, que esa conducta se halle taxativamente tipificada en la norma y que además le sea reprochable a este sujeto activo o autor; que se valga de los medios idóneos para su consumación, mediante una serie de actos preparatorios; y que la finalidad del autor de la conducta trasgredida, no sea otra que la de lesionar un bien jurídico protegido, cuyo titular será la víctima o sujeto pasivo.

CONCLUSIONES

CONCLUSIONES

Respecto al tema analizado -por cierto de gran interés y preocupación- se puede inferir que, dado el carácter transnacional de los delitos cometidos bajo la modalidad de "phishing" mediante el uso las computadoras, es preciso y útil establecer tratados de extradición, como también acuerdos de mutua colaboración judicial, entre los países que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional y así, contrarrestar eficazmente la incidencia de la criminalidad informática.

De igual modo, siendo el tema de análisis de este trabajo, se debe buscar evitar cualquier laguna o ambigüedad que pudiese presentarse en torno al "phishing", como también definir la cuestión de competencia territorial, ya que, en muchos de estos casos y como se pudo abordar, el autor de este tipo de delitos se encuentra operando desde el extranjero y, en aquellos casos en que se ha podido localizar el lugar de operaciones del delincuente, se plantea el problema de la competencia en materia del territorio por una característica de este tipo de delitos informáticos como es la *transterritorialidad*, ello al observar la acción y la consecuencia dañosa del delito, pues estas cuestiones no siempre se dan en un mismo espacio determinado, ya que el espacio donde se desarrolla, no es físico, sino virtual. Ante ello, se podría presentar la dificultad de aplicar a un mismo caso concreto, legislaciones que pudieran resultar antagónicas o diferentes.

Otra situación compleja se da ante la pregunta de qué juez deberá entender en la causa, qué derecho resultará aplicable. Ello, además de lograr definir, según la teoría del delito cuándo y dónde se debe entender que el delito tiene su forma. Ya que muchos juristas sostienen que los actos preparatorios no resultan definitorios a la hora de determinar el derecho aplicable, sino el resultado mismo conseguido. Pero qué sucede con un delito que se materializa en el campo informático, conocido como el ciber espacio ¿Cuál sería entonces el lugar real donde se comete el delito mismo? Si bien nuestra jurisprudencia ya cuenta con fallos -como los citados en el Capítulo I del presente trabajo- los cuales lograron poner claridad respecto al conflicto en cuanto a definir el ámbito temporo-

espacial en que se desenvuelve la comisión delictiva mediante el "phishing", ello no se traduce en haber logrado dar una cobertura total a la cuestión de la competencia territorial, hasta tanto no se resuelva el definir qué sucede con los actos preparatorios de esta modalidad, que a mi entender resultan tan importantes como el lugar donde el delito se haya consumado. Por ello, el legislador deberá tener en cuenta este aspecto a la hora de incorporar dicho punto en la futura modificación de la Ley de Delitos Informáticos.

Como cuestión central de este trabajo, se presenta el interrogante de si debería incorporarse en la Argentina la figura de la obtención o captación de datos personales con fines ilícitos, entendida como conducta típica antijurídica. Al respecto y a modo de cierre, considero que dicha conducta puede y debe ser incorporada por el legislador a nuestra norma penal de fondo, toda vez que, con la misma se lograría castigar de modo total la figura del "phishing" y con ello, lograr determinar cuándo y dónde comienza a cometerse esta modalidad, que a posteriori desencadenará en delitos tales como el fraude, estafas, hurtos, entre otros.

Con la posible incorporación de este tipo penal, se deberá determinar de manera indubitable el cómo y el cuándo se encuadrará en una figura delictiva, por ello la labor del legislador deberá ser minuciosa y no dejar lugar a duda alguna de la conducta requerida a ser castigada, tal como lo hicieran Colombia o República Dominicana, al momento de incorporar la obtención de datos como un delito tipificado en sus respectivas legislaciones, máxime siendo preciso entender que el "phishing" no puede ser considerado como delito autónomo o independendiente, ya que el mismo, por sí sólo no puede castigarse hasta que no se haya completado en otra conducta tipificante que de él derive.

La Ley N° 26.388 de Delitos Informáticos, vigente en la República Argentina requiere -a mi entender- de una pronta modificación y actualización, siempre ajustándose a los tiempos que corren, evitando con ello, dejar cabos sueltos que abran las puertas hacia los tan mencionados "vacíos legales" y a las "lagunas normativas", pero además debiendo el legislador, poner cuidado en que con la potencial modificación, no se caiga en la incorporación de figuras penales que deriven en planteos de inconstitucionalidad, por ser tenidas como delitos de peligro abstracto, por ello siempre se debe destacar que la

finalidad de conductas como la obtención de datos personales deberá ser con fines ilícitos; fines que ineludiblemente deberán ser alcanzados para su completo encuadre penal.

Es cierto que existe una tendencia preponderante en la legislación en general a introducir nuevos tipos penales, o el agravamiento de los ya existentes, muchas veces en miras a una reinterpretación de las garantías clásicas del derecho penal sustantivo y del derecho penal procesal, que -recordando la opinión de Arocena- "*Con ello se logra la creación de los llamados "bienes jurídico-penales", con la consiguiente ampliación de riesgos jurídico-penalmente relevantes, se flexibilizan las reglas de imputación y se relativizan los principios político-criminales de garantía, en una tendencia general a la que podría designarse con la expresión "expansión del derecho penal"*[17].

Más allá de todo lo analizado, resulta necesario continuar siendo optimistas en que finalmente se llegue a la realización y materialización de una ley penal más ajustada, profusa y actualizada a los tiempos que corren y que ello suceda en el menor plazo posible, castigándose todas las modalidades hasta hoy existentes, en materia de delitos informáticos y desarrollando programas de prevención para la población en general, de manera masiva, ya sea conferencias, campañas publicitarias, e incluso a través de los medios de comunicación, alertando así a la ciudadanía toda a poder estar debidamente informados y al resguardo, lejos de convertirse en víctimas del que -desde mi punto de vista- es el delito en pleno auge y expansión en nuestro tiempo actual.

Por todo lo expuesto, ante la pregunta central de este trabajo, quisiera cerrar sosteniendo y considerando que la ley penal debe ser modificada y que la compilación de datos personales debe ser finalmente castigada.-

[17] AROCENA, Gustavo – Regulación de Delitos Informáticos - 2012. UNAM, Instituto de Investigaciones Jurídicas, Boletín Mexicano de Derecho Comparado.

BIBLIOGRAFÍA

BIBLIOGRAFIA

I) DOCTRINA:

1 - ANZIT GUERRERO, Ramiro, TATO, Nicolás, PROFUMO, Santiago (2010). El Derecho Informático - Aspectos fundamentales. Buenos Aires: Cathedra Jurídica.

2 - BACIGALUPO, Enrique (2014). Lineamientos de la Teoría del Delito. Buenos Aires: Hammurabi.

3 - Código Penal de la Nación Argentina – Ley 11.1179 (2018). Buenos Aires: Abeledo Perrot

4 - LUCERO, Pablo Guillermo y KOHEN, Alejandro Andrés (2010). Delitos informáticos. Buenos Aires: Ediciones D&D.

5 - PALAZZI, Pablo A. (2016). Los delitos informáticos en el Código Penal: Análisis de la ley 26.388 - 3a ed., act. y amp - Buenos Aires: Abeledo Perrot.

6 - TELLES VALDEZ, Julio (2008). Derecho Informático – 4° Edición – México: MC GRAW HILL

II) LEGISLACION:

a) <u>Internacional</u>:

1 - Computer Fraud and Abuse Act - Tit 18 – U.S. Code 1030 (a) (5) – U.S.A.

2 - Computer misdaden wet (1993) – Nederland.

3 - Convenio Sobre Ciber Delincuencia – Budapest – Hungría.

4 - Ley N° 53-07. De Delitos Informáticos y Obtención ilegítima de fondos - Rep. Dominicana.

5 - Ley N° 1.273 de Fraude Informático – Rep. de Colombia.

6- Ley N° 27.309 de Delitos Informáticos – Código Penal de España.

7 - Loi 88/19 Sur la fraude informatique (1988) - République Française.

8 - Gesetz gegen Wirtschaftskriminalität – Art. 200a, 263a; 303a

9 - New York General Business – Art. 26 – N° 390-B. Inc. 3. EE.UU.

10 - OCDE (Organización para Cooperación y Desarrollo Económico) Convención Anual – "Nouvelles Technologies: Unestratégie pour les années 1990" - Paris – Francia 1983.

b) <u>Nacional</u>:

1 - Código Penal de la Nación Argentina – Ley 11.1179

2 - Ley 26.388 – Modificatoria - CODIGO PENAL DE LA NACION ARGENTINA – 04 de junio de 2008

III) JURISPRUDENCIA:

1 - C.N. Crim. y Corr., Sala VI "LANATA, JORGE" 4 de marzo de 1999 - JA 1999-III-237. 2ª INSTANCIA

2 - "Pavón, Cristian Sebastián s/estafa", Comp. CCC 66074/2014, 29 de noviembre de 2016

3 -"Piccadaci, José Guillermo s/estafa", Comp. CCC 60569/2015, 20 de diciembre de 2016.

IV) OTRAS FUENTES:

a) Revistas:

1 - AROCENA, Gustavo (2011). Regulación de Delitos Informáticos. UNAM, Instituto de Investigaciones Jurídicas, Boletín Mexicano de Derecho Comparado, núm. 135

2 - SORBO, Hugo Daniel (2007). Marco legal de los delitos informáticos - Revista del Colegio Público de Abogados de la Capital Federal, núm. 126.

3 - SUTHERLAND, Edwin (2011) "Una exposición de la teoría en delito y sociedad". Revista de Ciencias Sociales, Nº 31, Santa Fe.

b) Páginas web consultadas:

1 - Legislación y Delitos Informáticos – Austria (2009) Segu.Info – Seguridad de la Información. Disponible en: https://www.segu-info.com.ar/delitos/austria.htm

2 - Legislación y Delitos Informáticos – Holanda (2009) Segu.Info – Seguridad de la Información. Disponible en: https://www.segu-info.com.ar/delitos/holanda.htm

3 - Legislación Informática de Francia (2014). Código Penal Internacional contra Delitos Informáticos. Disponible en: http://catherinpacheco01.blogspot.com.ar/2014/11/legislacion-informatica-de-francia.html

4 - Computer Misue Act 1990 (2018). Disponible en: https://en.wikipedia.org/wiki/Computer_Misuse_Act_1990

ANEXO E – FORMULARIO DESCRIPTIVO DEL TRABAJO FINAL DE GRADUACIÓN

AUTORIZACIÓN PARA PUBLICAR Y DIFUNDIR TESIS DE POSGRADO O GRADO A LA UNIVERIDAD SIGLO 21

Por la presente, autorizo a la Universidad Siglo21 a difundir en su página web o bien a través de su campus virtual mi trabajo de Tesis según los datos que detallo a continuación, a los fines que la misma pueda ser leída por los visitantes de dicha página web y/o el cuerpo docente y/o alumnos de la Institución:

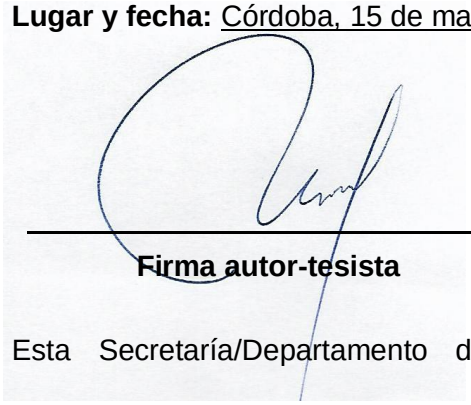
Autor-tesista *(apellido/s y nombre/s completos)*	SALVI GRILLETTI, Norberto Cristian Matías
DNI *(del autor-tesista)*	28.689.516
Título y subtítulo *(completos de la Tesis)*	El Phishing en la Argentina
Correo electrónico *(del autor-tesista)*	matiassalvi@hotmail.com
Unidad Académica *(donde se presentó la obra)*	Universidad Siglo 21

Otorgo expreso consentimiento para que la copia electrónica de mi Tesis sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21 según el siguiente detalle:

Texto completo de la Tesis *(Marcar SI/NO)*[1]	SI
Publicación parcial *(Informar que capítulos se publicarán)*	I,II, III y IV

Otorgo expreso consentimiento para que la versión electrónica de este libro sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21.

Lugar y fecha: Córdoba, 15 de marzo de 2019



Matías Salvi Grilletti

Firma autor-tesista **Aclaración autor-tesista**

Esta Secretaría/Departamento de Grado/Posgrado de la Unidad Académica: _____certifica que la tesis adjunta es la aprobada y registrada en esta dependencia.

Firma Autoridad Aclaración Autoridad

Sello de la Secretaría/Departamento de Posgrado

[1] Advertencia: Se informa al autor/tesista que es conveniente publicar en la Biblioteca Digital las obras intelectuales editadas e inscriptas en el INPI para asegurar la plena protección de sus derechos intelectuales (Ley 11.723) y propiedad industrial (Ley 22.362 y Dec. 6673/63. Se recomienda la NO publicación de aquellas tesis que desarrollan un invento patentable, modelo de utilidad y diseño industrial que no ha sido registrado en el INPI, a los fines de preservar la novedad de la creación.