TRABAJO FINAL DE GRADUACION

SUPLANTACION DE IDENTIDAD

Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino

Carrera: Abogacía.

Autor: Montaperto, Javier Eduardo.

Año: 2.018.

DEDICATORIA

Al Dios Todopoderoso, fuente de toda razón y justicia, por haberme concedido la oportunidad, la salud, el tiempo y la sabiduría para comenzar y hoy poder terminar con mi carrera de Abogacía.

A mis padres Carlos y Mary, por haberme brindado su cariño, confianza, contención y apoyo incondicional en pos de alcanzar el objetivo final que hoy puedo concretar.

A mi amada Carolina, por ser el motor y el pilar emocional, que con su amor, comprensión y paciencia, me permitieron seguir y perseverar hasta lograr esta ansiada meta.

Al Santo Cura José Gabriel del Rosario Brochero, por los favores recibidos durante todas las etapas de la carrera y en ésta presentación.

A todos ellos dedico con gran amor y agradecimiento el presente trabajo final de graduación.

ÍNDICE

Resumen: El presente trabajo final de graduación tiene como objeto de estudio la investigación sobre la falta de marco jurídico regulatorio de la denominada suplantación de identidad de la persona en el derecho penal argentino y cómo dicha circunstancia puede afectar el principio penal de legalidad de la represión como garantía del debido proceso tanto en el art. 18 de la Constitución Nacional como en los tratados con jerarquía constitucional del art. 75 inc. 22 de nuestra carta magna.

A esos fines en primer término es necesario conceptualizar y caracterizar que se entiende por suplantación de identidad de la persona, cuáles son las modalidades más habituales de ejecución, cuáles son los medios empleados, las fases diagramadas, las finalidades perseguidas, los sujetos intervinientes de este comportamiento etc., desde el campo de la informática, para poder avanzar así y entrar en un análisis desde el ámbito técnico – jurídico, más precisamente sobre la temática abordada.

Por otra parte, consagrada en nuestra legislación la prohibición de aplicación de analogía en perjuicio del imputado en el derecho criminal y atento la mencionada falta de régimen jurídico del *phishing,* se determina en ese contexto que la falta de encuadre legal y la aplicación de analogía mediante tipos delictivos y penas diferentes a la conducta en cuestión, ergo configura la vulneración del mencionado principio de legalidad.

Ante la falta de regulación jurídica, también es de suma importancia analizar la suplantación de identidad, por un lado desde la órbita de la teoría del delito para su configuración como una conducta delictiva y por el otro, para que la misma sea receptada normativamente en la ley penal y sea de aplicación al caso concreto.

Asimismo con el objeto de observar el grado de avance y recepción en cuanto a la legislación jurídica del tema bajo análisis, se efectúa el contraste del derecho de nuestro país con relación al derecho comparado de Brasil. Paraguay, Colombia, Perú y de España.

PALABRAS CLAVES: suplantación de identidad de la persona – principio penal de legalidad – prohibición de analogía en el derecho penal.

Abstract: The present final work of graduation has like object of study the investigation on the lack of regulatory legal frame of the denominated person's impersonation in the Argentine penal law and how this circumstance can affect the penal principle of legality of the repression as a guarantee of due process in both art. 18 of the National Constitution as in the treaties with constitutional hierarchy of art. 75 inc. 22 of our magna carta.

For these purposes in the first place it is necessary to conceptualize and characterize what is meant by identity impersonation of the person, what are the most common modalities of execution, what are the means used, the diagrammed phases, the purposes pursued, the subjects involved in this behavior etc., from the field of computer science, to be able to advance like this and to enter into an analysis from the technical-legal scope, more precisely on the subject addressed.

On the other hand, enshrined in our legislation the prohibition of the application of analogy to the detriment of the accused in criminal law and mind the aforementioned lack of legal status of phishing, it is determined in this context that the lack of legal framing and the application of analogy through criminal types and penalties different to the conduct in question, ergo configures the violation of the aforementioned principle of legality.

In the absence of legal regulation, it is also very important to analyze the identity theft, on the one hand from the orbit of the theory of crime to its configuration as a criminal behavior and on the other, so that it is normatively accepted in the criminal law and be applicable to the specific case.

Likewise, in order to observe the degree of progress and reception regarding the legal legislation of the subject under analysis, the contrast of the law of our country with respect to the comparative law of Brazil is made. Paraguay, Colombia, Peru and Spain.

KEY WORDS: impersonation of the person - criminal law principle - prohibition of analogy in criminal law.

INTRODUCCION.

En el derecho positivo argentino, se observa que la conducta de suplantación de identidad de la persona también denominada *phishing*[1], no ha sido encuadrada normativamente por el legislador en una figura típica específica ni en una pena, incluso luego de haberse sancionado la ley de delitos informáticos Nº 26.388/2.008 que modifica algunos artículos del Código Penal.

Es condición *sine qua non*[2] en la tramitación de un debido proceso penal, que se respete el principio penal de legalidad, receptado como garantía constitucional en el art. 18 de C.N.[3] que prescribe que "*ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso*"; este principio se traduce en la regla *nullum crimen nulla poena sine lege*[4], que implica que no hay delito ni pena sin una ley previa que así lo determine; como consecuencia, toda persona que es acusada de un presunto hecho delictivo y como supuesto autor en un proceso criminal, obliga al juez competente de la causa a la aplicación – entre otras cuestiones – de dicho principio de legalidad para determinar si debe ser condenado, de corresponder, mediante una sentencia firme y fundada.

En ese orden de ideas consideramos que el problema jurídico detectado versa en que si la suplantación de identidad no se encuentra regulada penalmente en el derecho de nuestro país – ante la falta de tipo penal y de sanción punitiva –, no constituye *ab initio*[5] un delito del derecho criminal, supuesto en que el juez no podría o al menos no debería aplicar tipos o penas diferentes al tema objeto de análisis, puesto que en materia penal está prohibida la aplicación de analogía, máxime si es en perjuicio del imputado.

La pregunta de investigación es determinar si la suplantación de identidad del individuo que no se encuentra regulada en el derecho penal en un tipo delictivo ni en una pena, y se aplican otras figuras delictivas y penas por los magistrados, ¿configura esta actividad una vulneración, menoscabo o afectación del principio penal -

[1] *Phishing* es un término informático en inglés utilizado para conceptualizar a la suplantación de identidad de la persona.
[2] Condición *sine qua non* es una locución en latín que significa condición indispensable, sin la cual no se puede considerar una situación o circunstancia.
[3] Constitución de la Nación Argentina.
[4] *Nullum crimen nulla poena sine lege* es una locución en latín que significa que no hay delito ni pena sin ley previa que lo determine.
[5] *Ab initio* es una locución en latín que refiere al comienzo, origen de una circunstancia.

constitucional de legalidad como garantía del debido proceso y la violación de prohibición de analogía en derecho penal cuando es en perjuicio del imputado?.

El objetivo general del trabajo final de graduación consiste en realizar un análisis sobre la falta de regulación en el ordenamiento jurídico argentino de la suplantación de la identidad de la persona aún luego de la reforma del Código Penal mediante ley Nº 26.388 de delitos informáticos.

En cuanto a la hipótesis de trabajo se parte de la premisa que, si se considera a la suplantación de identidad del individuo como una conducta no regulada normativamente en un tipo delictivo ni en una pena por el derecho penal argentino en la mencionada ley de delitos informáticos, la utilización de otros tipos penales y sanciones distintas para la figura en cuestión constituye por un lado la vulneración del referenciado principio penal de legalidad receptado como garantía del debido proceso tanto en el art. 18 de la Constitución Nacional como en tratados con jerarquía constitucional del art. 75 inc. 22 de la ley suprema, y por el otro, configura la afectación en cuanto a la prohibición de aplicación de analogía en derecho penal, cuya actividad está vedada para los magistrados, más aun si es en perjuicio del imputado, pretendiendo así confirmar dicha hipótesis en el presente trabajo.

El primer capítulo está destinado a la conceptualización de la suplantación de identidad de la persona, analizando cuáles con sus notas tipificantes, las modalidades y los medios de comisión utilizados por los *phisher*[6]*;* cuáles son las fases y las finalidades que se persiguen en el *phishing* y quiénes son los sujetos activos y pasivos de la suplantación de identidad de la persona, intentando clarificar al lector acerca de la temática desde un enfoque informático para su conocimiento y aprendizaje.

En el segundo capítulo se analiza la falta de regulación jurídica de la suplantación de identidad de la persona en la ley de delitos informáticos Nº 26.388 del año 2.008 al no existir encuadre típico de la mencionada conducta en esta ley, siendo oportuno esbozar brevemente sobre los presupuestos o estadios de la teoría del delito que se requieren para que el *phishing* pueda configurar un delito del derecho criminal; además se realiza una breve exposición de algunos pocos intentos legislativos sobre la materia que fueron presentados por legisladores en el Senado de la Nación pero sin ningún éxito hasta la fecha; también se hacen aportes de doctrinarios que analizan la

[6] *Phisher* es el término informático en inglés para designar al sujeto activo de la suplantación de identidad.

temática abordada en un intento por darle una configuración legal, considerando a la suplantación de identidad como hurto en algunos casos y como estafa en otros. Finalmente, se citan algunos fallos de distintos tribunales del país que han encuadrado al *phishing* dentro del tipo penal hurto o dentro del tipo penal de la estafa genérica o las defraudaciones.

En el tercer capítulo se efectúa un tratamiento sobre el principio penal – constitucional de legalidad conforme lo establecido en las garantías del debido proceso penal del art. 18 C.N. como así también en los tratados con jerarquía constitucional del art. 75 inc. 22 de la carta magna con relación a la figura de suplantación de identidad; a su vez se analiza que la aplicación de analogía en perjuicio del imputado – atento la falta de tipo delictivo del *phishing*–, vulnera el mencionado principio de legalidad de la represión; por último y desde una visión de la teoría general del derecho, se pretende explicar y realizar una clasificación de los ilícitos en típicos y atípicos, cuando se presentan casos en que determinadas conductas sin constituir en sentido estricto un delito del derecho criminal, sólo configuran actividades ilícitas del derecho común.

En el cuarto y último capítulo se realiza un análisis comparativo de nuestro ordenamiento jurídico interno con relación al derecho comparado de otros países, más precisamente tomando como modelos la regulación normativa en el Derecho Penal brasilero, en el Derecho Penal paraguayo, en el Derecho Penal colombiano, en el Derecho Penal peruano y en el Derecho Penal español, referido al avance y la técnica legislativa sobre la suplantación de identidad de la persona.

CAPITULO I: CONCEPTUALIZACION DE LA SUPLANTACION DE IDENTIDAD DE LA PERSONA.

1.1. Introducción.

El presente capítulo está destinado a explicar cómo es conceptualizada y configurada la suplantación de identidad de la persona desde una perspectiva informática; además se esboza sobre aquellas características particulares que son las que determinan a la conducta en cuestión; también se analizan las distintas

modalidades y medios de comisión de *phishing*[7] que se efectivizan a través de las tecnologías informáticas, siendo necesaria la utilización y definición de lenguaje técnico a esos fines; asimismo se estudian aquellas fases y finalidades detectadas con relación a la suplantación de identidad y que son desplegadas por los *phishers*[8] desde su preparación, su concreción e incluso posteriormente a la realización de esta actividad; por último y haciendo una clasificación de aquellos individuos que realizan los ataques y aquellos que son víctimas de los mismos, se establece en líneas generales cuáles son los sujetos activos y pasivos intervinientes en la conducta de suplantación de la persona.

1.2. Concepto y caracterización sobre la suplantación de identidad de la persona.

La conducta denominada *phishing*, consiste en un ataque informático, de ingeniería social que tiene por finalidad la adquisición de información confidencial de la víctima mediante el uso de ardid o engaño, la que en muchos casos es utilizada también para producir perjuicios patrimoniales y extrapatrimoniales. Por lo general estos ataques son dirigidos en contra de personas físicas, pero también pueden ser víctimas distintas organizaciones, todo ello atento la falta de conocimiento técnico o especializado respecto a los sistemas informáticos, aplicación deficiente de medidas de seguridad en relación a correo electrónico, páginas web o navegadores de *internet*[9]. (Belisario Méndez, 2.014).

Explica la Ing. Aymara Noriley Belisario Méndez (2.014) que el destino de dicha información obtenida es variada, como por ejemplo utilizar credenciales para entrar a sistemas o bases de datos de la persona, realizar transacciones en su nombre, publicarlos para perjudicar su imagen o confidencialidad y vender la información a sujetos que les sea de interés.

Consideramos oportuno mencionar que la suplantación de identidad de la persona es una actividad desplegada por los *phisher,* cuya finalidad consiste en atacar tanto la faz patrimonial de la víctima, más precisamente su derecho de propiedad

[7] El *phishing* es el término informático en inglés utilizado para conceptualizar a la suplantación de identidad de la persona.
[8] *Phisher* es el término informático en inglés para designar al sujeto activo de la suplantación de identidad.
[9] *Internet* es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo que garantiza que las redes físicas heterogéneas que la componen, formen una red lógica única con alcance mundial.

como así también la faz extrapatrimonial. Se trata de sujetos que tienen un alto grado de conocimiento y preparación en sistemas informáticos, manejo de dispositivos electrónicos, en suma expertos en el ámbito de las tecnologías.

En cuanto a la afectación del derecho de propiedad, referimos que un ejemplo concreto está dado habitualmente en el envío de una aparente página *web* de una institución bancaria oficial – que en efecto no lo es – para la "confirmación" o "modificación" de los datos del cliente de la entidad, pero que en realidad y en la mayoría de los casos tiene como único y verdadero fin la obtención del usuario y contraseña del *home banking*[10] de la persona, para efectuar alguna transferencia de los activos de esa cuenta a la cuenta del victimario. En menor medida también los *phisher* piden a sus víctimas el pago de una suma de dinero para la recuperación de la cuenta bancaria.

Con relación a la vulneración del ámbito extrapatrimonial, manifestamos que la suplantación de identidad puede producirse en aquellos supuestos en que el victimario afecta el derecho a la intimidad, el buen nombre, el honor y la imagen de la persona, cuestión que puede observarse frecuentemente en el ámbito de las redes sociales como por ejemplo *facebook*, *twitter*, *instragram* etc., cuya finalidad en este supuesto es *hackear* la cuenta y tomar el control de la misma para lograr la desacreditación, deshonra y exposición de la persona en cuestión, con las consecuencias dañosas que ello implica. El gran problema que existe en la actualidad es que se torna una tarea muy dificultosa poder determinar con certeza quién es el sujeto dañador y desde qué ordenador se produjo el ataque del *phisher* dado que – en el caso de las computadoras – todas tienen un número de identificación (IP) que es variable si la misma está conectada a una red informática. Dependiendo del momento en que el dispositivo se conecta, ese número de IP cambia constantemente y se vuelve prácticamente imposible determinar el momento exacto y desde qué dispositivo se efectuó el ataque, como asimismo quién es el atacante que se encuentra detrás del ordenador. Por estas razones nos parece que lo más conveniente es hacer hincapié en la prevención de los usuarios que utilizan navegadores, sitios *web*, *internet* etc., para

[10] *Home banking* es un término en ingles que refiere a la posibilidad que tiene el cliente de un banco de hacer operaciones y obtener información bancaria desde su propia casa, sin necesidad de dirigirse a la entidad bancaria.

evitar las consecuencias dañosas que un *hacker* informático puede ocasionar desde el momento en que toma el control de la víctima y de su información.

Por otra parte, enseña el INTECO[11] que el *phishing* posee cuatro elementos fundamentales que caracteriza a esta conducta, a saber:

- ✓ Ingeniería social: el *phishing* explota las debilidades de los individuos para engañarles y hacer que actúen contra sus propios intereses. Aclaramos que al respecto existe un cierto de grado de ignorancia y/o desconocimiento en la víctima del ataque al momento de estar navegando en un sistema informático, cuestión que es hábilmente aprovechada por el atacante.
- ✓ Automatización: las tecnologías de la información son utilizadas para desarrollar los ataques de *phishing* de forma masiva. En cuanto a ello, explicamos que una de las formas más habituales de suplantación de identidad es el ataque dirigido a personas indeterminadas, circunstancia que los victimarios conocen muy bien, esperando que tarde o temprano personas desaprensivas, sin preparación ni formación, caigan en su trampa para comenzar con su "trabajo".
- ✓ Comunicación electrónica: usan redes de comunicación, especialmente *internet*. Consideramos que el medio más idóneo y efectivo para concretar los ataques de suplantación de identidad, se realizan mediante el uso de *internet*, páginas y sitios *web* por medio de distintos dispositivos como pueden ser computadoras de escritorios, *notebooks*, *tablets*, celulares etc..
- ✓ Suplantación: un ataque de *phishing* requiere que los *phisher* suplanten a una empresa u organización legítima. Sobre este punto afirmamos que los ataques de *phishing* no solamente se efectúan a empresas u organizaciones, sino que también son sujetos pasivos de esta actividad, distintas personas físicas que a diario se ven afectadas con graves consecuencias dañosas. Más allá de las diferencias que pueden llegar a existir en uno y otro caso, el punto en común está dado en que los ataques se perpetran tanto en personas jurídicas como en personas físicas.

En un intento por expresar una definición sobre esta conducta, se manifiesta que el *phishing* es una forma de ataque basada en técnicas de ingeniería social, utilización de código malicioso o la combinación de ambas, en la que el sujeto activo

[11] INTECO es un acrónimo utilizado para designar al ex Instituto Nacional de Tecnologías de la Comunicación con sede central en la ciudad de León (España), cuyo nombre fue modificado desde el año 2.014 y hasta la actualidad con la denominación de Instituto Nacional de Ciberseguridad (INCIBE).

se denomina *phisher*, haciéndose pasar por alguna empresa o institución de confianza, y utilizando la tecnología de la información y las comunicaciones, trata de embaucar al atacado para que le proporcione información confidencial, que posteriormente es utilizada para la realización de algún tipo de fraude (INTECO, 2.007, p. 38).

1.3. Modalidades y medios de comisión utilizados.

En este punto intentamos clarificar cuáles son aquellas modalidades y medios que son empleados por los *phisher* en los casos de suplantación de identidad de la persona. Adelantamos al lector que se explican distintos conceptos y temática relacionada directamente con la informática y tecnologías, para conocer de manera pormenorizada y detallada cómo se producen los ataques de este tipo. A continuación se presentan y analizan dichos medios y modalidades:

- Por medio de *emails* y *spams*.

La mayoría de los ataques de *phishing* son realizados vía *email*[12]. Los *phishers* pueden llegar a enviar millones de *emails* a listas obtenidas por el atacante o compradas a organizaciones dedicadas a este fin, utilizando diversas técnicas y herramientas informáticas para envío masivo de *spam*[13]. Estos *emails*, tienen un título inusual indicando algún tipo de urgencia; ésta estrategia sirve para llamar la atención de la víctima y lograr que siga los pasos que indica el correo electrónico.

Los *phishers* se aprovechan de las fallas de diseño en los puertos debido a que se manejan en texto plano, así el atacante logra enviar *emails* con procedencia engañosa a destinos legítimos, agregando al cuerpo del mensaje una *URL*[14] con ligera semejanza al nombre de la página legítima o archivos adjuntos con código malicioso, como resultado; si el usuario no se detiene a observar con detenimiento el mensaje recibido, puede ser víctima del ataque. El objetivo del envío de dicha *URL* reside en solicitar información de credenciales personales o laborales como claves de cuentas de la víctima, datos de tarjetas de crédito, entre otros (Belisario Méndez, 2.014, p. 4).

Entendemos que, luego de la exposición técnica sobre estos medios empleados, más allá que es de suma importancia el conocimiento, capacitación y

[12] El *email* es un mensaje transmitido a través de un sistema de correo electrónico.
[13] El *spam* es un mensaje o correo electrónico no deseado, no solicitado, recibiendo otros nombres como correo o mensaje basura.
[14] El *Uniform Resource Locator* en su denominación en inglés o conocido también como localizador o identificador uniforme de recursos, es la ruta que se encuentra en la caja de texto ubicada en la barra de navegación del navegador y sirve para ubicar de manera precisa en un servidor, cualquier recurso (v.g. una imagen, un video o una página web).

aprendizaje sobre la temática abordada, lo determinante es poder detectar y prevenir eficazmente la presencia de algún *hacker* o *phisher* que esté intentando acceder a la información confidencial del usuario para repeler las potenciales consecuencias perjudiciales de este tipo de ataque. Lo crucial del asunto está orientado a la tarea de detección y prevención por partes de los usuarios para no ser presa fácil de estos suplantadores, ya que una vez que logran ingresar a los datos personales del individuo, pasan a tomar el dominio de la situación que en muchos casos es irreversible.

- Basado en páginas *web.*

Estos ataques se ejecutan a través de la inserción de código malicioso o explotando una vulnerabilidad existente en el servidor *web*[15], aplicación o *browser*[16] del usuario. El *phisher* puede comprometer una página *web* legítima o crearla con un servicio de *web hosting*[17], para luego ejecutar el código malicioso desde ahí. La página *web* puede ser una publicidad engañosa en *internet*, llamado *banner* en inglés.

Algunas de las técnicas más conocidas de ataques de *phishing* se realizan a través de páginas *web* se consuman mediante la creación de publicidad falsa en *internet*, *banner*, con texto y/o imágenes gráficas para redirigir al usuario a su página *web* y obtener información confidencial; también puede ser por medio del uso de artículos ocultos dentro de la página *web*, para búsqueda y captación de posibles víctimas; asimismo, se utilizan ventanas emergentes conocidas como *pop-up* del *browser*, simulando provenir de un sitio válido, que anuncia a la persona que fue ganadora de una lotería, redirigiéndola a una página *web* falsa.

Es frecuente a su vez que los *phishers* saquen ventaja de una vulnerabilidad conocida en un *browser*, insertándole contenido malicioso, por ejemplo *keyloggers*[18], captura de pantalla, *backdoor*[19] (puertas traseras), troyanos[20], *botnet*[21] y otros

[15] El servidor *web* o servidor HTTP es un programa informático que se encarga de realizar diferentes tipos de conexiones con el cliente de *internet* y generando o cediendo una respuesta en él. Por lo general el código recibido se obtiene mediante un navegador web, debiendo usar para la transmisión de esos datos un protocolo, siendo el más utilizado el HTTP.
[16] *Browser* es un navegador de *internet*, que requiere de un *software* o programa que permita la visualización de los contenidos que presenta una página web.
[17] *Web hosting* es el nombre que recibe el alojamiento u hospedaje de páginas *web*.
[18] *Keyloggers* es un programa informático que registra cada golpe de teclado hecho por un usuario de la computadora, especialmente con el fin de obtener acceso fraudulento a las contraseñas y otra información confidencial.
[19] *Backdoor* es una característica o defecto de un sistema informático que permite el acceso no autorizado.
[20] Troyano es un programa informático que contiene código malicioso que se hace pasar por un programa confiable y legítimo.

programas, desde una página *web* oficial previamente comprometida para descargarlo a la computadora de la víctima. También se explotan fallas o vulnerabilidades de sitios *web* de confianza a través de métodos como *cross site scripting*[22], para ocultar el nombre de la página *web* falsa. Por último, los *phishers* se aprovechan del exceso de confianza que tienen los usuarios para almacenar claves, *cookies*[23] e historial en el *browser*, como asimismo explotan alguna vulnerabilidad del *browser* de la víctima o protocolo que la afecte (Belisario Méndez, 2014).

Observamos que luego de haber definido varios de los conceptos utilizados desde un enfoque informático y con relación a este método aplicado por los *phishers*, estos últimos apuntan vehementemente al aprovechamiento de las debilidades, flaquezas, falta de información y de conocimiento de las víctimas que navegan en distintos sitios o páginas *web*, para concretar la finalidad ilícita. Es claro que la nota tipificante está en el ardid o engaño que utilizan los victimarios a la hora de conseguir con éxitos aquellos resultados esperados por ellos.

- Por medio de *tabnabbing.*

Aza Raskin[24] descubrió este ataque de *phishing* basado en *web*, el cual consiste solicitar al usuario sus credenciales de acceso a cuentas de correo electrónico o redes sociales, en páginas *web* que aparentan ser reales.

Para que el ataque funcione, es necesario que el usuario esté navegando en *internet* con varias pestañas abiertas en el *browser* (*tabs* por su término en inglés) y que al menos una posea códigos de *tabnapping* (pestaña en reposo). Éste reconoce si las pestañas abiertas en el *browser* tuvieron inactividad por algunos segundos.

Insertando código malicioso en *javascript*[25] llamado *tabnabbing*, se modifica una función de *HTML*[26] en el código de *tabnapping*, así el *phisher* reemplaza la páginas *web* con inactividad, por una copia exacta.

---

[21] *Botnet* es una computadora o servidor infectado con un programa malicioso que permite que sea controlado de forma remota por un servidor principal para realizar diversas actividades criminales.

[22] *Cross site scripting* es una técnica utilizada por el hacker que se aprovecha de las vulnerabilidades encontradas en el código de aplicación *web*, para enviar contenido malicioso al usuario y recolectar información de la víctima.

[23] *Cookie* o galleta informática es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

[24] *Aza Raskin* es un diseñador de interfaz estadounidense, destacado por trabajar como jefe de experiencia de usuario Mozilla Labs y diseñador principal para Firefox.

[25] *Javascript* es un lenguaje de programación que permite crear contenido nuevo y dinámico, controlar archivos de multimedia o crear imágenes animadas.

[26] *HTML* significa Hyper Text Markup Language, provee una estructura básica el cual es usado para crear documentos electrónicos que son mostrados en Word Wide Web; páginas web en *internet*. Cada página contiene una serie de conexiones a otras páginas web llamadas Hypelinks o Links a páginas

Luego de un par de segundos, el sitio web con código de *tabnapping*, cambia de *favicon*[27] y muestra la copia insertada por el *hacker*[28].

El *favicon* y título de la página *web* falsa actúan como una fuerte señal visual. Debido a que la memoria del ser humano es flexible, cuando el usuario regresa a la página *web* con el código de *tabnabbing* insertado piensa que, por ejemplo, dejó abierta la página de *gmail* (mensajería electrónica de *google*) y que su sesión expiró.

De esta forma el usuario ingresa sus credenciales, las cuales serán almacenadas en un servidor del atacante, para luego ser direccionado automáticamente a la página *web* legítima de *gmail*. Los *browser* de *Mozilla Firefox* y *Chrome*[29] son susceptibles a este ataque (Belisario Méndez, 2.014, p.8).

Analizamos en esta modalidad específica de suplantación de identidad que, por cierto es bastante novedosa, la actividad ilícita de los atacantes apunta a los casos en que el usuario se encuentra navegando con varias ventanas o pestañas de manera simultánea y que se encuentran en estado de reposo o inactividad. Es en ese momento en que el *phisher* procede a la emisión del código malicioso que tiende a la obtención de la información personal del individuo. Mediante el engaño manipulado es que los datos que consigue el victimario es a causa de la propia torpeza o error al momento de la operación que ejecuta voluntariamente el usuario – víctima, siendo él mismo el que proporciona valiosos datos al atacante.

- Basados en voz sobre IP (VoIP)

El ataque de *phishing* basado en voz sobre IP se denomina *vishing.* Al igual que los casos anteriores, el objetivo es que la víctima provea información sensible. Por lo general, estos *hackers* informáticos pueden llamar a un directorio de números telefónicos de una región o tener acceso a una lista de teléfonos de una organización o de personas. En una llamada telefónica se pueden obtener detalles como la fecha de nacimiento, fecha de expiración de tarjetas, PIN de acceso, porque se basan en la interacción humana para persuadir a la víctima.

El *phisher* dejar un mensaje de voz automatizado haciéndose pasar por una entidad de confianza, como un banco, indicando que hubo algún tipo de problema con

---

web. Cada página web en *internet* está programada con alguna versión de HTML. Sin HTML los browser o navegadores para acceso a *internet*, no sabrían cómo mostrar texto o imágenes.

[27] *Favicon* es la imagen asociada a una página web, que se encuentra al principio de la barra de búsqueda.

[28] *Hacker* es un individuo con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.

[29] Mozilla Firefox y Chromes son navegadores de *internet*.

la cuenta bancaria, por ejemplo: necesidad de cambiar el PIN de cajero o autorizar un pago. Dicho mensaje indica un número telefónico para comunicarse y resolver el problema o le indica que vaya a una página *web* específica, parecida a la del banco, para que introduzca datos validando la identidad de la víctima para finalmente, obtener acceso a su cuenta y dinero.

Debido al incremento de ataques de *vishing*, se han investigado formas de prevenir o detener estos ataques a través del estudio del comportamiento humano. Los métodos o algoritmos detectores de mentiras convencionales, no han sido muy eficientes para ser aplicados a la comunicación digital, por lo que *J.-H. Chang y K.-H. Lee*[30] crearon un algoritmo específicamente para la detección de *phishing* en VoIP. Debido a que el ser humano experimenta signos involuntarios cuando miente como cambios en el registro de la voz, movimientos faciales, de ojos y/o manos, la voz fue el factor de relevancia para el desarrollo de dicho algoritmo.

La cualidad de voz de una persona se define por el tono de voz, volumen e inflexiones, conformando los factores para diferenciar entre una verdad y una mentira. Cuando un argumento es verdadero, la duración en la pronunciación silábica es mayor (tiempo de duración entre silabas y palabras). Para probar el algoritmo, se tomaron voces de personas comunes y *phishers* reales, extraídos de comunicaciones vía telefonía celular, VoIP y pública (PSTN) para obtener resultados más reales, en lugar de una base de datos con información y situaciones controladas.

Los resultados de dicha investigación comprobaron ser eficaces para la detección de *vishing*, dando la posibilidad de utilizar la tecnología para detección de estafas vía telefónica (Belisario Méndez, 2.014, pp. 17-18).

Examinamos en esta oportunidad otro de los métodos analizados, el que se denomina *vishing* que se trata de otra modalidad relativa a la suplantación de identidad concretada en este supuesto mediante aparente comunicación de una "institución o entidad bancaria oficial", en que el cliente es advertido por presuntos problemas en los datos de la tarjeta de crédito o cuenta bancaria. El engaño consiste en este caso en el hecho que la voz que se comunica con la víctima es muy similar a la de las operadoras de los bancos, llevando así adelante el plan ilícito en la obtención de información sensible. Si bien todas las personas se encuentran expuestas a este tipo de

[30] *J.-H. Chang y K.-H. Lee* son doctores en informática coreanos.

ataques, lo sufren con mayor frecuencia las personas de la tercera edad, quienes en su gran mayoría, no piensan que están siendo víctimas de *phishers*, por lo que proporcionan todos los datos que le son solicitados, siendo engañados en su buena fe. Es por ello que se recomienda ante todo la no facilitación ni revelación de información confidencial a ningún desconocido.

- Basados en mensajería instantánea.

La mensajería instantánea es un medio de comunicación a través del uso de programas tipo cliente para intercambiar mensajes de texto y voz en tiempo real. Entre los programas más conocidos se encuentran: *skype, whatsapp, hangouts, pidgin y yahoo! messenger*. Estos pueden ser instalados en cualquier tipo de dispositivo con conexión a *internet*, como computadora, *tablet o smartphone*.

Dichos programas permiten el intercambio de archivos, *URL*, imágenes, videos, lo que permite que los ataques vía *web* sean aplicables a mensajería instantánea. Sólo es necesario que la víctima haga *click* en la *URL* o archivo adjunto para que el código malicioso pueda ejecutarse sin intervención del usuario.

Primero el *phisher* crea un mensaje y lo envía de forma automática a una lista de contactos. Una vez que toma el control de una víctima, localiza su lista de contactos para aumentar su base de datos y seguir expandiéndose y por último, insertar un virus y extrae información (Belisario Méndez, 2.014, p.19).

Aportamos sobre esta modalidad que existe un trabajo previo del *phisher* al momento de confeccionar el mensaje malicioso que es enviado a un listado de personas a las que contacta para infiltrarse entre sus contactos. Solo requiere que la víctima ingrese presionando solo un botón de cualquier dispositivo para que el código de ataque recabe toda la información necesaria, sumado también otras personas a este método, los que son potenciales víctimas. En este tipo de casos se recomienda que el usuario verifique la procedencia y contenido de la mensajería que llega a su dispositivo y que incluso ante la duda, no ejecute ningún tipo de operación, evitando así el dominio y la extracción de información confidencial de parte del *hacker*.

- Por medio de *spear phishing.*

La definición de *spear phishing* por *search security* indica que es un fraude de suplantación de identidad vía *email*. La diferencia entre los ataques de *phishing*

común basado en *email* y el *spear phishing* es que no son ataques aleatorios y generalizados, sino que están dirigidos a una organización o individuo en particular.

Los ataques de *spear phishing* tienen altas probabilidades de ser exitosos porque no son detectados fácilmente por herramientas de *antispam*[31]. Utilizando suplantación de identidad, el origen del correo electrónico pareciera ser de una persona de alta jerarquía dentro de la organización solicitando algún tipo de información con carácter de urgencia e importancia, engañando así a usuarios con y sin conocimientos en informática. Así obtiene acceso completo a información de interés del atacante.

La secuencia del ataque consiste en cuatro operaciones bien diferenciadas:

- ✓ Primero, el atacante ubica la información de contacto de la página *web* de la organización que desea atacar.
- ✓ Segundo, se detecta en la misma página *web*, un acceso a un sistema de su interés que requiere autenticación con usuario y contraseña, como por ejemplo, la *intranet*[32].
- ✓ Tercero, busca datos de contacto que aparecen en la página *web* de la organización para enviar un correo electrónico que parezca auténtico, usando como origen, la identidad de un individuo autorizado para solicitar información confidencial a los empleados, tal como ocurre en el caso de un gerente o administrador de la red.
- ✓ Cuarto, envía el *email* a un empleado de la misma organización, solicitándole cualquier tipo de información sensible o indicarle que se autentique a la *intranet* de la compañía a fin de instalar y difundir código malicioso para poder extraer información sensible la organización. Si el empleado de la compañía cae en la trampa, el atacante suplanta su identidad y obtiene acceso a información sensible desde sistemas a la cual está autorizado (Belisario Méndez, 2.014, pp. 25-26).

Consideramos con relación a este tipo de modalidad que se trata de una especie de suplantación de identidad de difícil detección al momento en que el *phisher* está intentando conseguir la información sensible de la empresa, organización o persona. Como surge de lo detallado, se trata de comunicaciones vía *mail* que aparentemente efectúan personas de gran importancia dentro de la compañía, que tiene como destinatarios a trabajadores de la organización con el fin de acceder a una

[31] El *antispam* es un método o estrategia para prevenir el correo o mensajería no deseada, no solicitada o basura.

[32] *Intranet* es una red informática interna de una empresa u organismo, basada en los estándares de *internet*, en la que las computadoras están conectadas a uno o varios servidores web.

base de datos o información confidencial, y de quienes es altamente probable que se apodere dado que el *phisher* se hace pasar por esa persona importante de la organización; pasa desapercibido dentro de los empleados de la compañía en cuestión. Más allá de lo explicado ut supra, creemos que contratando personal extremadamente capacitado como es el caso de ingenieros, licenciados en sistemas y de profesiones afines, es factible crear o reforzar los sistemas de seguridad que trunquen los fines ilícitos de estos tipos de ataques.

- Por medio de *whaling.*

La técnica de *whaling*[33] tiene un mayor nivel de sofisticación que *spear phishing*. Se basa en el mismo concepto, pero difiere en que solo ataca a personas con altos cargos ejecutivos y líderes claves dentro de importantes corporaciones empresariales y políticas. Se pueden encontrar dos diferencias significativas entre *whaling, spear phishing* y ataques de *phishing* tradicional:

- ✓ *whaling* no es un *spam*; ya que requiere de investigación previa de un alto ejecutivo determinado, para así desarrollar un *email* personalizado, para parecer lo más creíble y genuino posible. En esa investigación se busca obtener datos puntuales como título profesional, cuenta de correo electrónico personal y laboral, número de interno telefónico y nombres de personas de jerarquía similar en la corporación.
- ✓ La segunda diferencia consiste en que el *hacker* tiene como objetivo obtener el control de la computadora de la víctima para conseguir acceso a cualquier información relevante para el atacante, tales como sus claves de acceso (Belisario Méndez, 2.014, pp. 38-39).

Examinamos por último la modalidad conocida como *whaling* que es una subespecie del *spear phishing,* cuya particularidad está dada en el estudio, investigación y seguimiento previo que se realiza sobre el tipo de víctima a la que se persigue o se pretende engañar, antes de lanzar el ataque. En el caso los sujetos pasivos son altos ejecutivos, de alto rango que pertenecen a empresas multinacionales, corporaciones que manejan información de un extremo valor para la organización. Como corolario de lo expuesto, consideramos que debido a la sofisticada modalidad de suplantación de identidad presentada, para repeler todo ataque de los *phisher*, éstas

[33] *Whaling* es una modalidad específica de *phishing.*

corporaciones no sólo deberían contratar el mejor y más capacitado personal en sistemas informáticos, sino que también se torna diríamos necesario la implementación de programas de seguridad informática e inclusive la intervención de las fuerzas de seguridad (v.g. policías) altamente preparadas en el ámbito de las tecnologías para que – según las circunstancias del caso y coadyuvándose entre sí – trabajen en la prevención, detección y frustración de esta forma avanzada de ataques en pos de la conservación de la información valiosa de la corporación.

1.4. Fases y finalidades de la suplantación de identidad.

El análisis de estas etapas puede constituir una valiosa información en la lucha contra los *phishers*. La existencia de distintas variantes de este fraude implica que, en muchas ocasiones, las fases pueden cambiar en cuanto a su profundidad, extensión y dificultad, al igual que respecto a los agentes que deben intervenir y cuál es el papel que deben jugar.

Se observa que son seis las fases principales que se completan en todo ataque de *phishing:* de planificación, preparación, ataque, recolección, fraude y post ataque (INTECO, 2.007, p. 50).

- ✓ Fase de planificación.

Durante esta etapa, el *phisher* se encarga de tomar las principales decisiones que va a llevar a cabo como es por ejemplo a quién va dirigido el ataque, cómo y dónde se va a realizar, qué tipo de argucia se va a utilizar, cuál es el objetivo del fraude o qué medios necesitará para hacerlo.

Una de las primeras cuestiones que se plantea un *phisher*, cualquiera que sea la modalidad elegida, es tomar la decisión de realizar el ataque de forma conjunta o bien de forma individual. Otra de las decisiones tomadas por el victimario en esta fase es qué tipo de datos se desean conseguir, cómo puede ser información de cuentas bancarias, nombres de usuario y contraseñas o datos personales de diversa índole. Esta cuestión estará vinculada a cuál es el tipo de engaño que se intenta cometer.

La planificación es variable y puede consistir desde la aceptación de una base de direcciones electrónicas conseguidas al azar, hasta el *spear phishing*, que puede conllevar el estudio pormenorizado del perfil de las víctimas, pasando por todas las posibilidades existentes entre ambos extremos. Asimismo es de suma importancia poder determinar la institución o empresa a suplantar, ya que muchas de las estafas

implican que el *phisher* se haga pasar por una entidad en la que la víctima tenga confianza (INTECO, 2.007).

Advertimos que ésta es una primera fase previa a la consumación del ataque en que el *phisher* se encarga de realizar un análisis exhaustivo de aquellas personas u organizaciones que pretende atacar y sacar información; puede tratarse de ataques lanzados en forma aleatoria o bien puede tratarse de una ofensiva dirigida a una persona en particular. Esta fase viene a configurar aquella etapa racional, del proyecto en abstracto que debe organizarse y prepararse con antelación a su puesta en marcha.

- ✓ Fase de preparación.

Algunas de las tareas que deben realizar los delincuentes es conseguir el *software*[34], los datos de contacto, localizar los destinos de sus ataques, preparar sus equipos, construir los sitios *web* diseñados para efectuar el fraude y otras tareas, teniendo en cuenta las necesidades de cada tipo de modalidad.

En algunas ocasiones, los *phishers* realizan ataques muy localizados dirigidos a personas u organizaciones específicas, lo que requiere el envío de correos mucho más elaborados que los que se utilizan en envíos masivos. Lo que es interesante de este tipo de ataques es su estudiada segmentación en la búsqueda de objetivos y preparación del engaño (INTECO, 2.007).

Comentamos que en esta segunda fase, se presentan las primeras manifestaciones e indicios que muestran la gestación tangible de la actividad ilícita de los *phishers.* Del plan elaborado en su faz lógica, se avanza gradualmente en la faz material, que se exterioriza en las tecnologías utilizadas como por ejemplo los dispositivos empleados (v.g. pc, *tablets*, *notebooks*), y también en cuanto a los programas informáticos usados para el envío de distintos correos o *mail* a las potenciales víctimas. Lo central radica en la preparación del campo o terreno en que será efectuado el ataque.

- ✓ Fase de ataque.

En esta oportunidad las estafas que implican una participación de las víctimas requieren de su concurso, ya que acciones como abrir un correo electrónico, visitar una página *web* o realizar una búsqueda, son acciones necesarias para que el ataque se consuma. En cuanto a las tareas, no hay tareas comunes, ya que dependen del tipo de *phishing* seleccionado. Los puntos de infección en este tipo de ataques son el

[34] Software es un conjunto de programa informáticos que posee una computadora para la realización de diversas actividades.

momento de la propia infección, como es el caso donde entra en el sistema el *malware*[35], sin ser necesaria su ejecución o bien en el momento en que se ejecuta el código malicioso (INTECO, 2.007).

Respecto a la consecución del objetivo por parte del atacante, esto es, la captación de información confidencial, también difiere en ubicación o en función del tipo de aplicación utilizada:

• Ataques en los que el propio *phisher* se apropia de la información por la fuerza (secuestradores de sesión, troyanos *web* y reconfiguración de sistema a través de *proxy*[36]).

• Ataques en los que el código malicioso recopila la información dentro de los dispositivos de almacenamiento de la máquina infectada.

• Situaciones en las que es el usuario, de forma involuntaria, quien proporciona la información (*keyloggers/screenlogger* y envenenamiento del fichero *hosts*[37]) (INTECO, 2.007, p. 56).

Si bien esta y las demás fases son analizadas desde un enfoque informático, disentimos jurídicamente sobre la afirmación que la suplantación de identidad analizada en el presente trabajo sea en *stricto sensu* un fraude o estafa, ya que se trata a nuestro entender de una conducta autónoma, con características particulares y que ergo requiere de regulación legal específica en nuestra legislación penal; es probable que a partir de la perpetración del *phishing* y como derivación de ello, puedan cometerse fraudes o estafas, lo que no es igual a decir que la suplantación de identidad sea *per se*[38] una estafa o fraude.

Aclarado el punto, creemos conveniente expresar que en esta fase de ataque, toda la planificación y preparación que fuera ideada por los *hackers* informáticos, necesita en esta etapa de la "colaboración" de las personas u organizaciones a las que están dirigidas como así también de la producción material de todas las acciones llevabas a cabo por aquellos para el logro del objetivo. Como se explicó anteriormente, existen diversas modalidades de *phishing*, pero el común denominador

[35] *Malware* conocido también como código o programa malicioso, es un tipo de *software* que tiene como objetivo infiltrarse o dañar una computadora o sistema de información.
[36] *Proxy* dentro de una red informática, es un sistema de *software* que se ejecuta en un equipo de cómputo que actúa como intermediario entre un dispositivo de punto final, como una computadora, y otro servidor del cual un usuario o cliente solicita un servicio.
[37] El fichero o archivo host de un ordenador es utilizado por el sistema operativo para guardar la correspondencia entre los dominios de *internet* y direcciones IP.
[38] *Per se* es una expresión latina que significa en sí mismo.

es que para la producción del resultado esperado por el *phisher*, es necesaria la "participación y ejecución" activa en las órdenes dadas por el destinatario en su sistema informático, que viene a configurar el último eslabón de la cadena y que permite a los victimarios el éxito de la operación: recabar toda la información confidencial deseada.

- ✓ Fase de recolección de datos.

La fase de recolección de datos implica actividades de "colaboración" del damnificado como se ha mencionado anteriormente. Ello implica la espera de víctimas que entren en el servidor atacado, que respondan al mensaje enviado o que visiten la *web* fraudulenta.

A su vez, en el caso de ataque a un servidor, normalmente una vez instalado el código en la fase anterior es necesaria su ejecución para conseguir los datos, tarea más propia de esta fase (INTECO, 2.007).

Observamos que en esta fase, los *phisher* han concretado el envío de distintos *mails* y correos a las potenciales víctimas con la finalidad de conseguir la mencionada información confidencial; estimamos que son potenciales porque ello se encuentra sujeto a la condición de la apertura o no de la mensajería enviada. Claro está que no en todos los casos la suplantación de identidad tendrá resultados positivos para los *phishers*, aunque son presa fácil aquellos individuos que no tiene preparación o formación en informática, tecnologías y que a su vez ejecutan acciones sin la precaución del caso ni el asesoramiento adecuado.

- ✓ Fase de ejecución del fraude.

Una vez realizada la recolección de aquellos datos que sean de interés para el *phisher*, el siguiente paso efectuado por el delincuente informático es la realización de la defraudación, que puede ser de forma directa o bien de forma indirecta mediante la venta de los datos obtenidos para que otros estafadores consuman este tipo de modalidad (INTECO, 2.007).

Pensamos sobre esta fase que la terminología utilizada por el INTECO al referirse a "delincuente, defraudación, estafa" con respecto a la temática abordada, no es adecuada si se parte de la base que la suplantación de identidad no está regulada en el derecho penal español ni en nuestro derecho penal. Por ello, preferimos referirnos a los sujetos activos de esta actividad como *phishers*, victimarios, *hackers* y a la conducta en cuestión, denominarla *phishing* o suplantación de identidad., evitando de esa forma el uso incorrecto de conceptos jurídicos.

Por otra parte, negamos que la suplantación de identidad sea soló con fines de defraudar a través de la información confidencial recabada. Afirmamos que si bien en muchos casos se pueden consumar estafas o defraudaciones patrimoniales a partir de esta actividad, en otros casos también puede tener como finalidad el daño a la imagen, el buen nombre, el prestigio y el honor de la persona sin exigir el pago de un precio; otras veces se pide el pago de un monto de dinero para evitar que se publiquen o difundan datos sensibles de la víctima para resguardar su intimidad; en otros casos por ejemplo, se extorsiona a la víctima mediante el pago de un "rescate" en dinero para la recuperación del usuario y contraseña de una cuenta bancaria, la clave de una tarjeta de crédito y demás información personal, con el riesgo latente de efectuar el pago y no recuperar dichos datos confidenciales. En suma, a partir de la realización de la suplantación de identidad es diversa la gama de objetivos y fines que pueden perseguir los *hackers* informáticos y que no se reducen sólo a estafas o defraudaciones.

- ✓ Fase de post-ataque.

La última fase, denominada de post-ataque está referida a la finalidad que tienen los *phishers* de eliminar todas aquellas pistas o rastros que hayan quedado del ataque efectuado. En este sentido, todos los implicados en dicho ataque pueden ser susceptibles de participar – activa o pasivamente – en el proceso, mientras que las tareas serán específicas dependiendo del tipo de aporte o colaboración realizada.

Lógicamente, además de las actividades propias de esta actividad, los estafadores procederán al blanqueo de los beneficios obtenidos de la operación y otros procesos normales en cualquier tipo de robo o fraude (INTECO, 2.007).

Detectamos como en las etapas anteriores el uso incorrecto o confuso de los términos en relación al *phishing*; insistimos y a los fines de una crítica constructiva, que debiera corregirse la utilización de este lenguaje informático, adaptándose al leguaje técnico–jurídico. Referimos en cuanto a esta última fase, que luego de lograr los resultados esperados, los *phishers* que han actuado en conjunto y a lo largo de todo el proceso y fases, en esta oportunidad van a avocarse a la eliminación de rastros, indicios, huellas, a la "limpieza" de toda aquella actividad que directa o indirectamente esté relacionada con los daños y perjuicios, producto de la suplantación de identidad. Dependiendo de las tareas o funciones de los sujetos activos, tendrá cada uno un propósito que cumplir, una actividad tendiente a lograr en definitiva la impunidad de todos los integrantes.

1.5. Sujetos activos y pasivos en la suplantación de la persona.

En lo referido a los sujetos activos de la suplantación de identidad, son personas físicas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, que tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de ilícito (Temperini, 2.012).

En relación a los diferentes sujetos que llevan adelante actividades delictivas relacionadas a la suplantación de identidad digital, se pueden identificar dos grandes grupos:

- ✓ Aquellos delincuentes que actúan solos, generalmente de una franja etaria de menores de 25 años y con conocimientos técnicos limitados pero que sirven a sus objetivos. En América Latina la mayoría de los delitos relacionados al *phishing* son cometidos por este tipo de personas.
- ✓ Grupos organizados, compuestos por personas con distintas especialidades y recompensas de acuerdo a sus funciones del riesgo que asumen dentro del grupo. En este caso se destacan grupos de Europa del Este, EEUU y Brasil.
- ✓ Si bien no puede existir el ilícito como tal sin la participación de estos grupos mencionados, dada la falta de educación del usuario, le cabe cierta responsabilidad al mismo, dado que por lo general no se suele proteger de manera adecuada la información personal, entregándola ante el más mínimo engaño o ante la ingenuidad de obtener un supuesto "beneficio" por ello. Ejemplos de este tipo de comportamiento son las loterías falsas que prometen premios millonarios con sólo enviar un nombre y apellido, o las cadenas de correo electrónico que ofrecen ventajas adicionales a quienes realicen tal o cual acción, a cambio de entregar información personal (Temperini, 2.012).

Con respecto a los sujetos pasivos de la suplantación de identidad, se mencionan:

- ✓ La víctima del ilícito, es el usuario o el hombre "común" sin una formación técnica o especializada en informática, siendo uno de los sujetos pasivos

más vulnerables y expuestos a los distintos ataques de suplantación de identidad, desplegada por los sujetos activos antes mencionados.

- ✓ Las entidades comerciales, financieras y crediticias que conceden servicios, créditos y entrega de fondos a terceros no apropiadamente identificados, o que realizan controles débiles y fácilmente evitables por los delincuentes. En Argentina, la Ley Nº 25.246, establece la obligación para las financieras (junto a otros tantos sujetos obligados) a recabar de los usuarios los documentos que prueben fehacientemente su identidad.
- ✓ Finalmente el Estado que ante su actuar negligente, también lo transforma en parte responsable, porque posibilita la comisión del ilícito a través de la falta de normativa, campañas de concientización y controles indispensables a la documentación del ciudadano, la dificultad para denunciar esta actividad ilícita y sobre todo la ausencia de auditorías - que existen en la teoría pero son ineficientes en la práctica- impuestas a empresas de servicios y entidades financieras y crediticias mencionadas anteriormente (Temperini, 2.012).

1.6. Conclusiones parciales.

Luego de abordar este primer capítulo, hemos trabajado sobre la conceptualización del *phishing* como también sobre sus características particulares para su mejor delimitación y comprensión, afirmando que dicha conducta consiste en un ataque informático, de ingeniera social, desplegado por los *phishers* que son sujetos con alto grado de conocimiento y preparación en sistemas informáticos, cuya finalidad se traduce en la adquisición de información confidencial de la víctima mediante el uso de ardid o engaño. Entendemos que se trata de una actividad ilícita, pues según los casos se utiliza para producir daños patrimoniales y extrapatrimoniales.

La suplantación de identidad de la persona es realizada mediante la utilización de diferentes dispositivos informáticos – llámese computadoras, celulares, *tablets* etc. –, modalidades, fases, finalidades y objetivos. El perfil del *phisher* es diverso ya que la franja etaria puede variar en el atacante, que en ocasiones actúa solo pero que también puede hacerlo de manera organizada con otros individuos, con una función específica y que es determinante para llevar a cabo este tipo de actividad.

Por otra parte, avizoramos que los ataques de *phishing* no hacen ningún tipo de distinción y están dirigidos tanto a personas físicas como jurídicas; en el primer caso, recomendamos al usuario que ante la duda respecto de la procedencia y el contenido de la mensajería o correos enviados a su casilla o cuenta de *mail*, no ejecuten la tarea que el *phisher* espera que la potencial víctima realice, evitando así consecuencias dañosas. En el caso de las organizaciones la situación es diferente pues cuentan con sistemas de seguridad que las previenen y defienden en alguna medida de potenciales ataques de este tipo, aunque no hay garantías de protección en aquellos casos de *phishing* sofisticado, que en ocasiones vulneran estas defensas.

En suma enfatizamos en las funciones de prevención, detección y frustración de los ataques de suplantación de identidad que todo sujeto debe observar al momento del uso de sistemas informáticos, ya que en el caso de ingresar a la zona de control del *phisher*, éste tendrá el dominio de la situación, de la información confidencial, difícilmente podrá ser recuperada y lo que es peor aún, podrá causar daños y perjuicios irreparables.

CAPITULO II: FALTA DE MARCO REGULATORIO DE LA SUPLANTACION DE IDENTIDAD EN EL DERECHO ARGENTINO.

2.1. Introducción.

Comenzando con el análisis del presente capítulo se parte de la afirmación que en el derecho penal argentino vigente no se encuentra regulada típicamente la figura de la suplantación de identidad de la persona; si bien es cierto que la misma puede constituir un ilícito que vulnera el ordenamiento jurídico en sentido amplio, también no es menos cierto que esta actividad no configura desde el derecho penal una conducta delictiva que sea merecedora de una sanción penal.

Por otra parte se hace una transcripción en concreto de tres proyectos de ley sobre el *phishing,* el primero de ellos elaborado por el legislador de ese momento Jorge Monastersky mediante el proyecto D. 4643/2010, el que no tuvo sanción legislativa; posteriormente los legisladores por aquel entonces María de los Ángeles Higonet y Carlos Verna elaboran los proyectos de ley S. 2257/2.011 y S. 1312/2.012 los que tampoco tuvieron recepción en el ordenamiento jurídico argentino; se aclara en esta oportunidad que más allá de la crítica que pueda surgir de los términos

técnicos o jurídicos empleados por los legisladores en esos proyectos – que conceptualizan al *phishing* en algunos casos como hurto o como defraudación en otros –, esos intentos pretendieron regular la suplantación de la persona, siendo tal vez esa falta de precisión técnica uno de los puntos determinantes por los que no fueron sancionados como ley.

En un sentido similar la jurisprudencia argentina en un difícil intento por determinar el encuadre típico de la suplantación de identidad ante la falta de tipicidad y mediante la aplicación de analogía a nuestro entender, ha configurado a esta figura dentro del tipo penal del hurto y en el tipo penal de la estafa o defraudación genérica, según los casos y fallos que se mencionarán oportunamente.

Asimismo, comenzando por dar una definición de delito como aquella acción típica, antijurídica y culpable y habiendo afirmado que la conducta denominada *phishing* no constituye jurídicamente un delito del derecho penal, será necesario analizar brevemente los elementos que conforman la teoría del delito, a saber: acción, tipo penal, antijuridicidad y culpabilidad para establecer los estadios o presupuestos que deben cumplirse efectivamente para la configuración de la suplantación de identidad como una conducta delictiva.

2.2. *Falta de marco regulatorio en la ley 26.388 de delitos informáticos sobre suplantación de identidad.*

Por medio de la sanción de la ley Nº 26.388[39], sancionada el 04 de Junio de 2.008 y promulgada de hecho el 24 de Junio de 2.008, se sanciona en nuestro país la ley de delitos informáticos que modifica artículos específicos del Código Penal. El texto legal de la norma reza:

> Artículo 1: Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:
>
> El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
>
> Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

[39] Ley de delitos informáticos Nº 26.388.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

Artículo 2: Sustitúyese el artículo 128 del Código Penal, por el siguiente:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Artículo 3: Sustitúyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente:

"Violación de Secretos y de la Privacidad"

Artículo 4: Sustitúyese el artículo 153 del Código Penal, por el siguiente:

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Artículo 5: Incorpórase como artículo 153 bis del Código Penal, el siguiente:

Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Artículo 6: Sustitúyese el artículo 155 del Código Penal, por el siguiente:

Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Artículo 7: Sustitúyese el artículo 157 del Código Penal, por el siguiente:

Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Artículo 8: Sustitúyese el artículo 157 bis del Código Penal, por el siguiente:

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) 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 un (1) a cuatro (4) años.

Artículo 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.

Artículo 10: Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:

En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Artículo 11: Sustitúyese el artículo 184 del Código Penal, por el siguiente:

Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:

1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;

2. Producir infección o contagio en aves u otros animales domésticos;

3. Emplear substancias venenosas o corrosivas;

4. Cometer el delito en despoblado y en banda;

5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Artículo 12: Sustitúyese el artículo 197 del Código Penal, por el siguiente:

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

Artículo 13: Sustitúyese el artículo 255 del Código Penal, por el siguiente:

Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

Artículo 14: Deróganse el artículo 78 bis y el inciso 1º del artículo 117 bis del Código Penal.

Artículo 15: Comuníquese al Poder Ejecutivo.

Observamos en esta oportunidad y luego de la transcripción de los artículos correspondientes a la ley de delitos informáticos del año 2.008 que modifica los arts. 77, 128, el epígrafe del Capítulo III, del Título V, del Libro II, el art. 153, la incorporación del art. 153 bis, la modificación de los arts. 155, 157, 157 bis, la incorporación del inc. 16 al artículo 173, el segundo párrafo del art. 183, la modificación de los art. 184, 197, 255 y la derogación de los arts. 78 bis y el inc. 1 del art. 117 del Código Penal Argentino, no surge de la norma en cuestión analizada *ut supra* regulación jurídica alguna, ni tipo penal delictivo que encuadre a la suplantación de identidad de la persona, ni mucho menos una pena relacionada a la cuestión planteada; creemos que la pretendida configuración del *phishing* como conducta delictiva – desde un enfoque teórico y académico – deberá tratarse en primer término dentro de la teoría del delito para posteriormente ser tratada en un proyecto de ley, técnica y legalmente adecuado en miras a su sanción como figura delictiva en la ley penal.

2.3. Proyectos de ley sobre suplantación de identidad en la legislación argentina.

En materia de proyectos de ley existen unos pocos intentos por parte de legisladores nacionales destinados a regular la suplantación de identidad en el articulado del Código Penal. Tal es el caso del proyecto de ley D. 4643/2.010[40] que buscaba reformar el capítulo II sobre supresión y suposición del estado civil y de la identidad, incorporando el art. 139 ter en el que se regulaba sobre el mínimo y máximo de la pena y la acción típica sobre la suplantación de identidad, el que tampoco tuvo resultados positivos a la fecha. El texto original de la norma preveía que:

> Artículo 1. Incorpórese el art. 139 ter. del Código Penal que quedará redactado de la siguiente manera:
>
> Será reprimido con prisión de 6 meses a 3 años el que adoptare, creare, apropiare o utilizare, a través de *internet*, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca.
> La pena será de 2 a 6 años de prisión cuando el autor asumiera la identidad de un menor de edad o tuviese contacto con una persona menor de dieciséis años, aunque mediare su consentimiento o sea funcionario público en ejercicio de sus funciones.
>
> Artículo 2: de forma.

Entre los fundamentos dirigidos al Sr. Presidente del Senado para la aprobación del presente proyecto, el Dr. Monasterky analiza y expone que el "robo" de identidad es una de las actividades ilícitas de mayor auge en todo el mundo y que en nuestro país no es considerado un delito el hecho de hacerse pasar por otra persona por ejemplo en un *blog*, en una red social o en otro medio electrónico, concluyendo que dicha conducta no está tipificada.

Sobre la cuestión referida a la designación de la figura con el nombre de "robo" de identidad discrepamos, pues entendemos que la denominación más apropiada debería ser suplantación de identidad; el robo es un tipo delictivo con una fórmula regulada en la ley penal, mientras que la suplantación de identidad es una actividad que si bien puede ser considerada ilícita, a la fecha no está tipificada como

[40] Proyecto de Ley D. 4643/2.010 impulsado por el Dr. Jorge Monastersky ante el honorable Senado de la Nación Argentina para el tratamiento de la suplantación de identidad como delito.

delito. Intentar fusionar dos conductas – el robo que está tipificado y la suplantación de identidad que no lo está – sería incurrir en un error conceptual a la hora de darle un correcto encuadre legal; es por ello que lo más atinado sería regular de forma autónoma y con una fórmula inequívoca, la figura de suplantación de identidad.

En lo que respecta a la falta de tipificación mencionada por el autor del proyecto, adherimos a la idea esbozada al expresar que en ese momento no estaba y a la fecha no está regulada la suplantación de identidad de la persona; prueba de ello es que no surge del articulado del Código Penal ningún tipo delictivo con referencia a la conducta bajo análisis.

Por otra parte, en otro de sus fundamentos, afirma el proponente que el *phishing* es un tipo de conducta delictiva que está identificada como *white collar crime* (crimen de cuello blanco), desplegado por un grupo de sujetos que son conocedores de técnicas sofisticadas para ser llevada a cabo.

Nuevamente disentimos sobre la premisa de la que parte el dicente, pues conceptualiza al *phishing* como un crimen de cuello blanco o delito, cuando en *stricto sensu* no constituye penalmente tal conducta. Si en su proyecto buscaba la regulación típica de la suplantación de identidad a los fines de configurar un delito del derecho penal, es una equivocación tratar de antemano a una conducta como crimen o delito cuando en suma no lo es. Creemos que hubiera sido más acertado mencionarla como una actividad ilícita cuanto menos, pero bajo ningún punto de vista podía tratarse de una conducta delictiva si el proyecto pretendía justamente su regulación legal.

Siguiendo con el análisis crítico de los fundamentos del autor del proyecto, en otro orden de ideas, éste designa también a la conducta bajo análisis como "usurpación" de identidad y que a partir de ella pueden perpetrarse la comisión de gran cantidad de delitos como puede ser a modo de ejemplo una extorsión, una estafa o *grooming*[41].

Contrastamos otra vez en torno a la terminología empleada en este punto, pues si el tipo penal de usurpación está regulado dentro de los delitos que atentan contra la propiedad, específicamente sobre inmuebles, configura yerro haber tratado a esta

[41] *Grooming* es un delito que, utilizando comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos para contactar a un menor de edad, tiene por finalidad atentar contra la integridad sexual de la misma.

figura de suplantación de identidad - nombre que consideramos el correcto – como una usurpación, primero porque su concepto se encuentra relacionado con un ataque informático, de ingeniera social y cuya finalidad se traduce en la adquisición de información confidencial de la víctima mediante el uso de ardid o engaño y segundo, porque se trata de una actividad atípica; entendemos que si la intención del legislador era procurar la aprobación del proyecto, el uso de vocabulario técnico – jurídico debería haber sido más preciso a los fines de obtener su sanción.

Compartimos con el autor la idea que a partir de la producción de la suplantación de identidad de la persona, pueden cometerse conductas delictivas como son los ejemplos mencionados de extorsión, estafa o *grooming*. Discernimos que, si de una conducta que a la fecha no configura *per se* un delito pero de la cual se pueden cometer delitos del derecho penal como los expuestos ut supra, ergo es razonable sostener que debería legislarse sobre *phishing*, en un tipo penal delictivo con su correspondiente pena; por un lado para tener una regulación autónoma y por otro, para evitar su confusión con otras figuras penales.

Cabe mencionar también el proyecto de ley S. 2257/2.011[42] presentado por ante el Senado de la Nación Argentina como Cámara de origen del proyecto, que pretendía modificar el capítulo III sobre violación de secretos y de la privacidad, incorporando el art. 157 ter. que detallaba el mínimo y máximo de la pena y la acción típica de la conducta conocida como *phishing*, el que hasta la fecha no tuvo el resultado pretendido. El texto original de la norma preveía que:

> Artículo 1: Incorporase como Artículo 157 ter. del Código Penal de la Nación el siguiente:
>
> Art. 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.

[42] Proyecto de ley S. 2257/2.011 presentado por María de los Ángeles Higonet y Carlos Verna ante el honorable Senado de la Nación Argentina para el tratamiento de la suplantación de identidad como delito.

Artículo 2.- Comuníquese al Poder Ejecutivo.

Entre los fundamentos dados por los legisladores Higonet y Verna dirigidos al Sr. Presidente del Senado, manifestaban que el proyecto de ley tenía como objetivo la tipificación del delito del *phishing,* que definían como la capacidad de duplicar una página *web* para hacer creer al visitante que se encuentra en un sitio *web* original en lugar de uno falso y que normalmente se concreta mediante el envío de *spam*, que invita a la potencial víctima a la página falsa usada como señuelo y que el objetivo del engaño es adquirir información confidencial del usuario como es el caso de contraseñas, tarjetas de créditos o datos financieros y bancarios.

Coincidimos parcialmente en que si bien la conducta conocida como *phishing* o suplantación de identidad puede afectar la faz patrimonial de la persona mediante la adquisición de información confidencial con ardid o engaño, como es el caso de usuarios y contraseñas de cuentas bancarias, claves de tarjeas de crédito etc., agregamos que esta actividad no se limita sólo a ese ámbito porque también podría verse afectada la faz extrapatrimonial de la víctima como es el ataque que sufre en su buen nombre, prestigio, imagen, identidad o intimidad, habitualmente por medio del *hackeo* de sus cuentas en redes sociales – v.g. *facebook, instagram, twitter* etc. –, cuyas consecuencias dañosas dependerán de cuál sea en definitiva la finalidad que persiga el *phisher*.

En otro argumento sobre el presente proyecto, los presentantes consideraron en aquel tiempo que – al igual que en la actualidad – el *phishing* no estaba penado como un delito autónomo y que la obtención de datos a través de esta conducta o por cualquier otro medio, con la finalidad de defraudar, estaría encuadrada dentro de las previsiones del art. 173, inciso 16, incorporado al C.P. mediante Ley Nº 26.388 y que castiga con pena de un (1) mes a seis (6) años, a quien "*defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos*".

Al respecto, no estamos de acuerdo en el fundamento dado por los legisladores y es necesario aclarar dos puntos importantes: por un lado, la suplantación de identidad no era un delito autónomo pero tampoco podía considerarse un delito accesorio de uno principal, ni mucho menos aplicarse a esta figura atípica, otro u otros tipos penales por la prohibición de analogía que rige en el derecho penal; y por otro

lado, en cuanto a las finalidades del *phishing* podían variar dependiendo las características particulares del caso. Si bien es cierto que merecía regulación como delito autónomo, tampoco es menos cierto que no debía sólo circunscribirse a la finalidad de estafa o defraudación especial mencionada en comentario en el art. 173 inc. 16 del C.P., cuando los objetivos que tiene el *phisher* como se dijo anteriormente podrían ser la afectación del patrimonio (v.g. el derecho de propiedad) pero también la vulneración de derechos extrapatrimoniales de la víctima como puede ser la identidad, la imagen, el buen nombre o el honor.

Por otra parte, afirmaban los autores del proyecto que en principio el *phishing* era un tipo especial de estafa común del art. 172 del C.P. y que era necesario recurrir a la doctrina clásica del delito de estafa para saber cuándo quedará configurado el delito de estafa – y por lo tanto el de *phishing –,* sosteniendo que primero debe existir el ardid o engaño y luego el perjuicio patrimonial consecuencia de dicho engaño.

Advertimos y surge de manera evidente la contradicción puesta de manifiesto en los dos cometarios anteriores, ya que por un lado los dicentes expresaban en su primer comentario que el *phishing* era considerado como un tipo especial de estafa del art. 173 inc. 16 y en el segundo de los comentarios era tomado como una estafa común del art. 172. Más allá de la confusión y contrasentido de sus fundamentos, afirmamos acabadamente que la suplantación de identidad debía (y debe) legislarse como delito por su falta de tipificación penal. Asimismo entendemos que no configuraba ni uno ni otro tipo de estafa porque el concepto dado sobre el *phishing* es el de una actividad autónoma, con características particulares y más allá de requerirse la presencia del ardid o engaño, tendría que haber sido tratada como una conducta distinta del tipo de estafa común o especial, con un tipo y pena específica; prueba de su falta de regulación normativa, fue la presentación de ese proyecto para su legislación como conducta delictiva.

En un mismo sentido y mediante proyecto de ley S. 1312/2.012[43] por ante el Senado de la Nación Argentina, se realizó un nuevo intento de reforma pero en esta oportunidad se pretendía modificar el capítulo II sobre supresión y suposición del

[43] Proyecto de ley S. 1312/2.012 presentado por María de los Ángeles Higonet y Carlos Verna ante el honorable Senado de la Nación para el tratamiento de la suplantación de identidad como delito.

estado civil y de la identidad, incorporando el art. 138 bis que detallaba el mínimo y máximo de la pena y la acción típica de la suplantación de identidad, el que a la fecha tampoco prosperó. El texto original de la norma preveía que:

> Artículo 1: Incorporase como Artículo 138 bis del Código Penal de la Nación el siguiente:
>
> Art. 138 bis: Será reprimido con prisión de 6 (seis) meses a 3 (tres) años o multa de pesos veinte mil a pesos doscientos mil, el que sin consentimiento, adquiriere, tuviere en posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica que no le pertenezca, a través de *internet* o cualquier otro medio electrónico, y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para sí o para terceros.
>
> Artículo 2: Comuníquese al Poder Ejecutivo.

En un nuevo intento normativo, los legisladores Higonet y Verna, presentaban otro proyecto sobre suplantación de identidad (el anterior no había sido aprobado) y entre los fundamentos expuestos ante el Sr. Presidente del Senado entendían que el objetivo del presente era la tipificación del delito de suplantación de identidad que ellos consideraron "robo de identidad digital", manifestando que dicha conducta ocurre cuando una parte adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la intención de cometer fraude u otros delitos relacionados.

Consideramos errada la afirmación en el presente proyecto de la suplantación de identidad como "delito" cuando en ese momento no revestía (ni reviste) tal calidad; ¿qué sentido tendría entonces pretender la tipificación de una conducta que los legisladores estimaban de antemano como delictiva?; tampoco nos parece acertada la designación de esta actividad como "robo de identidad digital" porque nuevamente confundieron el tipo robo y la suplantación de identidad no tipificada. Por ello en un comentario anterior, afirmábamos la necesidad de su tratamiento como figura penal autónoma con su correspondiente sanción, sin perjuicio de reconocer que de esta actividad atípica, pueden cometerse distintos delitos. Asimismo coincidimos parcialmente sobre la finalidad de fraude que puede existir en cuanto al tema bajo análisis, pero asegurando que no es esa la única finalidad que dicho comportamiento persigue como se mencionó oportunamente.

En otro fundamento, los redactores del ensayo expresaron que en aquel tiempo, la suplantación de identidad digital estaba en auge por su falta de regulación legal; que había aumentado la base de datos ilegales con información privada, permitiendo acceder así a los "delincuentes" con relativa facilidad a esos datos, que constituye la materia prima para concretar la "usurpación" de identidad.

Sobre el punto hacemos notar que el *phishing* – de un fundamento a otro –, pasó de ser un delito a dejar de serlo ya que en este último supuesto, el crecimiento de esta conducta se debía a su falta de regulación legal; observamos en este análisis la evidente contradicción sobre cómo es considerada la suplantación de identidad en un caso y en otro. Por su parte, disentimos en la denominación de los sujetos activos de la suplantación de identidad, pues en sentido estricto, no puede definirse como "delincuentes" a individuos que legalmente no comenten un delito; podría hablarse en todo caso de victimario, suplantador, *phisher, hacker* etc, pero bajo ningún punto de vista ser calificados como delincuentes, máxime si lo que se intentó justamente era regular típicamente a esta actividad, por no configurar un delito del derecho penal.

También fundamentan los legisladores que, independientemente de ser considerada la propuesta de tipificación de la suplantación de identidad digital, debe tenerse en cuenta la necesidad de contar con campañas de concientización a la sociedad sobre la existencia, riesgos y consecuencias de este tipo de delitos informáticos, afirmándose que como en muchos otros delitos, la mejor manera de evitarlos es la prevención, que debería ser a través de la enseñanza de un uso responsable y adecuado de las nuevas tecnologías.

Reflexionamos en este fundamento que lo determinante del proyecto era lograr la finalidad de tipificación de la suplantación de identidad para su sanción como delito penal. Reconociendo que sería necesaria la función de prevención y detección de delitos informáticos por el organismo al que le corresponda realizar esa tarea (aclarando que no se mencionan en el fundamento cuáles serían esos delitos), vislumbramos que dicha labor no era oportuna que sea incorporada como argumento o justificación, por ser ajena al objeto de este proyecto que es en suma el tratamiento del *phishing* para su legislación como delito.

Habiendo efectuado un estudio crítico a favor y en contra de los distintos fundamentos de los proyectos sobre suplantación de identidad aquí expuestos,

concluimos que todos fueron rechazados porque los legisladores erraron en cuanto a la falta de rigor en la utilización del lenguaje técnico-jurídico en su pretensión de aprobación de los mismos, tratando al *phishing* en algunos casos como un "delito", como un "robo" de identidad, como una "usurpación" de identidad, cuando ninguna de esas denominaciones es correcta, máxime si la conducta no estaba tipificada y el fundamento de cada ensayo apuntaba a la regulación legal de la suplantación de identidad como conducta delictiva.

2.4. Análisis doctrinario de la suplantación de identidad.

Los doctrinarios elegidos en esta oportunidad hacen un análisis detallado y exhaustivo en sus libros, sobre la problemática referida a la falta de regulación legislativa sobre la suplantación de identidad de la persona en la legislación penal vigente, apuntando a mostrar que aún después de la última reforma realizada, conductas como el *phishing* todavía no tienen una regulación típica específica. Así y en ese orden de ideas, se pueden mencionar los siguientes fundamentos aportados por el Dr. Pablo Andrés Palazzi que manifiesta:

> 1. El *phishing* es una modalidad defraudatoria que consiste en remitir un correo electrónico engañoso a clientes para que revelen información personal – tales como su número de tarjeta de crédito o débito o claves de cuentas bancarias – a través de sitios web simulados o en una respuesta de correo electrónico... Algunas veces el "pescador fraudulento" solicita encarecidamente a las víctimas que "confirmen" la información de cuenta que ha sido "robada" o esta "perdida". Otras veces el pescador fraudulento incita a las víctimas a que revelen información personal diciéndoles que han ganado un premio especial o que se merecen una jugosa recompensa *(Palazzi, 2.016, pp. 165-166).*

Reiteramos como en otro aporte realizado, que la suplantación de identidad, también denominada *phishing*, es un concepto informático y consiste en un ataque de ingeniera social que tiene por finalidad la adquisición de información confidencial de la víctima mediante el uso de ardid o engaño, utilizada para producir perjuicios patrimoniales y extrapatrimoniales. Habiendo realizado una conceptualización de la figura, aseveramos que la suplantación de identidad tiene su naturaleza y esencia propia y afirmar que se trata de una modalidad defraudatoria en sí, es una noción equivocada porque el fraude es una de las finalidades que pueden cometerse a partir de esta actividad y distinto a decir que sea *per se* una defraudación.

> 2. No se legisló por ejemplo sobre robo de identidad porque esa figura estaba cubierta en forma abarcativa por la estafa y la falsedad de documentos. Sin embargo queda más que claro que en materia de robo de identidad existe un enorme vacío de parte del Estado en prevención y educación de usuarios de *internet* y una real toma de conciencia de entidades financieras *(Palazzi, 2.016, p. 29).*

Si bien adherimos a la idea que no se legisló sobre el *phishing* en el Código Penal hasta la fecha, disentimos – como se puso de manifiesto – en que no se trata de un "robo" de identidad cuando lo que se pretende es la regulación legal de esta conducta. En todo caso hubiera sido más acertado referirse a esta temática como suplantación de identidad digital o suplantación de identidad de la persona, para evitar el yerro que configura denominar una conducta que estrictamente no es delito, con el uso de un tipo penal distinto como es el robo.

> 3. El robo de identidad no se limita a obtener créditos de baja monta en entidades financieras con documentos falsificados. Hay robo de identidad y de claves en forma masiva, a través de *phishing* o nombres de dominio falsos. Todo esto afecta la seguridad del comercio electrónico y la seguridad y la estabilidad de la infraestructura de *internet*. Es un delito que analizado globalmente supera claramente a la víctima individual del caso concreto *(Palazzi, 2.016, p. 29).*

Siendo un hecho el mal uso de la denominación del *phishing* porque venimos justificando que no configura estrictamente un delito, compartimos la opinión del autor en reconocer que el comercio electrónico que se maneja en *internet* no es infalible, es vulnerable y susceptible que la persona pueda sufrir consecuencias dañosas si es engañada en su buena fe por un *phisher*, porque una vez concretada la suplantación, es muy improbable reparar el daño causado a la víctima, ya que el suplantador tendrá el control de la situación y quedará en su voluntad qué decisión tomará luego de la obtención de la información confidencial.

> 4. La reciente reforma del art. 173 del Código Penal por la ley 25.390 hace referencia al "uso no autorizado de datos". Pero en doctrina se sostiene que el inc. 15 del art. 173, Cód. Penal, no puede ser aplicado al *phishing* (claro ejemplo de robo de identidad), porque la norma se refiere a datos insertos en plásticos bancarios obtenidos en forma ilegal *(Palazzi, 2.016, p 167).*

En este caso, coincidimos con el aporte del autor sobre la premisa que considera que no puede ser aplicado al *phishing* el tipo especial de estafa del art. 173 inc. 15 del C.P., pues el supuesto de hecho que prevé la norma en cuestión deja afuera

de su alcance a la suplantación de identidad y además porque la misma a nuestro entender es atípica; prueba de ellos son los intentos legislativos que pretendieron tipificarla, sin éxito hasta el momento.

Por su parte los Dres. Gabriel H. Tobares Catalá y Maximiliano J. Castro Argüello explican las perjudiciales consecuencias causadas mediante la suplantación de identidad, cuáles son las causas y qué técnicas de protección podrían utilizar los usuarios para protegerse ante los ataques de los *phisher*, lo que demuestra la necesidad de una legislación específica y concreta sobre la figura, expresando que:

> 1. Los daños causados por el *phishing* oscilan entre la pérdida de contraseñas de los correos electrónicos a pérdidas económicas sustanciales. Este estilo de robo de identidad se está haciendo más popular por la facilidad con que personas confiadas normalmente revelan información personal a los *phishers*, incluyendo números de tarjetas de crédito y números de la seguridad social. Una vez que esta información es adquirida, los *phishers* pueden usar datos personales para crear cuentas falsas en el nombre de la víctima, gastar el crédito de la víctima, o incluso impedir a las víctimas acceder a sus propias cuentas *(Tobares Catalá y Castro Argüello, 2.009, pp. 111-112).*

Dejando en claro la opinión fundada que estrictamente se trata de una suplantación de identidad y no de un "robo" de identidad, confirmamos las consecuencias perjudiciales que pueden ocasionar el *phishing* sobre el patrimonio de las personas víctimas de la misma y cuya "colaboración" es determinante para la producción del daño por los suplantadores. Agregamos también que pueden producirse daños extrapatrimoniales de diversa índole por medio de los datos personales adquiridos y la finalidad buscada por el *phisher*.

> 2. El estafador, mejor 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. Dado el creciente número de denuncias de incidentes relacionados con el mundo del *phishing* se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica, campañas para prevenir a los usuarios y con la aplicación de medidas técnicas a los programas *(Tobares Catalá y Castro Argüello, 2.009, p. 112).*

Consideramos que definir al *phisher* como un *estafador* sería afirmar que el *phishing* es una estafa, conclusión que no aceptamos por entender que a partir de esta conducta atípica pueden efectuarse una gama variada de finalidades entre las que pueden encontrarse la estafa o defraudación. No es lo mismo aseverar que el *phishing* es una estafa a decir que a través de aquella conducta pueda perpetrarse como objetivo una estafa o defraudación. Ello a partir de la afirmación de considerar a la

suplantación de identidad como una actividad que en sí misma no es delictiva y que merece ser tratada de manera autónoma y separada para su configuración típica.

Por otra parte Dres. Pablo Guillermo Lucero y Alejandro Andrés Kohen exponen sobre los vacíos legales existentes sobre la conducta denominada *phishing* indicando que a pesar de no existir una regulación típica específica, se ha incluido a la suplantación de identidad en la figura genérica de estafa o defraudación, dejando en evidencia la aplicación de analogía mediante el uso de un tipo delictivo distinto a esta actividad:

> 1. Finalmente, cabe destacar que todos los casos que no se puedan comprender dentro del inciso 15 del artículo 173 del Código Penal Argentino, serán atrapados por la descripción del inciso 16, ya que la manipulación de sistemas informáticos o transmisión de datos que se vincula con tarjetas de crédito, débito o de compras, será una modalidad defraudatoria propia del primer inciso mencionado, mientras que toda otra operación no vinculada con tales instrumentos encontrará su adecuación típica en el siguiente inciso *(Lucero y Kohen, 2.010, p.121).*

Cuestionamos a los autores por el hecho de pretender incorporar, dentro de los tipos especiales de estafa del art. 173 incs. 15 y 16 respectivamente, a una figura como el *phishing* que actualmente no tiene regulación legal, porque de ser así se estaría vulnerando la prohibición de analogía que rige en el derecho penal y además porque las fórmulas de los tipos penales a que se refiere el artículo e incisos supra mencionados, no contemplan en suma a la suplantación de identidad.

> 2. Es cierto que no quedan incluidos dentro de este supuesto los casos de ingeniería social, donde el autor, con cierta pericia y habilidad, logra que se le haga saber la clave de acceso a un sistema informático, ya sea telefónicamente o mediante "*phishing*"; sin embargo, estos casos quedan abarcados por la figura genérica de estafa prevista en el art. 172 del Código Penal Argentino, toda vez que aquí no hay manipulación informática destinada a alterar el sistema, sino un accionar sobre el punto más débil de la cadena de seguridad informática, que es el usuario final *(Lucero y Kohen, 2.010, pp.121-122).*

Rechazamos vehementemente la opinión de los autores en cuanto consideran que el *phishing* o casos de ingeniería social como se apunta, deban ser incluidos dentro del tipo penal de estafa genérica del art. 172 porque el hecho de no existir un tipo penal específico de suplantación de identidad, no es motivo suficiente ni valedero para intentar configurar ésta figura atípica dentro de un tipo penal como estafa que en la letra de su fórmula legal no atrapa a los casos de *phishing*.

Por su parte el Dr. Marcelo Alfredo Riquert exponiendo sobre defraudaciones con tarjetas de compra, de crédito y de débito y técnicas de manipulación informática reguladas en el art. 173 incs. 15 y 16 del Código Penal, expresa acerca de la falta de encuadre típico del *phishing* dentro de la actual legislación argentina, advirtiendo que el principio de legalidad de la represión prohibiría adecuar esta modalidad al tipo penal de estafa genérica o defraudación, manifestando que:

> 1…. En el marco del análisis del *phishing*, Toselli, Nicolosi y Chouela concluyen que, siendo que este tipo de maniobras apunta a la obtención de datos electrónicos, sean provenientes o no de tarjetas de esta clase, ya que en muchas ocasiones los estafadores informáticos apuntan a datos relacionados directamente con cuentas bancarias, claves de acceso al servicio de "*home banking*" o contraseñas, el principio de legalidad vedaría el encuadre de este orden de conductas en la previsión en comentario *(Riquert, 2.010, pp. 27-28).*

Con respecto al comentario del autor que antecede, adherimos y compartimos el análisis que manifiesta al considerar que los casos de *phishing* no se encuentran alcanzados por la descripción del tipo de estafa o defraudación genérica y que en consecuencia el principio penal de legalidad prohíbe el encuadre típico de la suplantación de identidad en la figura penal mencionada.

> 2. A todo evento, la interpretación a realizar tendrá como un norte insoslayable el "cerrar" los alcances del tipo, hacerlo aplicable a los casos en que el bien jurídico afectado sea el patrimonio. Puede rescatarse que varias de las conductas que habíamos señalado quedaban fuera del inc. 15, tienen ahora recepción en la nueva norma. *(Riquert, 2.010, p. 30).*

Ponemos a consideración que una cuestión es cerrar el alcance de un tipo delictivo que está regulado y que prevé la descripción abstracta del supuesto de hecho y otra diferente es crear o sancionar tipos delictivos destinados a contemplar conductas no reguladas legalmente, determinando con exactitud cuál es la conducta delictiva; estimamos que en ésta última situación se ubica la suplantación de identidad.

2.5. Jurisprudencia de distintos tribunales referida a la suplantación de identidad.

En esta oportunidad se mencionan distintos fallos de tribunales del país en los que afirmamos, se aplicó la analogía en los alcances del tipo en relación a la suplantación de identidad de la persona, habiendo sido encuadrada en algunos casos

en el tipo genérico de estafa o defraudación, mientras que en otros ha sido incluida dentro del tipo hurto.

Dejamos sentada nuestra postura que estima a la suplantación de identidad como una actividad ilícita pero atípica en rigor porque no es en sí un delito y consideramos que más allá de su falta de regulación legal, tiene su propia autonomía, particularidades, matices que requieren de su tipificación penal, sin perjuicio que a partir de esta figura puedan cometerse en sentido estricto conductas delictivas.

Aclaramos que los fallos que se describen *infra* atentan contra el principio penal de legalidad como garantía del debido proceso, receptado en el art. 18 de la C.N. y en los tratados con jerarquía constitucional del art. 75 inc. 22, ya que no existe en la legislación penal actual ningún tipo delictivo ni pena referido a la suplantación de identidad. Asimismo entendemos que los tribunales hayan sentenciado utilizando los tipos penales hurto y estafa en este caso, configura una clara vulneración de la prohibición de analogía que rige en materia penal, máxime cuando es aplicada en perjuicio del imputado.

Por el encuadramiento de la suplantación de identidad en el tipo penal de estafa o defraudación se inclinaron:

- CNC Penal. Sala VII. "Castellini, Alfredo J. y otros". (Sentencia de fecha: 30/03/2005), considera como delito de estafa la tenencia de instrumentos destinados a la falsificación de tarjetas de créditos, aun cuando no se haya acreditado la existencia de movimientos no autorizados en las cuentas individualizadas, considerándose un delito en concurso material de tentativa de defraudación, dado que con los datos obtenidos se crean tarjetas de créditos falsas.
- CNC Penal. Sala IV. "T., C. R. y otro". (Sentencia de fecha: 02/07/2.007). entiende que constituye delito de estafa los fraudes del vendedor en mercados virtuales, en el cual existe dolo *ab initio* cuando la actividad del estafador estaba destinada a sacar un pago a un consumidor sin la intención de enviarle el bien o producto concreto.
- CNA Comercial. Sala D. "Bieniauskas, Carlos c/ Banco de la Ciudad de Buenos Aires". (Sentencia de fecha: 15/05/2.008) fundamenta que la estafa se configuró cuando los sujetos activos estafaron a la víctima utilizando los datos de su

tarjeta de crédito en el que el *modus operandi*[44] fue llamarlo haciéndose pasar por representantes de auditoría de una tarjeta, le dijeron que con su tarjeta de débito se estaba realizando una compra en un determinado local, haciéndole creer que otra persona estaba usando su tarjeta. Aceptado el hecho por el damnificado, llamó a un 0800 en el que se le pidió el nombre completo, D.N.I., y que ingresara su PIN si tenía teléfono por tonos, configurándose en ese momento la estafa, ya que era posible con esos datos hacer luego transferencias bancarias. Todas estas razones, fueron las que determinaron que la Cámara Comercial condenara al Banco a pagar los daños ocasionados en esos supuestos, haciéndolo responsable con fundamento en la obligación de seguridad.

- CNA Criminal y Correccional. Sala VI. "G.R. y otro s/ procesamiento". (Fallo de fecha: 03/08/2.010), confirma el procesamiento de dos personas imputadas por fraude, a raíz del uso de la técnica de manipulación informática conocida como "*phishing*", imputándoseles a los acusados haber llevado a cabo maniobras de fraude, mediante la creación de una página paralela, por la cual obtuvieron los datos necesarios (código de transferencia y número de tarjeta de crédito) para poder operar en las cuentas bancarias de la víctima efectuando transferencias dinerarias desde la caja de ahorro y cuenta corriente de ésta a otra caja de ahorro, todas de la misma entidad bancaria, sin el consentimiento del titular de esas cuentas.

- CFC Penal. Sala III. "C.P.A. s/ Recurso de Casación". (Sentencia de fecha 16/06/2.015), resuelve que corresponde condenar al imputado como autor penalmente responsable del delito de defraudación mediante técnicas de manipulación informática, pues se acreditó que a través de la manipulación indebida de datos informáticos obtuvo el usuario y contraseña del *home banking* del denunciante y efectuó la transferencia de una suma de dinero desde la cuenta bancaria de éste a la de un tercero que cobró el dinero y se lo entregó al encartado, y si bien éste refirió que tal suma de dinero se debía al pago de un trabajo que había realizado en forma *freelance*[45], no se logró ubicar al supuesto cliente, que se hubiera puesto en contacto con él, ni la realización del presunto trabajo encargado.

[44] *Modus operandi* es una expresión en latín que refiere al modo de obrar de una persona o conjunto de personas.
[45] *Freelance* es la actividad que realiza la persona que trabaja de forma independiente o autónoma que le permite desenvolverse en su profesión o en aquellas áreas que pueden ser más lucrativas y que están orientadas a terceros que requieren de servicios específicos.

Por el encuadramiento de la suplantación de identidad dentro del tipo hurto se inclinaron:

- CNC Penal. Sala II. "Coronel, Orlando". (Sentencia de fecha: 05/10/2.004).
- CN Criminal y Correccional. Sala III. "Iglesias, Carlos M.". (Sentencia de fecha: 04/06/1.992).
- SCJ Mza. Sala II. "Fiscal c. Russo Beraldo". (Sentencia de fecha: 19/08/1.997).

En los fallos mencionados que tienen similares razones fundadas, se sostuvo que en aquellos supuestos de manipulaciones de una máquina automática – tal el sistema informático de un banco – para obtener un artículo o dinero, no puede decirse que dicha manipulación constituya el delito de estafa porque de esa manera no puede lograrse una mente errada y sin la presencia del error – elemento fundamental del tipo objetivo – no habrá estafa sino hurto.

- C Criminal y Correccional Nº 24. "M. s/ Hurto". (Sentencia de fecha: 19/07/1.995), expresa que constituye delito de hurto el caso de una empleada bancaria que mediante la alteración del número de cuenta de su propia tarjeta Banelco y sustituyéndolo por el de otra persona clienta del banco, logra efectuar una extracción de dinero a su favor fundamentando el tribunal que tal situación es así dado que no se provocó error en persona alguna que llevara a una disposición patrimonial perjudicial. Lo que hizo M. fue que, utilizando sus conocimientos y aprovechándose de las funciones que cumplía en la entidad bancaria y de la confianza en ella depositada, alteró el sistema informático de modo tal que pudo sustraer de un cajero automático la suma de quinientos pesos de la que consecuentemente desapoderó a su empleadora, lo cual no resulta atípico sino que encuentra adecuación a la figura del hurto.

2.6. Necesidad de adecuación de la suplantación de identidad en la teoría del delito para su configuración como conducta delictiva.

2.6.1. De la teoría del delito.

Iniciando el presente apartado y a los fines de intentar configurar a la suplantación de identidad de la persona como una conducta delictiva, se aclara que la intención es efectuar solamente un análisis teórico al respecto y por ello se torna

preciso definir al delito como aquella acción (en sentido amplio), típica, antijurídica y culpable; de esta definición surgen los elementos o estadios que integran la teoría del delito, a saber: la acción, el tipo penal, la antijuridicidad y la culpabilidad, que serán abordados oportunamente. Lo determinante es analizar y establecer si se presentan de manera gradual, concatenada y secuencial, todos y cada uno de estos elementos, caso en el que la conducta será considerada delito. Si faltase alguno de estos elementos, irremediablemente no deberá configurar una conducta delictiva.

Al momento de determinar que es delito, la función de la norma penal es describir determinadas conductas que son individualizadas y luego son desvaloradas doblemente porque por un lado existe una desvaloración de la conducta y por otro hay una desvaloración de su autor en su circunstancia, que es una característica de esa conducta. Esos juicios proviene de la propia ley y la persona solo se limita a verificar su existencia (Zaffaroni, 1.981).

Lo que se intenta a partir de la aproximación general acerca de la teoría del delito, que es entendida como acción típica, antijurídica y culpable, que funciona como un sistema de filtros y permite abrir sucesivos interrogantes acerca de una respuesta habilitante del poder punitivo por parte de las agencias jurídicas, es que constituye la más sobresaliente función del derecho penal con relación a ese poder represivo y que se encuentra plasmado en las diferentes leyes penales (Zaffaroni, 2.002).

Es por esta razón que la elaboración de la dogmática-jurídica alcanzó en este punto su máxima expresión, tal vez en algunas ocasiones sobredimensionado con relación al resto del derecho penal. Tomando este fenómeno en su modalidad actual, tiene su origen en el siglo XIX, con autores (v.g. Binding y Merkel) que presuponían la existencia de un estado racional y que no se planteaban la subsistencia del estado de policía bajo múltiples carátulas, dedicando sus esfuerzos a la perfección de los elementos de operatividad de un poder que consideraban sustancialmente racional (Zaffaroni, 2.002).

Fue favorable para la teoría del delito, el desarrollo de la función pragmática, consistente en lograr dilucidar de un modo razonable aquellos caracteres que ofrecieran un paradigma de análisis que facilite la enseñanza del derecho por docentes y profesores de las universidades y sirva de ayuda a los jueces en su tarea de

resolución de casos. Ello potenció de manera significativa el desarrollo teórico del delito porque cobró importancia el hecho de encomendar la tarea a agencias burocratizadas y verticalizadas, a las que sólo se podía acceder luego de un gran entrenamiento académico (Zaffaroni, 2.002).

Esboza Zaffaroni (2.002) que el privilegio de la función pragmática de la teoría del delito favoreció lo que se conoce como sistemas clasificatorios, que se centraban en distinguir y combinar caracteres y elementos, sin derivar la sistemática de una teoría de la pena o del derecho penal a la que fuese funcional, llegando a mantener una mera teoría preventiva y/o disuasiva de la pena, con el fin de sostener la función motivadora de las normas y construir un discurso jurídico penal que le asigne al poder punitivo una supuesta función tutelar que lo legitime.

2.6.2. De la acción.

Con respecto a este primer carácter de la teoría del delito, ha evolucionado de manera gradual dentro de la ciencia del derecho penal del siglo XIX. Es Hegel quien realiza la formulación del primer concepto jurídico-penal de la acción (Lascano[h], Piñero, Balcarce, Agostinetti y Bonetto, 2005).

Enseñan que el concepto de acción ha tenido las más variadas denominaciones dependiendo de la concepción sobre la misma. En ese sentido, pueden citarse las siguientes corrientes dogmáticas:

- ✓ Concepción causal de la acción: tiene una visión mecanicista de la acción y sus principales fuentes cognoscitivas son:

a) El positivismo jurídico o sistema clásico, cuyos máximos exponentes fueron Von Liszt, Beling y Radbruch. Conciben a la acción como aquella conducta o actividad voluntaria realizada por el agente, que causa un cambio en el mundo exterior. De ello surge que sus elementos son: 1) la manifestación de la voluntad – entendida como toda conducta comisiva u omisiva, libre de coacción física o psíquica – y 2) el resultado, que consiste básicamente en una transformación del mundo exterior y que se produce por aquella manifestación de voluntad – tratándose de una actividad – o bien puede referirse a la no mutación del ambiente ante la falta de acción que se espera. En pocas palabras, la acción comprende tanto el hacer como el no hacer (Lascano [h] et. al., 2.005).

b) Normativismo neokantiano o sistema neoclásico, tiene su origen en el siglo XX, bajo la influencia del pensamiento filosófico de la escuela sudoccidental alemana. La acción se convierte en un concepto que posee una valoración, dejando de ser sólo un concepto natural. El principal exponente de esta corriente es Mezger que afirma que la acción es toda conducta humana valorizada de una determinada manera. También incluye en su contenido la actividad y la omisión. Aquel autor aclara que la valoración del contenido de la voluntad del sujeto se difiere para el estadio de la culpabilidad, por lo que sostiene que el concepto de acción es estructurado y construido como un concepto natural. Es por ello que, más allá de esta referencia valorativa, afirma el concepto natural de la acción (Lascano [h] et. al., 2.005).

- ✓ Concepción finalista de la acción: surge a comienzos de la década de 1.930 con la obra desarrollada por Welzel, teniendo su origen filosófico en Aristóteles. Este autor niega la concepción natural o mecanicista de la acción – perteneciente al causalismo – afirmando que el concepto de la acción en el ámbito del derecho penal es un concepto ontológico, que proviene del ser y es preexistente a toda valoración. Expresa Welzel que acción humana es ejercicio de actividad final. Esboza que la finalidad comienza con el saber causal que tiene el hombre, pudiendo prever dentro de ciertos parámetros, aquellas consecuencias probables de la actividad desplegada; es decir que puede plantearse distintos fines y dirigir su conducta conforme un plan estratégico que esté destinado a esos fines propuestos. Esta corriente doctrinaria entiende que la acción comprende dos etapas; la primera se produce en la faz interna del pensamiento del individuo, comprendiendo lo que es el fin perseguido por el autor, los medios a emplear y la representación de los efectos concomitantes. En la segunda etapa – de realización exterior –, el autor pone en marcha, conforme el plan ideado, aquellos medios de acción seleccionados con anterioridad y que están dirigidos a la concreción del resultado esperado (Lascano [h] et. al., 2.005).
- ✓ Esquemas funcionalistas: esta corriente se desarrolla en la década de 1.970, dándole prevalencia a las consideraciones teleológicas-normativas respecto del delito. Pueden mencionarse como posturas destacadas:

a) Funcionalismo moderado de Roxin, quien caracteriza a la acción como manifestación de la personalidad. Entiende que sólo pueden ser consideradas acciones las conductas exteriores del autor, excluyendo de esa forma su faz interna.

Por otra parte considera que el concepto de la acción es un supraconcepto que incluye a todas las manifestaciones de la conducta delictiva como son las acciones doloras e imprudentes, como así también las omisiones. A su vez, opera como elemento de enlace porque permite vincular a todas las correspondientes categorías del delito. Finalmente la manifestación de la personalidad determina cual es el criterio decisivo para delimitar la acción y la falta de acción (Lascano [h] et. al., 2.005).

b) Funcionalismo radical y sociológico de Jakobs, quien considera que la acción debe ser concebida como expresión de sentido. Dicho concepto permite establecer que la acción consiste en la causación individualmente dolosa o imprudente de la persona, de determinadas consecuencias, las que no se producirán si existirá una motivación dominante que esté dirigida a evitarlas.

La mencionada expresión de sentido jurídico-penalmente relevante de una acción considerada injusta, toma protagonismo frente al concepto de vigencia de la norma, cuyo autor no le reconoce autoridad. Esa falta de reconocimiento constituye el resultado jurídico-penal específico y que en definitiva lo reprochable es la actitud del sujeto ante la vigencia de la norma, que se pone de manifiesto en la ejecución de la acción delictiva (Lascano [h] et. al., 2.005).

A pesar de los diferentes conceptos y posturas de la dogmática jurídico-penal, existen características que identifican el concepto de la acción. Así se pueden mencionar:

- Exterioridad: las conductas alcanzadas por el derecho penal son sólo aquellas que se manifiesta en el ámbito exterior y que trascienden la faz interna del sujeto, dado que es la única manera de poner en peligro o lesionar aquellos bienes dignos de tutela jurídica.
- Sujetos de la acción: son considerados únicamente sujetos activos del derecho penal a las personas físicas, porque sólo a ellas puede imputárseles la comisión de un hecho delictivo.
- Formas de conducta: el término conducta es utilizado en sentido amplio y puede presentarse mediante dos modalidades, a saber: a) mediante la forma de acción en sentido estricto, que se refiere a la actividad desplegada por la persona que transgrede lo vedado por una norma prohibitiva; b) mediante una omisión o abstención que se produce en el momento de una inactividad que es violatoria de una norma prescriptiva, es decir que se trata de una norma que ejerce un mandato y su deber de realización (Lascano [h] et. al., 2.005).

Por su parte Nuñez (1.999) explica la existencia de una concepción causal, finalista y social de la acción. En relación a la concepción causal, esboza que se trata de una concepción mecanicista de la acción humana, cuya idea es compartida por corrientes como el normativismo de Mezger y el positivismo jurídico de Liszt, Beling y Radbruch. Se trata de una función que es exclusivamente causal de la voluntad con relación al movimiento exterior efectuado por el agente, desvinculando el contenido de esa voluntariedad, ya que en esta teoría no se analiza la finalidad de aquella conducta.

La acción es definida como todo movimiento corporal que se produce con un acto voluntario, entendido éste como aquél libre de todo tipo de coacción.

Para la concepción finalista, la acción es considerada como un acontecer final y la voluntad cumple una función directriz hacia la consecución de fines que han sido previamente observados por el autor, como así también en lo referido a la elección y aplicación por éste de aquellos medios que son aptos para su logro. En ese orden de ideas, Maurach define que la acción es actividad final humana, que el autor divisa la finalidad antes que el medio a elegir, que dicha acción se caracteriza por la anticipación del fin en el pensamiento del sujeto, quien dirige todo los medios de los que dispone al momento de la consecución de la meta (Nuñez, 1.999).

Finalmente y con respecto a la última concepción, Nuñez (1.999) manifiesta que aquella idea que no es factible someter la acción y la omisión a un concepto común, fue superada por la concepción social de la acción, la que tiene un criterio valorativo superior que va más allá del hacer o el no hacer.

Este criterio valorativo, que parte de la consideración de la conducta humana frente a la sociedad, condujo a la noción de la acción como la realización de un resultado socialmente relevante, que desde el punto de vista jurídico-penal, se traduce en la producción de un resultado típico. Esta conducta socialmente relevante puede consistir: a) a una actividad finalista, b) en la causación de consecuencias dominables por el autor y c) en una inactividad frente a una acción esperada (Nuñez, 1.999, p. 119).

2.6.3. De la tipicidad.

Avanzando en el segundo elemento de la teoría del delito, es oportuno analizar la tipicidad, la que es conceptualizada como la descripción abstracta de la conducta

prohibida por la norma sancionada por el legislador. El tipo es equivalente al supuesto de hecho utilizando este esquema: el que haga esto o el que no haga esto. Tomando el ejemplo concreto del art. 79 del C.P.[46], la fórmula empleada por la ley para el supuesto de hecho es el que matare a otro (Lascano[h] et. al., 2.005).

La tipicidad es el resultado de un juicio u operación mental llevada a cabo por el intérprete o juez, que permite determinar que la conducta objeto de examen coincide con la descripción abstracta contenida en la ley penal. Por el contrario, si realizado dicho procesamiento surge que el resultado es negativo porque el comportamiento en cuestión no se adecua al respectivo tipo penal, se dirá que estamos en presencia de la atipicidad (Lascano [h], et. al., 2.005, p. 262).

Por otra parte y con respecto a la función garantizadora del tipo, ella se deriva del principio de legalidad – *nullum crimen sine lege*[47] –, el que asegura que solamente aquellas conductas descriptas previamente por la ley penal, serán merecedoras de pena. Es necesario frente a ello que el legislador utilice de manera precisa y adecuada el uso del lenguaje utilizado al momento de redactar la ley penal, cuáles son las conductas incriminatorias específicas y cuáles son los bienes jurídicos afectados (Lascano [h], et. al., 2.005).

En relación a las funciones del tipo delictivo, se pueden mencionar las siguientes, a saber:

a) Incidiaria: La doctrina mayoritaria entiende que el tipo penal es la *ratio cognoscendi*[48] de la antijuridicidad, sosteniendo que pueden encontrarse conductas típicas que no son antijurídicas porque en el caso particular puede estar presente alguna causa de justificación[49], que determina que ese comportamiento típico esté permitido por la ley penal.

b) Vinculante: El delito-tipo tenía el significado de un esquema regulador, tomando el ejemplo del homicidio y analizando la antijuridicidad, era necesario advertir que no se trataba de cualquier tipo de antijuridicidad sino aquella que se correspondiera con aquel delito-tipo. El mismo era un concepto determinante que

[46] Código Penal de la Nación Argentina – Ley Nº 11.179.
[47] *Nullum crimen sine lege* es una expresión en latín que significa que no hay delito ni pena sin una ley penal previa que lo determine.
[48] *Ratio cognoscendi* se refiere que el tipo es el indicio cognoscitivo de la antijuridicidad.
[49] Las causas de justificación son situaciones de hecho y de derecho cuyo efecto es excluir la antijuridicidad de un hecho típico.

tenía el dominio en extensión y profundidad del derecho penal. Asimismo la obligatoriedad corresponde para el caso de las formas delictivas accesorias como son la tentativa y la participación criminal, en las que resulta inescindibles el concepto tipificante (Lascano [h], et. al., 2.005).

c) Didáctica: El tipo exige que los destinatarios de la norma penal deben tener la oportunidad – antes de la comisión de la conducta – de poder conocer si ella es prohibida o no y si hay amenaza sobre la imposición de una pena. Es así que podrán deliberar en su conciencia sobre esta exigencia de la ley y a ser motivados para respectar aquellos bienes jurídicamente protegidos en cada caso. Expresado de otro modo, la función didáctica está dirigida a todos los individuos para disuadirlos de la realización del comportamiento prohibido por la norma penal.

d) Limitadora: Cuando el legislador tiene la tarea de sancionar una ley penal, selecciona de entre un conjuntos de conductas antijurídicas – utilizando un criterio de mínima intervención – aquellas conductas que atentan más gravemente a los bienes jurídicos importantes, aplicándoles la imposición de una pena. Por su parte, los hechos típicos son comportamientos penalmente relevantes, que presuponen la vulneración o puesta en peligro de un bien jurídicamente valioso para el sistema penal y que debe imputarse a un comportamiento que es previamente disvalioso (Lascano [h], et. al., 2.005).

Lascano [h] et. al. (2.005) explica que el tipo penal es una construcción compleja que se efectúa mediante la descripción objetiva-subjetiva de la conducta. Así habla de un tipo complejo conformado por un tipo penal objetivo y un tipo penal subjetivo. Con relación al primero, enseña que comprende el aspecto externo del comportamiento humano prohibido por la norma, que abarca no solo la descripción abstracta sino también las distintas valoraciones del sujeto. El tipo objetivo presenta elementos también objetivos cuyo núcleo está constituido por la acción descripta por el verbo (v.g. matar, robar, estafar etc.). Además se encuentran distintas circunstancias como su relación con otras personas, cosas, la vinculación con el tiempo y espacio y el modo de ejecución de las acciones.

El tipo subjetivo tiene en miras la actitud subjetiva de su autor con relación al bien jurídico tutelado y cómo dirige su voluntad. Así existen dos clases de este tipo:

a) Tipos dolosos, en el que el autor es plenamente consciente que con su actuar se lesiona un bien jurídico digno de tutela y a sabiendas quiere afectarlo. En estos tipos el sujeto infringe una norma prohibitiva.

b) Tipos culposos, en los que el agente no pretende la lesión del bien jurídicamente protegido, pero que igualmente su conducta desaprensiva produce la afectación. En estos tipos el sujeto infringe una norma de cuidado (Lascano [h], et. al., 2.005).

2.6.4. De la antijuridicidad.

Avanzando en la teoría del delito, corresponde analizar el tercer carácter, la antijuridicidad, que dando una noción general, se utiliza para designar aquella característica del supuesto de hecho concreto que se torna contradictorio con el ordenamiento jurídico en general y específicamente con las normas jurídico-penales (Lascano [h] et. al., 2.005).

Lascano [h] et. al. (2.005) menciona como característica destacada del supuesto de hecho abstracto, que la antijuridicidad general – consistente en la contradicción con el derecho –, ya viene afirmada por la comprobación de la tipicidad; mientras que la antijuridicidad específica – consistente en la contradicción con la ley penal –, implica la verificación de si ese supuesto de hecho es merecedor de una pena.

No se puede saber con exactitud qué doctrinario fue quien utilizó por primera vez el término antijuridicidad. Sin embargo, el concepto de antijuridicidad objetiva fue incorporado a la estructura de la teoría del delito gracias a los aportes de Von Liszt y Beling. A su vez Binding separó del derecho penal el vocablo antijuridicidad como una categoría autónoma dentro de la teoría de las normas.

En la doctrina existen dos posiciones divergentes con respecto al concepto dado sobre antijuridicidad:

a) Para algunos autores la antijuridicidad es la contradicción del ámbito exterior del hecho acontecido con el ordenamiento jurídico (antijuridicidad objetiva).

b) Para otros, la antijuridicidad es la intención contraria a la norma de determinación dirigida al individuo, manifestada a través del hecho externo (antijuridicidad subjetiva) (Lascano [h] et. al., 2.005, p. 380).

La distinción de los conceptos antijuridicidad formal y material tiene su génesis en Von Liszt. Actualmente el concepto de antijuridicidad formal se refiere al vínculo existente entre la acción u omisión y la norma penal de determinación; esta acción u omisión en abstracto es formalmente antijurídica en la medida que vulnera una prohibición o un mandato de la norma penal; la antijuridicidad material hace referencia a la contradicción con la norma de valoración en el ámbito que ésta exceda la norma de determinación, es decir haciendo hincapié en el contenido disvalioso. La mencionada acción u omisión es materialmente antijurídica cuando ella produce una lesión de bienes jurídicos, que es socialmente dañosa y los medios extrapenales existentes son insuficientes (Lascano [h] et. al., 2.005).

Por otra parte, Nuñez (1.999) enseña que la antijuridicidad "*es la calidad del hecho que determina su oposición al orden establecido por el derecho*" (Nuñez, 1.999, p. 153).

La tipicidad de la conducta es un indicio de la antijuridicidad, la que se excluye en el caso de la concurrencia de una causa de justificación. En otras palabras, no debe concurrir una causa de justificación para que la conducta pueda ser encuadrada como antijurídica (Nuñez, 1.999).

2.6.5. De la culpabilidad.

Analizando el cuarto y último carácter de la teoría del delito, es oportuno señalar que en la actualidad – desde el punto de vista jurídico-penal –, el vocablo culpabilidad posee dos acepciones, a saber:

a) Se refiere al significado de una garantía individual del sujeto; así se habla de un principio de culpabilidad, que se aloja dentro de aquellos postulados esenciales a todo Estado de derecho, que vienen a operar como límites a la potestad represiva y que a su vez se traduce en las condiciones necesarias tanto para la imputación de responsabilidad penal como para la imposición de una pena. Siendo admitida la culpabilidad como condición *sine qua non* de la pena, la ley penal le reconoce al delincuente la categoría de persona, es decir un ser que es capaz de autodeterminarse

al momento no solo de realizar la conducta lesiva sino también en su actitud espiritual que lo empuja a comportarse de esa manera (Lascano [h] et. al., 2.005).

Las consecuencias más importantes que surgen del principio de culpabilidad son la responsabilidad siempre por el hecho propio – es inadmisible la responsabilidad por la conducta de terceros –, la responsabilidad penal de acto – la conducta objetivamente realizada por el agente – y la responsabilidad penal subjetiva, que exige que dicha conducta pueda serle "imputable" al sujeto que la realiza, es decir que tenga la posibilidad y la aptitud de conocer que con su comportamiento está infringiendo la norma penal.

b) Está referida a la culpabilidad como una categoría o como un elemento constitutivo de la teoría del delito, que es conceptualizada como la actitud anímica y jurídicamente reprochable del agente productor de un hecho penalmente típico y antijurídico – según la concepción normativa – o bien puede ser considerada como puro juicio de reproche hacia el autor – conforme lo afirma la concepción finalista – (Lascano [h] et. al., 2.005).

Existen dos condiciones necesarias para la configuración de la culpabilidad del autor de una conducta típica y antijurídica:

- ✓ La infracción personal de una norma primaria penal, cuyo imperativo es dirigido en concreto al sujeto y requiere de: 1) la capacidad personal de evitar la conducta objetivamente desvalorada y 2) la posibilidad de conocimiento de la antijuridicidad.
- ✓ La responsabilidad penal del sujeto, que determina que la infracción personal del agente hacia la norma primaria, permite imputarle la antijuridicidad penal, pero es un requisito necesario para la aplicación de una pena, que el sujeto sea idóneo y se encuentre en condiciones de normalidad motivacional para responder penalmente (Lascano [h] et. al., 2.005).

Por otra parte, el C.P. en su art. 34 inc. 1º, consagra para determinar la imputabilidad del agente, un sistema mixto conformado por presupuestos biológicos – psicológicos. En ese sentido, los presupuestos biológicos son:

1) La madurez mental, por medio del art. 1 de la ley Nº 22.803[50] se establece en la edad de dieciséis (16) años, siendo considerada una presunción *juris et de jure*[51].

2) La salud mental, partiendo de la fórmula empleada por el C.P. en su art. 34 inc. 1º, el sujeto activo del delito goza de salud mental si no está afectado de una "insuficiencia de sus facultades" o por una "alteración morbosa de las mismas"; las facultades referidas son mentales.

3) Conciencia, referida a la conciencia "perceptiva o lúcida", que consiste en el claro o nítido conocimiento de los acontecimientos internos y externos de la psiquis del sujeto, que le permite percibir correctamente, estar orientado en el espacio y tiempo, respondiendo adecuadamente a los estímulos ambientales, los que pueden ser evocados cronológicamente (Lascano [h] et. al., 2.005).

A su vez, los presupuestos psicológicos son los siguientes, a saber:

1) Capacidad de comprensión de la criminalidad del acto, es uno de los requisitos exigidos por la norma penal para caracterizar aquel efecto psicológico. Requiere que la norma primaria pueda ser recibida por su destinatario y que tenga la posibilidad de ser motivado por ella, para que de esa manera le pueda ser atribuido el injusto penal.

2) Posibilidad de dirección de la conducta, requiere que el agente tenga la posibilidad de actuar de otro modo, de poder elegir entre violar o no la norma primaria y que en el eventual caso de vulnerarla será por su propia deliberación, debiendo aplicarse la sanción penal que corresponda (Lascano [h] et. al., 2.005).

2.7. Conclusiones parciales.

Luego de analizado el presente capítulo, aseveramos que desde la sanción de la ley de delitos informáticos Nº 26.388 del año 2.008 en Argentina y observando los tipos penales y las sanciones que prescribe la ley en todo su articulado, no surge ninguna figura o tipo penal – mucho menos una pena – de la suplantación de identidad de la persona. Prueba de ello y ante la falta de tipificación es que en el año 2.010, 2.011 y 2.012 respectivamente los legisladores que han sido mencionados supra presentaron sus respectivos proyectos de ley intentando que se legisle sobre

[50] Ley Nº 22.803 sobre elevación de la edad mínima de punibilidad respecto de menores que cometieron delitos.
[51] Presunción *juris et de jure* es una locución en latín que significa que la presunción de derecho no admite prueba en contrario.

phishing como delito integrante de la ley penal, no habiendo sido receptados en la legislación argentina por aquel entonces y cuestión que hasta la fecha se insiste que no se encuentra regulada legalmente en un tipo ni en una pena; en un mismo sentido, la jurisprudencia que ha sido citada demuestra que al momento de intentar encuadrar la conducta en un tipo penal del código de rito, no consiguen tal cometido atento a lo que se viene reiterando, que no existe tipo penal en donde se encuadre a la suplantación de identidad. Es por ello que los jueces sentenciaron los casos mediante la utilización de otros tipos penales como la estafa o el hurto, configurando ello aplicación de analogía en materia penal, que se encuentra prohibida en nuestro derecho.

Por otro lado, a los fines de su estudio académico, explicamos brevemente acerca de los elementos o presupuestos necesarios para que la suplantación de identidad bajo el análisis de la teoría del delito, pueda ser considerada como conducta delictiva. En concreto, afirmamos la necesidad de realizar una reforma penal a la actual ley de delitos informáticos (de escasa o insuficiente regulación en materia de figuras que emplean sistemas informáticos y tecnologías digitales) que expresamente indique cuál es el tipo mediante su respectiva fórmula que encuadre al *phishing* con la pena correspondiente. A modo de ejemplo podría utilizarse la siguiente fórmula: "se aplicará pena de prisión de dos a cinco años, al que suplantare la identidad de una persona física o jurídica mediante ardid o engaño, con el fin de obtener información confidencial, datos personales que afectaren el ámbito patrimonial o extrapatrimonial de la víctima". Más allá de la mejora en la técnica legislativa que pudiere hacerse, el punto de inicio de la conducta a regular es el tipo delictivo que permitirá analizar los siguientes elementos de la teoría del delito – antijuridicidad y culpabilidad –, en miras a regular jurídicamente la figura bajo estudio.

CAPITULO III: PRINCIPIO DE LEGALIDAD Y PROHIBICION EN LA APLICACIÓN DE ANALOGIA A LA SUPLANTACION DE IDENTIDAD.

3.1. Introducción.

Comenzando con una breve introducción de este capítulo, es oportuno manifestar que en el ámbito de lo que se denomina derecho penal constitucional en los actuales sistemas jurídicos de los estados de derecho, la Constitución se presenta

como el marco normativo insoslayable, regulador y limitador de ese sistema de control social conocido como sistema penal. En cuanto a nuestro país, a partir de la reforma del año 1.994, la doctrina y jurisprudencia inician la construcción de un modelo constitucional penal, entendido como un sistema interpretativo y explicativo que actúa como mediador entre la realidad y el pensamiento.

El fundamento del principio de legalidad en el castigo de una conducta sólo puede ser mediante una ley en sentido formal sancionada según el procedimiento, la competencia y el contenido limitado que regula nuestra Constitución Nacional, que esté vigente al momento de la comisión del hecho y que prevea como delictiva la conducta reprochada. Se trata de una garantía sustantiva que delimita el poder punitivo del Estado en todo su alcance. Es una garantía criminal, ya que exige que el hecho perseguido penalmente esté contemplado como delito, previamente, por una ley; es una garantía penal, dado que esos mismos recaudos no sólo tienen que tomarse respecto de la descripción de la conducta, sino también para el monto de la pena; es una garantía jurisdiccional, porque exige que la existencia de un delito y la imposición de una pena deriven de un pronunciamiento judicial; y es también una garantía de ejecución , ya que exige que el cumplimiento de la pena esté regulado por una ley.

Dentro del derecho penal argentino, la regla general es que está prohibida la aplicación de analogía como fuente de conocimiento pues ello contradice los arts. 1, 18 y 19 de la carta magna. Así es que si el hecho objeto bajo análisis no se encuentra contemplado concretamente en la ley criminal, no podrá aplicársele una norma ni pena que castigue un hecho similar. En ese sentido si analizamos el ejemplo del tipo hurto con la suplantación de identidad de la persona que no se encuentra regulada en un tipo penal, no podría (ni debería) aplicarse por analogía la pena de hurto al que realiza tal suplantación por la falta de encuadre jurídico y a su vez se configuraría la vulneración del mencionado principio penal de legalidad. Sólo eventualmente y en casos excepcionales podrá aplicarse la analogía cuando sea en beneficio o a favor de procesado o reo, dado el carácter protectorio y garantista del actual sistema penal; como consecuencia de ello, si hipotéticamente la intención del juzgador es la aplicación de analogía en detrimento o perjuicio del imputado en un caso concreto, ergo se produciría la violación de prohibición de analogía *in malam partem* que rige en el derecho criminal.

3.2. Principio de legalidad en el art. 18 de la Constitución Nacional.

En coherencia con lo que fue expuesto en anteriores capítulos, con relación a los antecedentes doctrinarios, legislativos y jurisprudenciales, afirmamos que la suplantación de identidad constituye una conducta atípica por la falta de tipo y sanción penal y que la misma no se encuentra regulada penalmente a la fecha; haciendo hincapié en los casos que fueron mencionados en su oportunidad, entendemos que surge de las sentencias dictadas por los jueces – en la utilización de otras fórmulas típicas y penas como las que corresponden al hurto o estafa – , la indefectible vulneración del principio penal de legalidad.

A partir de ésta afirmación y pretendiendo resaltar el respeto como el efectivo cumplimiento del citado principio penal en el sistema constitucional, es que se torna necesario efectuar un estudio pormenorizado sobre el principio de legalidad de la represión, que está vinculado a la función de garantía que tiene la ley penal frente al poder punitivo del Estado. Dicho principio – en su aspecto formal – con el aforismo *nullum crimen, nulla poena sine lege* (cuya formulación se atribuye a Feuerbach), consagra a la ley penal previa como la única fuente del derecho penal. En cuanto a su aspecto material, implica que el contenido de dicha norma debe adecuarse a los límites constitucionales descriptos con anterioridad (Lascano [h] et. al., 2.005).

Como antecedentes se puede mencionar que el principio de legalidad fue receptado como garantía limitadora de la norma penal en el Derecho Constitucional Estadounidense – a través de la declaración de independencia de 1.776 – y en el Derecho Constitucional Francés – por medio de la Declaración de los Derechos del Hombre y del Ciudadano de la Revolución Francesa de 1.789 – (Lascano [h] et. al., 2.005).

En nuestro país se encuentra inmerso de manera expresa como garantía del debido proceso penal en el art. 18 de la C.N. que reza: "*ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso…*".

Sobre los aspectos a desarrollar, el principio de legalidad es considerado como:

a) Una garantía criminal, que requiere que el delito (equivalente a crimen), se encuentre determinado por la ley (*nullum crimen sine lege*).

b) Una garantía penal, que exige que la ley indique la pena que corresponde al hecho (*nulla pena sine lege*).

c) Una garantía jurisdiccional, que requiere que la existencia del delito e imposición de la sanción penal se configuren mediante una sentencia judicial, dentro de un proceso legalmente tramitado.

d) Una garantía de ejecución, que exige también – en el supuesto de mediar condena – que el cumplimiento de la sanción penal esté determinada por una ley que la regule a tales fines (Lascano [h] et. al., 2.005).

Lascano [h] et. al. (2.005) agrega que la ley penal reguladora del delito y pena, debe cumplir con los requisitos de ser previa, escrita y estricta. En cuanto al requisito de ley previa, está consagrado en nuestro sistema penal el principio de la irretroactividad de la ley penal más severa, siendo necesario que el sujeto tenga la posibilidad de conocer en el momento de actuar, si es que incurre o no en un delito, y en el caso afirmativo, saber cuál es la pena para dicha conducta; en contraposición, beneficiando al imputado rige el principio de retroactividad y ultraactividad de la ley penal más benigna, que se recepta en el art. 2 del C.P. y prescribe que "*si la ley vigente al tiempo de cometerse el delito fuere distinta de la que exista al pronunciarse el fallo o en el tiempo intermedio, se aplicará siempre la más benigna*". Con la condición de ley escrita, se excluye la costumbre como eventual fuente de delitos y penas; dicha norma debe ser sancionada por el Poder Legislativo, en su carácter de representante del pueblo, ya sea nacional, provincial o municipal. Por último, el requisito de ley estricta, exige un cierto grado de precisión y especificación de la norma penal y excluye la aplicación de analogía *in malam partem*[52]. Esa precisión se exige tanto respecto de la delimitación del tipo penal, como de la determinación de la sanción penal.

En esa línea de pensamiento, Zaffaroni (2.002), añade que conforme el principio de legalidad formal, se cimienta el tipo normativo de ley penal constitucional que sirve para eliminar las restantes leyes penales ilícitas y significa que la única fuente productora de ley penal en el sistema argentino son los órganos constitucionalmente designados a tal fin y la única ley penal es la ley formal que de ellos emana, de conformidad al procedimiento ordenando en el texto constitucional. La C.N. rechaza que la doctrina, la jurisprudencia o costumbre puedan configurar poder represivo. Sin embargo, los usos y costumbres establecen los límites de la tipicidad penal cuando la propia ley – expresa o implícitamente – se refiere a ellos

[52] Analogía *in malam partem* es una locución en latín que significa aplicación de analogía en perjuicio de la parte.

(v.g. límites del fraude comercial, prohibición de maniobras publicitarias entre otros.); continúa expresando que "*toda ley que imponga una pena sin presuponer delito es inconstitucional, pues le falta el hecho del proceso*" (Zaffaroni, 2.002, p. 113).

Asimismo, la Dra. María Luisa Piqué (2.012) señala que el principio de legalidad es una garantía compleja pues obliga y limita a los tres poderes del Estado. Es así que el Poder Ejecutivo está vedado en la creación de tipos penales por decreto; es decir que una pena será legítima cuando esté basada en una ley en sentido formal emanada del órgano legislativo; ello en razón que la imposición de una sanción penal supone una restricción a los derechos fundamentales del individuo como es el caso de la libertad – v.g. de una pena de prisión – o la propiedad – v.g. de una multa –.

Como corolario del principio de legalidad surge la idea de reserva de ley, que exige que los derechos fundamentales sólo pueden ser restringidos por ley. En cuanto a la obligación del Poder Legislativo en la redacción de los tipos penales, debe emplear en sus fórmulas términos que sean claros y precisos y determinar su alcance, para que el juez pueda aplicarlos en aquellos casos que tenga que resolver. Es por ello que está prohibida en el derecho penal la indeterminación en la redacción de las conductas penalmente reprochables, pues ello implicaría una absoluta inseguridad jurídica en un estado de derecho (Piqué, 2.012).

Es necesaria la elaboración y especificación de los tipos penales, utilizando términos estrictos y unívocos que determinen claramente y sin lugar a dudas aquellas conductas punibles, de manera tal que exista una clara definición de la conducta incriminada, que fije sus elementos y permita el deslinde de los comportamientos no punibles o conductas ilícitas sancionadas con medidas no penales (v.g. una reparación de daños y perjuicios del derecho civil). (Piqué, 2.012).

En cuanto a las obligaciones de los jueces, están obligados a considerar sólo como delictivos aquellos comportamientos que fueron determinados previamente como tales por el legislador y en ese orden de ideas, deben limitarse estrictamente a lo prescripto por la ley penal y observar de manera rigurosa la conducta de la persona incriminada con el tipo penal de la norma que se trate, evitando incurrir en la penalización de actos no punibles por el ordenamiento jurídico. El principio de legalidad impide que los jueces consideren como delictivas conductas que sólo guardan una débil semejanza con otro comportamiento que esté incriminado por la ley (Piqué, 2.012).

3.3. Principio de legalidad en los tratados con jerarquía constitucional del art. 75 inc. 22 de la Constitución Nacional.

Cabe aclarar que los tratados con jerarquía constitucional se encuentran mencionados en el art. 75 inc. 22 segundo párrafo de nuestra ley fundamental, a saber: a) Declaración Americana de los Derechos y Deberes del Hombre, b) Declaración Universal de Derechos Humanos, c) Convención Americana sobre Derechos Humanos, d) Pacto Internacional de Derechos Económicos, Sociales y Culturales, e) Pacto Internacional de Derechos Civiles y Políticos, f) Convención sobre la Prevención y Sanción del Delito de Genocidio, g) Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial, h) Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer, i) Convención contra la Tortura y otros Tratos o Penas Crueles, Inhumanos o Degradantes y j) Convención sobre los Derechos del Niño.

Luego de hacer un análisis, estudio y comparación de los mencionados tratados, se advierte que el principio de legalidad de la represión sólo está contemplado como garantía del debido proceso en la Declaración Universal de Derechos Humanos en su art. 11.2; en el Pacto Internacional de Derechos Civiles y Políticos en su art. 15.1; en la Convención Americana de Derechos Humanos en su art. 9 y en la Convención sobre los Derechos del Niño en su art. 40.2 con una similar técnica legislativa para regular el mencionado principio, no siendo regulado en los restantes tratados supra referenciados.

Es en ese orden de ideas que el principio de legalidad en la D.U.D.H.[53] está regulado en el art. 11.2 el que prescribe textualmente: "*Nadie será condenado por actos u omisiones que en el momento de cometerse no fueron delictivos según el Derecho nacional o internacional. Tampoco se impondrá pena más grave que la aplicable al momento de la comisión del delito*".

Por su parte, dentro del P.I.D.C.P.[54], está configurado el principio de legalidad en su art. 15.1, el que reza:

> Nadie será condenado por actos u omisiones que en el momento de cometerse no fueran delictivos según el derecho nacional o internacional. Tampoco se impondrá pena más grave que la aplicable en el momento de la comisión del

[53] D.U.D.H. es la sigla de la Declaración Universal de Derechos Humanos.
[54] P.I.D.C.P. es la sigla del Pacto Internacional de Derechos Civiles y Políticos.

delito. Si con posterioridad a la comisión del delito la ley dispone la imposición de una pena más leve, el delincuente se beneficiará de ello.

Asimismo, el principio penal de legalidad en la C.A.D.H.[55], está explicitado en el art. 9, prescribiendo que:

> Nadie puede ser condenado por acciones u omisiones que en el momento de cometerse no fueran delictivos según el derecho aplicable. Tampoco se puede imponer pena más grave que la aplicable en el momento de la comisión del delito. Si con posterioridad a la comisión del delito la ley dispone la imposición de una pena más leve, el delincuente se beneficiará de ello.

Finalmente el mencionado principio de legalidad está regulado en la C.D.N.[56] en su art. 40.2, rezando que:

> Con este fin, y habida cuenta de las disposiciones pertinentes de los instrumentos internacionales, los Estados Partes garantizarán, en particular:
> a) Que no se alegue que ningún niño ha infringido las leyes penales, ni se acuse o declare culpable a ningún niño de haber infringido esas leyes, por actos u omisiones que no estaban prohibidos por las leyes nacionales o internacionales en el momento en que se cometieron;
> b) Que todo niño del que se alegue que ha infringido las leyes penales o a quien se acuse de haber infringido esas leyes se le garantice, por lo menos, lo siguiente:
> I) Que se presumirá inocencia mientras no se pruebe su culpabilidad conforme a la ley;
> II) Que será informado sin demora y directamente o, cuando sea procedente, por intermedio de sus padres o sus representantes legales, de los cargos que pesan sobre él y que dispondrá de asistencia jurídica u otra asistencia apropiada en la preparación y presentación de su defensa;
> III) Que la causa será dirimida sin demora por una autoridad u órgano judicial competente, independiente e imparcial en una audiencia equitativa conforme a la ley, en presencia de un asesor jurídico u otro tipo de asesor adecuado y, a menos que se considerare que ello fuere contrario al interés superior del niño, teniendo en cuenta en particular su edad o situación y a sus padres o representantes legales;
> IV) Que no será obligado a prestar testimonio o a declararse culpable, que podrá interrogar o hacer que se interrogue a testigos de cargo y obtener la participación y el interrogatorio de testigos de descargo en condiciones de igualdad;
> V) Si se considerare que ha infringido, en efecto, las leyes penales, que esta decisión y toda medida impuesta a consecuencia de ella, serán sometidas a una autoridad y órgano judicial superior competente, independiente e imparcial, conforme a la ley;

[55] C.A.D.H. es la silga de la Convención Americana de Derechos Humanos.
[56] C.D.N. es la sigla de la Convención sobre los Derechos del Niño.

VI) Que el niño contará con la asistencia gratuita de un intérprete si no comprende o no habla el idioma utilizado;

VII) Que se respetará plenamente su vida privada en todas las fases del procedimiento.

Destacando que hay sutiles diferencias en cuanto a la redacción del articulado de los tratados en los que se hace mención del principio de legalidad, se vislumbra que será necesario en todo proceso penal en el que está consagrado este principio, funcione como una garantía procesal para el imputado, debiéndose respetar el aforismo *nullum crimen, nulla poena sine lege* que como se abordó implica que no existe delito ni pena sin una ley penal previamente determinada por el legislador.

3.4. De la prohibición en la aplicación de analogía

Con respecto a la prohibición de la analogía en el ámbito penal como derivación del principio de estricta legalidad, la analogía es entendida como una herramienta extensiva para la aplicación de una solución prevista en una ley penal a casos fáctica y valorativamente similares al que está contemplado, pero que no encastra en la norma. Es oportuno diferenciar este concepto de la interpretación extensiva, pues esta última conducta sometida a examen si está prevista en la norma pero que para llegar a esa conclusión se exige un análisis pormenorizado y más profundo. Atento esta diferencia es que se habla de aplicación analógica en lugar de interpretación analógica.

En cambio Lascano [h] et. al. (2.005) considera que dentro del derecho penal liberal, conforme al principio de legalidad y de reserva, el juez debe dilucidar cuál es la voluntad de la ley, que constituye la única fuente de conocimiento, permitiéndose tanto la interpretación extensiva – al momento de determinar que el sentido literal del texto de la norma es insuficiente, entrando a regularse hipótesis de hecho que solo han sido contempladas de modo implícito –, como la interpretación analógica ordenada por la misma ley penal, cuando la descripción casuística no abarca todos los casos pero se añade la exigencia que el juez la aplique a supuestos similares a los previstos (v.g. art. 140 del C.P. que sanciona al que redujera a una persona a servidumbre o a otra condición análoga). El límite entre lo tolerado y lo prohibido en ambas interpretación, estará condicionado por el sentido literal y lingüístico del texto de la norma.

Sin embargo es necesario aclarar que los supuestos hermenéuticos de la ley penal no deben confundirse con el instituto de la analogía como fuente del derecho

penal, en pos de pretender completar los vacíos o lagunas legales de punición o zonas de impunidad que se producen cuando la acción que el juez analiza en un caso concreto no presenta estricta adecuación con la descripción abstracta que está contenida en el tipo penal que a *prima facie* podría aplicársele (Lascano [h], et. al., 2.005).

Esta conducta es atípica dado que la norma penal no la tuvo en miras al momento de configurarla, por lo que el tribunal que intervenga en la resolución del caso, no podrá utilizar - en la determinación legal – otro tipo delictivo previsto para regular otra hipótesis fáctica diferente, por la razón de guardar similitud con aquella conducta (Lascano [h], et. al., 2.005).

Admitir lo contrario, es decir la analogía legal – que el art. 2 del C.C.C.N.[57] reconoce como fuente para la solución de lagunas del derecho –, sería reemplazar la voluntad del legislador plasmada en la ley por la voluntad del juez, destacando que en materia penal el juzgador nunca podrá crear una norma imitando a otra, como así tampoco es adecuado imponer a una conducta prevista en un tipo penal especifico, una sanción más grave (Lascano [h], et. al., 2.005).

No cabe duda que la analogía jurídica está igualmente vedada en el ámbito jurídico penal para reprimir conductas atípicas o hacerlo con mayor severidad, en base a las orientaciones teleológicas del sistema normativo, pues ella importaría una verdadera creación del derecho por voluntad del sentenciante, para regir situaciones que no han sido reguladas expresa ni implícitamente en la ley punitiva (Lascano [h], et. al., 2.005, p.150).

En el mismo orden de ideas Nuñez (1.999) esboza que del principio de legalidad y reserva penal se prohíbe que la ley penal se aplique por analogía; de ello surge que le está vedado al Poder Judicial sancionar un caso por su analogía con otro que la ley castiga – lo que se denomina analogía legal – o por analogía basado en la imperiosidad de brindar protección en el caso concreto – denominada analogía jurídica –.

La analogía legal conlleva la aplicación de una sanción que está conminada por la ley para un tipo penal concreto y especifico, a otro que no está contemplado al previsto en aquel tipo pero que – por su semejanza – en los supuestos que se

[57] Código Civil y Comercial de la Nación.

presentan, existe el mismo argumento para penarlo (*ubi eadem est ratio, eadem est o debet esse juris dispositio*[58]). (Nuñez, 1.999).

En cuanto a la analogía jurídica, por exigencia en la protección de un interés por una razón política, parte de un hecho que, no tipificado penalmente, se le aplica la pena al tipo de características más similares; se aplica el llamado principio de similitud de necesidad de protección, que es una razón para castigar – con arreglo a la norma legal que reprime el hecho de significado más semejante – otro hecho no previsto en la ley penal como delito (Nuñez, 1.999).

Con relación a la analogía *in malam partem*, existe consenso entre los doctrinarios sobre su prohibición, es decir aquella aplicada por el juzgador en perjuicio del imputado en una causa penal, con la finalidad de ampliar la zona de represión que es definida taxativamente por la norma penal (Lascano [h], et. al., 2.005).

Por su parte, Nuñez (1.999) sobre el tema afirma que la prohibición de la aplicación de analogía de la ley penal sólo rige en aquellos casos en que sea perjudicado el imputado – analogía *in malam partem* –, siendo tal la que justifica la aplicación de una sanción penal o que agrave la situación del procesado o condenado.

Diferente es el caso de la analogía *in bonam partem*[59] pues está controvertida su aceptación dentro de la doctrina nacional; para algunos autores como es caso del Dr. Lascano [h] y del Dr. Nuñez que se pronuncian a favor, la extienden hacia los principios generales del derecho. Ellos entienden que encuentra su fundamento en el art. 18 de la C.N., actuando como una garantía procesal que funciona en beneficio y no en perjuicio del imputado, considerando en definitiva que debe admitirse la aplicación de la norma penal por analogía *in bonam partem*, ya sea en un caso para excluir o en otro caso para morigerar la sanción penal o bien para mejorar la situación procesal del interesado (Lascano [h], et. al., 2.005).

En similares palabras explica Nuñez (1.999) que las garantías constitucionales – entre ellas la del art. 18 de la C.N. – funcionan en beneficio y no para perjudicar al imputado; de ello se consagra la aplicación de la ley penal por analogía *in bonam partem* para aminorar o finiquitar una pena o para mejorar la situación del imputado.

[58] *Ubi eadem est ratio, eadem est o debet esse juris dispositio* es una locución en latín que significa donde hay la misma razón, debe ser igual la disposición del Derecho.
[59] Analogía *in bonam partem* es una locución en latín que significa aplicación de analogía en beneficio de la parte.

3.5. Falta de tipo penal: Atipicidad.

La falta de configuración de la conducta concreta a la descripción abstracta contenida en el tipo penal, genera lo que se conoce como atipicidad de la acción del sujeto, lo que excluye su delictuosidad penal, aunque podría subsistir su ilicitud, susceptible de la correspondiente responsabilidad civil resarcitoria (Lascano [h], et. al., 2.005).

La ausencia de cualquiera de los elementos del tipo objetivo supone aticipidad:

a) Cuando el hecho realizado no concuerda con la acción descripta en el núcleo del tipo; cuando no se produce el resultado que éste requiere; o cuando, a pesar de la existencia del comportamiento exterior y del resultado típico, no se comprueba el nexo causal entre ambos o no se puede atribuir objetivamente el resultado a la actuación del sujeto.

b) Por falta de sujeto activo ("oficial público", art. 136 C.P.; "jefe de prisión, art. 143 inc. 4 C.P.; "comerciante declarado en quiebra", art. 176 C.P.).

c) Por falta de sujeto pasivo o de objeto ("orador", art. 160 C.P.; "persona incapaz de valerse", art. 106 C.P.).

d) Por falta de las circunstancias temporales o espaciales (en tiempo de "guerra", art. 218 C.P.; "en el mar o en ríos navegables", art. 198, inc. 1 C.P.).

e) Por carencia del medio ("fuerza en las cosas o violencia en las personas", art. 164 C.P., "intimidación", art. 168 C.P.).

Asimismo puede generarse la mencionada aticipidad de la conducta del sujeto, cuando se presentan defectos en el tipo subjetivo:

a) Por error de tipo, al recaer en cualquiera de los elementos del tipo objetivo, sean fácticos o descriptivos, sean normativos o valorativos. Al excluir el dolo, no hay tipicidad dolosa, aunque puede subsistir responsabilidad penal si existe el tipo culposo y la conducta del sujeto se adecua a éste.

b) Por ausencia de elementos subjetivos del tipo distintos del dolo ("con la intención de menoscabar su integridad sexual", art. 130 del C.P.). (Lascano [h], et. al., 2.005, pp.282-283).

3.6. De clasificación de los ilícitos en típicos y atipicos.

Desde un enfoque de la teoría general del derecho, enseñan Atienza y Ruiz Manero (2.006) que los problemas teóricos en la elaboración de una idea sobre ilicitud atípica son consecuencia primordialmente del hecho que la teoría estándar de la norma jurídica se ha centrado – al menos hasta ahora – en el análisis de algunos tipos de reglas jurídicas, pero descuidando otros tipos de reglas, en especial los principios.

Su base es a partir de lo que dieron en llamar la teoría general de los ilícitos atípicos. Mencionan que existen normas regulativas que conforman una estructura de dos niveles, 1) el de las reglas y 2) el de los principios. Este tipo de normas regulan conductas – reglas de acción y principios en sentido estricto – o estado de cosas – reglas de fin o directrices – y no sólo poseen una dimensión directiva sino además una dimensión valorativa, proporcionando criterios de valoración de esas conductas. Mientras que los principios manifiestan directamente los valores incorporados al sistema jurídico y las directivas que de ellos derivan, las reglas conforman concreciones relativas a las circunstancias genéricas de sus condiciones de aplicación, que se derivan del balance entre los principios destacados en esas circunstancias (Atienza y Ruiz Manero, 2.006).

Los principios y las reglas son elementos del derecho considerado de forma integral o cada una de las instituciones que lo conforman. Se considera que quien le da el sentido a las reglas, en cuanto a su fundamentación, son los principios; además estos principios no se aplican en forma directa en la resolución de casos sino que dan paso primero a las reglas (Atienza y Ruiz Manero, 2.006).

Un ilícito es un acto contrario a una norma regulativa de mandato; puede calificarse como ilícito una acción en sentido amplio – como acción propiamente dicha u omisión – que se califica como obligatoria o prohibida, o bien la consecuencia de acciones u omisiones cuando aquella consecuencia está calificada (Atienza y Ruiz Manero, 2.006).

Pudiendo ser las normas de mandato reglas o principios, se encuentran dos tipos de ilícitos, 1) los ilícitos típicos, que se conceptualizan como acciones contrarias a reglas de mandato y 2) los ilícitos atípicos, que son acciones contrarias a principios de mandatos.

Atienza y Ruiz Manero (2.006) ante lo expuesto, realizan una clasificación de actos ilícitos en típicos y en atípicos, tomando como punto de partida el análisis sobre el concepto de tipicidad efectuado por penalistas.

Distinguen entre el denominado "tipo de garantía" y el "tipo sistemático"; el tipo de garantía consiste en que la descripción de los delitos deben ser relativamente precisas, siendo una acción típica aquella que debe subsumirse estrictamente en dicha descripción, conforme el principio *nullum crimen, nulla poena sine lege*. En contraste, el tipo sistemático no presenta la completa descripción del delito, sino algunos aspectos de ella; según esta segunda acepción un tipo es el conjunto de algunos aspectos determinantes de la descripción efectuada por la ley como requerida para aplicar el castigo. Esa conceptualización de tipo cumple con la función de fijar los límites entre la tipicidad y la antijuridicidad; la acción típica es sospechosa de ser antijurídica, requiriendo de una posterior encuadramiento respecto de si está justificada o no (Atienza y Ruiz Manero, 2.006).

Pasando al análisis de la tipicidad conforme al tipo de garantía – en el que se hará hincapié –, es consecuencia directa del principio de legalidad que rige en todo estado constitucional de derecho. Así, los delitos deben estar determinados por reglas y no en meros principios. Con respecto al principio de legalidad, el doctrinario Luigi Ferrajoli propuso una distinción entre el principio de "mera legalidad", que establece que solo las leyes (y no otras fuentes externas) dicen que es delito, y el principio de estricta legalidad, que prohíbe que las leyes penales determinen elementos sustanciales, que se decidan por medio de juicios de valor, como condiciones que deben ser necesarias y suficientes para determinar los delitos; es decir que las leyes penales no pueden tipificar como delitos acciones configuradas tan solo en términos valorativos (Atienza y Ruiz Manero, 2.006).

Esbozan Atienza y Ruiz Manero (2.006) que la exigencia de la estricta legalidad es el requisito que debe cumplir el derecho penal – máxime los derechos penales garantistas – y que en más o menos variabilidad es aplicable a otros campos del derecho sancionatorio.

Si la premisa es que los ilícitos típicos son conductas contrarias a una regla de mandato, los ilícitos atípicos serían conductas contrarias a principios de mandato. En cuanto a los primeros – los ilícitos típicos – son el resultado de extender

analógicamente la ilicitud establecida en reglas cuyo razonamiento se denomina *analogía legis,* o son el resultado de la ponderación entre los principios relevantes del sistema, cuyo balance exige la generación de una nueva regla prohibitiva, lo que se denomina *analogía iuris.* Con respecto a los ilícitos atípicos, éstos invierten o cambian el sentido de una regla, que a *prima facie* dicha regla permite la conducta en cuestión y sin embargo por oposición a algún/os principio/s, esa acción se convierte – cuando se consideran todos los factores – en ilícita (Atienza y Ruiz Manero, 2.006).

Clarifican Atienza y Ruiz Manero (2.006) que los ilícitos atípicos son conductas que – en principio – se encuentran permitidas por una regla, pero que al momento de ser consideradas la totalidad de las circunstancias, debe considerárselas prohibidas. Se produce un cambio de estado deóntico – de una acción permitida a otra que es prohibida – que tiene lugar en virtud de un proceso argumentativo, en el que se distingue dos mecanismos: 1) la analogía que, como se dijo, puede ser *analogía legis o iuris*, en estos dos supuestos se parte de la existencia de una laguna normativa en el nivel de las reglas – en principio la acción se encuentra permitida en el sentido de no estar subsumida en ninguna otra norma prohibitiva –; el cambio de estado deóntico se produce ante los supuestos de *analogía legis* por la similitud que el caso no regulado presenta con otros casos en los que si opera una regla prohibitiva; y es en ese momento que el balance entre principios justifican la prohibición de estos últimos supuestos que se producen en conexión con el caso que aparecía como no contemplado. Con respecto a los casos de *analogía iuris* la creación de la nueva regla prohibitiva es exigida por el balance entre los principios del sistema que se aplican al caso, aun cuando no existe una regla prohibitiva aplicable a casos similares; 2) el punto de partida es la existencia de una laguna axiológica – la conducta en principio está permitida encontrándose presente una regla regulativa que la permite –; en este caso el cambio de estado deóntico se produce como efecto que la subsunción del supuesto en dicha regla resulta contradictoria con el balance de los principios del sistema, que son aplicables al caso y dicho balance requiere el nacimiento de una nueva regla prohibitiva en donde subsumir el caso.

La razón de ser de los ilícitos atípicos responde a la necesidad que debe tener el sistema jurídico, intentando producir un ajuste entre la dimensión directiva y la dimensión justificativa del derecho, entre reglas y principios. Por ello puede decirse que la categoría de ilícitos atípicos es normal en todas las legislaciones jurídicas

contemporáneas, intentando evitar un excesivo formalismo en la aplicación del derecho, lo que eventualmente podría conducir a una incoherencia valorativa de las sentencias judiciales (Atienza y Ruiz Manero, 2.006).

La categoría general de los ilícitos atípicos tienen en común los siguientes elementos: a) la existencia – a *prima facie* – de una conducta permitida por una regla; b) la producción – intencional o no – como consecuencia de esa acción; c) el carácter injustificado de dicho daño, luego del correspondiente balance que se realizan entre los principios relevantes del sistema y d) la generación, desde la óptica de ese balance, de una nueva regla que limita el alcance de la primera, calificando como prohibidos aquellos comportamientos que en un principio aparecían como permitidos por esa primera regla (Atienza y Ruiz Manero, 2.006).

3.7. Conclusiones parciales.

Luego de haber sido abordado el presente capítulo, concluimos que tanto en la Constitución Nacional como en los tratados con jerarquía constitucional receptados en el art. 75 inc. 22 de nuestra ley fundamental, expresamente queda establecido que toda conducta en sentido amplio que pretenda ser configurada como delictiva, debe adecuarse necesariamente al principio penal de legalidad que entendida como garantía del debido proceso, exige al legislador que previamente determine aquella conducta que configura un delito y la pena que corresponda aplicar; asimismo se limita el poder punitivo del estado en su función de sancionar, delimitándose el campo de lo que es punible y de lo no punible. Con relación a la suplantación de identidad de la persona que no está penalmente regulada en la actualidad, manifestamos que la aplicación de tipos o penas diferentes a ella – como se mencionó oportunamente – ergo configura la vulneración del citado principio de legalidad expuesto.

Conforme a ello, es que además en nuestro derecho como principio general se prohíbe en los casos que se presentan ante el juez, la aplicación de analogía como fuente de conocimiento del derecho penal que pretenda reprimir conductas atípicas, cuando es en perjuicio del imputado, máxime si el magistrado intenta extender la zona de punición que establece la norma penal. Si bien la doctrina no es pacifica en lo que se denomina aplicación de analogía *in bonam partem*, este supuesto considerado de excepción por parte de la doctrina, podría ser aplicado por el magistrado en aquellas

causas en las que no se configura la conducta delictiva y sosteniendo que la garantía del art. 18 del C.N. es en beneficio y no para el perjuicio del imputado.

En esa dirección insistimos que los casos de *phishing* deben ser contemplados por el legislador conforme el mencionado principio de legalidad de la represión, especificando el tipo penal y la sanción para aquellos supuestos en que se realice la suplantación de identidad de la persona, teniendo en consideración lo expuesto sobre su falta de regulación jurídica dentro del derecho penal, a fin de evitar la violación del referenciado principio.

Por último enfatizamos que si bien la suplantación de identidad penalmente no configura hasta la fecha un delito ni es pasible de sanción punitiva conforme lo expuesto, podría ser adecuada esta conducta como un ilícito del derecho privado y a los fines de su reparación, sería razonable plantear la cuestión mediante la interposición de una acción por daños y perjuicios, con su correspondiente sanción resarcitoria.

CAPITULO IV: ANALIS DE LA SUPLANTACION DE IDENTIDAD EN EL DERECHO COMPARADO.

4.1. Introducción.

En este cuarto y último capítulo se realizará un análisis comparativo sobre la suplantación de identidad de la persona en países de América del Sur como es el caso de Brasil, Paraguay, Colombia y Perú; y de Europa se tomará como modelo de investigación a España, teniendo como finalidad mostrar cuál es el grado de avance, tratamiento y de regulación jurídica – o no – existente sobre la temática abordada, a cuyos fines será necesario el estudio y análisis de los códigos penales de cada uno estos países y determinar dentro del articulado de cada uno de ellos – con su respectiva transcripción –, cuál es el encuadre jurídico del *phishing*.

4.2. Regulación normativa en el Derecho Penal Brasilero.

Con relación al Derecho Penal Brasilero, fue sancionada recientemente en el año 2.012 la ley Nº 12.377 de delitos informáticos en aquél país, reformando el

C.P.B[60]. en sus arts. 154 – A y 154 – B dentro de la sección IV: "de los crímenes contra la inviolabilidad de los secretos".

Sobre la figura objeto de investigación, no existe un tipo penal específico relacionado con la suplantación de identidad, existiendo sólo la posibilidad de ser regulada de manera genérica dentro de los 2 artículos supra mencionados.

El art. 154 – A. refiere a la intromisión realizada de un dispositivo informático, regulando en sus incisos, distintos supuestos de que van aumentando gradualmente la penalidad de la conducta delictiva, dependiendo de las víctimas lesionadas por el delito, prescribiendo que:

> Invadir el dispositivo informático ajeno, conectado o no a la red de ordenadores, mediante infracción indebida de un mecanismo de seguridad y con el fin de obtener, adulterar o destruir datos o informaciones sin autorización expresa o tácita del titular del dispositivo o instalar vulnerabilidades para obtener ventaja ilícita: pena - detención, de 3 (tres) meses a 1 (un) año, y multa.
> 1º. En la misma pena incurre quien produce, ofrece, distribuye, vende o difunde dispositivo o programa de ordenador con el fin de permitir la práctica de la conducta definida en el encabezado.
> 2º. Se aumenta la pena de un sexto a un tercio si de la invasión resulta perjuicio económico.
> 3º. Si de la invasión resulta la obtención de contenido de comunicaciones electrónicas privadas, secretos comerciales o industriales, informaciones sigilosas, así definidas en ley, o el control remoto no autorizado del dispositivo invadido: pena - reclusión, de 6 (seis) meses a 2 (dos) años, y multa, si la conducta no constituye un crimen más grave.
> 4º En la hipótesis del inc. 3º, se aumentará la pena de uno a dos tercios si hay divulgación, comercialización o transmisión a tercero, a cualquier título, de los datos o informaciones obtenidos.
> 5º Se incrementa la pena de un tercio a la mitad si el crimen se practica contra:
> I - Presidente de la República, gobernadores y alcaldes;
> II - Presidente del Supremo Tribunal Federal;
> III - Presidente de la Cámara de Diputados, del Senado Federal, de Asamblea Legislativa de Estado, de la Cámara Legislativa del Distrito Federal o del Ayuntamiento;
> IV - Dirigente máximo de la administración directa e indirecta federal, estadual, municipal o del Distrito Federal.

En cuanto al art. 154 – B, hace mención a la acción penal referida al art. 154 – A, rezando:

[60] Código Penal de Brasil.

> En los crímenes definidos en el art. 154 – A no sólo se realiza mediante representación, salvo si el delito se comete contra la administración pública directa o indirecta de cualquiera de los Poderes de la Unión, Estados, Distrito Federal o Municipios o contra empresas concesionarias de servicios públicos.

4.3. Regulación normativa en el Derecho Penal Paraguayo.

La conducta denominada *phishing* tiene un tratamiento genérico en la figura penal de estafa o defraudación en el C.P.P[61]., pudiendo ser incluida dentro del título II: "hechos punibles contra los bienes de la persona" – capítulo III: "hechos punibles contra el patrimonio", en su art. 188 sobre operaciones fraudulentas por computadora y en el art. 189 sobre aprovechamiento clandestino de una prestación, que por ley Nº 4.439 (5/10/11) de ese país, su nombre fue rebautizado como "estafa mediante sistemas informáticos". El art. 188 del citado código prescribe:

> Operaciones fraudulentas por computadora:
>
> 1º El que con la intención de obtener para sí o para otro un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante:
>
> 1. programación falsa;
>
> 2. utilización de datos falsos o incompletos;
>
> 3. utilización indebida de datos; u
>
> 4. otras influencias indebidas sobre el procesamiento, y con ello, perjudicara el patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa.
>
> 2º En estos casos, se aplicará también lo dispuesto en el artículo 187, incisos 2º al 4º.

Por su parte, el art. 189 del código de mención reza:

> Aprovechamiento clandestino de una prestación:
>
> 1º El que con la intención de evitar el pago de la prestación, clandestinamente:
>
> 1. se aprovechara del servicio de un aparato automático, de una red de telecomunicaciones destinada al público, o de un medio de transporte; o
>
> 2. accediera a un evento o a una instalación, será castigado con pena privativa de libertad de hasta un año o con multa, siempre que no estén previstas penas mayores en otro artículo.

[61] Código Penal de Paraguay.

2º En estos casos, será castigada también la tentativa.

3º En lo pertinente se aplicará lo dispuesto en los artículos 171 y 172.

4.4. Regulación normativa en el Derecho Penal Colombiano.

La conducta de la suplantación de identidad se encuentra regulada en el título VII bis: "De la protección de la información y de los datos" – capítulo I: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", del C.P.C[62]., en una figura típica especifica en el art. 269 G: "suplantación de sitios *web* para capturar datos personales", el que prescribe:

> El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
>
> En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
>
> La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Esta figura combina la estafa con la importancia de la identidad en *internet*, tanto individual como empresarial. El artículo transcripto *ut supra* tipifica lo que comúnmente se denomina *phishing.*

Por otra parte, un punto importante a considerar es que el art. 269 H del citado código, agrega circunstancias de agravación punitiva de los tipos penales descriptos en el capítulo I, aumentando la pena de la mitad a las tres cuartas partes y reza:

> Circunstancias de agravación punitiva. Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
>
> 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
>
> 2. Por servidor público en ejercicio de sus funciones.
>
> 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

[62] Código Penal de Colombia.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

4.5. Regulación normativa en el Derecho Penal Peruano.

La modalidad denominada suplantación de identidad de la persona, está regulada normativamente en un tipo específico mediante la sanción de la ley Nº 30.096 de delitos informáticos del año 2.013 por el Congreso de Perú en su art. 9 que complementa el Código Penal de aquel país, encuadrado dentro de los delitos informáticos que atentan contra la fe pública. El mencionado art. reza:

> Art. 9. Suplantación de identidad. El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de la libertad no menor de tres ni mayor de cinco años.

Como surge del precepto legal, la conducta de *phishing* determina de manera inequívoca las dos partes que posee toda norma jurídica. Por un lado se determina cuál es el supuesto de hecho que debe encuadrar dentro de la descripción abstracta del artículo y por otro se establece la pena que corresponde para este tipo de conducta.

4.6. Regulación normativa en el Derecho Penal Español.

La temática en el ordenamiento jurídico español a la hora de valorar el tratamiento jurídico de los delitos informáticos, conviene anticipar dos premisas:

a) Existe entre los juristas un cierto debate acerca de la propia existencia jurídica de los delitos informáticos. Algunas posiciones sostienen, de manera clara, que el *ciberdelito* no existe, dado que se reduce al mero hecho de ser cometido sobre o mediante el ordenador. En este sentido, no sería necesario un tratamiento específico por parte de los ordenamientos jurídicos.

Sin embargo, quizás por puro pragmatismo, la mayor parte de los juristas consideran necesaria una tipificación específica de estos delitos, debido a la existencia

de una nueva realidad como son las autopistas de la información. Este último parece ser el camino seguido no sólo por el ordenamiento penal español, sino por la mayoría de los correspondientes a países de nuestro entorno.

b) Una segunda decisión consiste bien en separar los delitos informáticos de los delitos tradicionales a través de un tratamiento diferenciado, o bien la decisión de una regulación conjunta.

El legislador español se ha decantado por una regulación no autónoma, de modo que no existe en el C.P.E[63]. de 1995 un título propio relativo a los delitos informáticos insertándose su tipificación en los correspondientes a los delitos tradicionales.

La conducta denominada *phishing* está incluida de manera genérica, en el C.P.E. dentro del capítulo VI: de las defraudaciones, sección 1ª de las estafas, dentro de los delitos de naturaleza económica que afectan patrimonialmente a la persona.

Dentro de este grupo, el delito más habitual -por cuanto engloba una amplia variedad de conductas delictivas- es la estafa informática. Regulada en el art. 248 del citado código, en su inciso 1º se distingue entre los supuestos de estafa basados en técnicas de ingeniería social pura – donde se sitúa el *phishing –,* prescribiendo que: "*cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno*"; y los supuestos de utilización de código malicioso (*malware*) o de intrusión en sistemas de información son recogidos en el art. 248 inciso 2º a) del Código Penal Español, el que reza "*también se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero"*.

El legislador contempla también la posibilidad de delito en grado de tentativa en un tercer apartado del artículo, por lo que la posesión o distribución de programas maliciosos *(malware*) en sí misma podría ser constitutiva de delito.

[63] Código Penal Español.

4.7. Conclusiones parciales.

Habiendo analizado y estudiado la figura del *phishing* en los países que se trataron en este capítulo, señalamos que es oportuno mencionar que no hay en todas las legislaciones estudiadas la misma calidad o técnica legislativa al respecto. En el caso de Brasil, Paraguay y España, podemos observar que, más allá de la forma de redacción y particularidades que existen sobre la materia bajo análisis en el Código Penal de todos ellos, no existe un tipo penal específico sobre la suplantación de la persona, incluyendo esta actividad en todos los casos dentro de las defraudaciones o estafas, pudiendo configurarse la aplicación de la analogía en materia penal que como es sabido se encuentra prohibida. Es por ello que se debería realizar una reforma que incluya este tipo de conducta en un tipo penal con la determinación de la pena, a los fines de respetar el ya mencionado principio de legalidad y evitando su vulneración. En el caso de Colombia y de Perú, es notable el grado de avance y de la técnica legislativa que se ha efectuado sobre la suplantación de identidad, estableciendo – dentro de la composición de toda norma jurídica – cuál es la descripción abstracta del supuesto de hecho, es decir la identificación de un tipo penal especial y cuál es la pena merecedora para esta conducta considerada legalmente como delictiva en estos países.

Conclusiones finales.

Iniciando la conclusión final del presente trabajo, en el capítulo 1 explicamos técnicamente en qué consiste la suplantación de identidad de la persona, cuáles son sus modalidades más frecuentes, las fases concatenadas y secuenciales llevadas a cabo, las finalidades perseguidas y los sujetos intervinientes de esta conducta compleja.

La suplantación de identidad consiste en un ataque informático, de ingeniería social que tiene por finalidad la adquisición de información confidencial de la víctima mediante el uso de ardid o engaño, pudiendo provocar perjuicios patrimoniales, como es la afectación del derecho de propiedad y también consecuencias dañosas en el ámbito extrapatrimonial, como es la vulneración verbigracia del buen nombre, reputación, imagen, prestigio o intimidad de la persona.

Los ataques de *phishing* están destinados a personas físicas y jurídicas; en el primer caso, recomendamos al usuario que ante la duda respecto de la procedencia y el contenido de la mensajería o correos enviados a su cuenta de *mail*, no ejecute la

acción esperada por el *phisher*, evitando así consecuencias dañosas. En el caso de las organizaciones la situación es diferente pues cuentan con sistemas de seguridad que las previenen y defienden en alguna medida de potenciales ataques de este tipo, aunque no hay seguridad de protección absoluta en aquellos casos de *phishing* sofisticado, que en ocasiones vulneran estas defensas.

Habiendo determinado en qué consiste la conducta, enfatizamos en las funciones de prevención, detección y frustración de los ataques de suplantación de identidad que todo sujeto debe observar al momento del uso de sistemas informáticos, ya que en el caso de ingresar a la zona de control del *phisher*, éste tendrá el dominio de la situación, de la información confidencial, difícilmente podrá ser recuperada y lo que es peor aún, podrá causar daños y perjuicios irreparables.

Con relación al segundo capítulo, consideramos que la hipótesis de trabajo ha sido confirmada por configurarse la vulneración del principio de legalidad y la afectación de prohibición de analogía en el derecho penal, pues en primer lugar advertimos que desde la entrada en vigor de la ley de delitos informáticos Nº 26.388/2.008 que reforma algunos artículos del C.P., no surge tipo delictivo ni pena alguna que regule legalmente a la suplantación de identidad de la persona. Corroboramos esta aseveración ya que en los años 2.010, 2.011 y 2.012 se presentaron ante el Senado de la Nación algunos proyectos de ley sobre esta cuestión, que fueron rechazados probablemente por el confuso, impreso y erróneo lenguaje técnico – jurídico empleado con el fin de intentar encuadrar al *phishing* en el derecho penal nacional; entre los fundamentos que esbozan los legisladores para la aprobación de los mencionados proyectos, lo tratan de antemano como si fuese una conducta delictiva en algunos casos, como un delito en otros, como un robo de identidad, usurpación de identidad, hurto o también como una estafa utilizada con ardid o engaño con la potencialidad de producir daños en el futuro (lo que se critica por la eventualidad de esa circunstancia), entendiendo que esos tipos penales corresponden a conductas distintas de la suplantación de identidad, cuyo supuesto de hecho no se adecua a la descripción en abstracto que estos tipos penales configuran; en segundo lugar confirman la mencionada hipótesis las sentencias dictadas por los tribunales citados, por un lado al demostrarse la vulneración de la prohibición de analogía que rige en el derecho penal – máxime cuando es en perjuicio del imputado –, ya que los casos mencionados fueron resueltos aplicando el tipo delictivo del hurto en unos, y la

estafa o defraudación genérica en otros. Asimismo comprobamos la afectación del principio penal de legalidad como garantía del debido proceso, receptado en el art. 18 de la C.N. y en los tratados con jerarquía constitucional del art. 75 inc. 22, porque no existe regulación en la legislación penal argentina actual, de ningún tipo delictivo ni pena referida a la suplantación de identidad.

A su vez, consideramos a la suplantación de identidad como una actividad ilícita pero atípica en rigor porque no es en sí un delito y que más allá de su falta de regulación legal, tiene su propia autonomía, particularidades, matices que requieren de su tipificación penal, sin perjuicio que a partir de esta figura puedan cometerse en sentido estricto conductas delictivas.

Por otro lado, desde un enfoque académico planteamos como una alternativa, configurar al *phishing* dentro de los elementos o presupuestos de la teoría del delito, para poder ser considerada actividad delictiva. Es así que afirmamos la necesidad de establecer en primer lugar cuál sería la conducta típica, antijurídica y culpable que se refiera específicamente a la suplantación de identidad; a modo de ejemplo podría utilizarse la siguiente fórmula como tipo penal: "se aplicará pena de prisión de dos a cinco años, al que suplantare la identidad de una persona física o jurídica mediante ardid o engaño, con el fin de obtener información confidencial que afectare el ámbito patrimonial o extrapatrimonial"; en segundo lugar, consideramos adecuada la modificación o la sanción integral de una nueva ley de delitos informáticos complementaria al C.P., que encuadre legalmente a esta y otras figuras informáticas para alcanzar una completa tipificación y sanción de todas aquellas conductas que utilicen las nuevas tecnologías, sistemas de información digital e *internet* – que a la fecha no están reguladas–, actualizando de esta manera nuestro derecho penal argentino en pos de tipificar y castigar toda actividad delictiva que utilice sistemas informáticos.

Abordando el tercer capítulo, y en consideración a las conclusiones hasta aquí expuestas, expresamos que la falta de regulación normativa de la suplantación de identidad en nuestro derecho penal atenta contra principio penal de legalidad de la represión que es entendido como una garantía penal-constitucional del debido proceso, que exige al legislador la previa determinación de aquella conducta que es

configurada como un delito, bajo pena de sanción, delimitándose así el campo de lo punible y de lo no punible.

En esa dirección insistimos que los casos de *phishing* deben ser contemplados por el legislador conforme el mencionado principio de legalidad de la represión, especificando cuál es el tipo penal y la sanción para aquellos supuestos en que se realice la suplantación de identidad de la persona, teniendo en consideración lo expuesto sobre su actual falta de regulación jurídica dentro del Derecho Penal Argentino, a fin de evitar la violación del referenciado principio.

Así también manifestamos que se torna imperioso velar por el respeto y el cumplimiento efectivo de este principio consagrado expresamente por el art. 18 de la Constitución Nacional y en los tratados con jerarquía constitucional del art. 75 inc. 22 de la carta magna, más precisamente en la Declaración Universal de Derechos Humanos en su art. 11.2, en el Pacto Internacional de Derechos Civiles y Políticos en su art. 15.1, en la Convención Americana de Derechos Humanos en su art. 9 y en la Convención sobre los Derechos del Niño en su art. 40.2.

Ahora bien, si en nuestro derecho rige el principio general que prohíbe la aplicación de analogía como fuente de conocimiento del derecho penal, es lógico sostener que esta actividad está vedada a los magistrados. Pero habiendo probado que con relación al *phishing* se aplicaron tipos penales y sanciones distintos a él, concluimos que dicha actividad judicial configura una vulneración, menoscabo y afectación del referenciado principio penal de legalidad. Son los jueces quienes deben ser cuidadosos al momento de evaluar aquellas causas relacionadas con la suplantación de identidad antes de su resolución, para evitar así el incumplimiento de lo prescripto por este principio penal.

También enfatizamos que si bien la suplantación de identidad actualmente no configura un delito ni es pasible de sanción punitiva dentro del derecho penal como se expone; eventualmente podría ser adecuada esta conducta como un ilícito del derecho privado que intente una reparación integral mediante la interposición de una demanda por daños y perjuicios en cuanto al ámbito patrimonial y que también persiga la reparación del ámbito extrapatrimonial o daño moral, como son los derechos a la intimidad, identidad, imagen y honor de la persona que pudieran verse afectados; supuestos que están regulados en el nuevo Código Civil y Comercial y en razón que

dentro del derecho privado se admite la aplicación de analogía, podría utilizarse la acción resarcitoria como una vía alternativa para que esta conducta atípica no quede en la impunidad.

En cuanto al cuarto y último capítulo, realizamos un análisis comparativo de la figura del *phishing* en nuestro país con relación al derecho penal brasilero, paraguayo, colombiano, peruano y español que tratan esta temática, resultando que no hay en todas las legislaciones referidas el mismo avance legislativo. En el caso puntual de España, Paraguay y Brasil directamente no está regulada la suplantación de identidad de la persona en sus ordenamientos jurídicos, confirmando que no existe un tipo penal específico, y que encuadran a esta actividad dentro de las defraudaciones o estafas tradicionales y le aplican la pena destinada a estas figuras penales; cuestión que se entiende vulnera el principio de legalidad conforme al derecho argentino.

En cambio en el caso concreto de Colombia y de Perú, es notable el grado de avance y de la técnica legislativa que han efectuado sobre la suplantación de identidad, pues se encuentra definido en sus códigos penales cuál es el tipo delictivo que la regula como conducta delictiva y cuál es la especie de pena que le corresponde al *phishing*, siendo considerado en estos países como un delito del derecho criminal, ajustándose a lo reglado por el mencionado principio penal de legalidad que opera en nuestra Constitución y tratados con jerarquía constitucional como garantía del debido proceso que debe ser dirigido regularmente por los magistrados, quienes están obligados en cada caso que llega a su conocimiento a su aplicación efectiva y en claro respeto a lo ordenado por la ley suprema.

Referencias bibliográficas.

I) Doctrina:

a) Libros:

1. Tobares Catalá, G. y Castro Argüello, M. (2009). *Delitos informáticos*. Córdoba: Advocatus.

2. Lucero, P. y Kohen A. (2010). *Delitos informáticos*. Buenos Aires: D y D S.R.L.

3. Palazzi, P. (2016). *Delitos Informáticos en el Código Penal.* Ciudad Autónoma de Buenos Aires: Abeledo Perrot.

4. Lascano (h), C. et. al. (2.005). *Derecho Penal – Parte General*. Córdoba: Advocatus.

5. Nuñez, R. (1999). *Manual de Derecho Penal – Parte General*. Córdoba: Marcos Lerner Editora Córdoba.

6. Atienza, M. y Ruiz Manero, J. (2006). *Ilícitos Atípicos.* Madrid: Editorial Trotta.

7. Zaffaroni, E. (2002). *Derecho Penal – Parte General.* Buenos Aires: Ediar.

8. Zaffaroni, E. (1981). *Tratado de Derecho Penal – Parte General – Tomo III.* Buenos Aires: Ediar.

b) Ponencias.

1. Riquert, M. (2.010). *Legislación contra la delincuencia informática en el Mercosur*, organizado por las 1as. Jornadas de Profesores de Derecho Penal del MERCOSUR, en la Universidad Nacional de Mar del Plata, Mar del Plata, Octubre/2006.

2. Belisario Méndez, A. (2014). *Análisis de métodos de ataques de phishing,* realizado para la Universidad de Buenos Aires, Departamento de Ciencias Exactas y Naturales e Ingeniería, Buenos Aires, 2.014.

3. Temperini, M. (2.012). *Suplantación de identidad digital como delito informático en Argentina*.

4. Piqué, M. (2012). *Principio de legalidad y retroactividad*, Convención Americana de Derechos Humanos y su Proyección en el Derecho Argentino, organizado por la Universidad Nacional de Buenos Aires, Buenos Aires, 2.012.

5. Instituto Nacional de Tecnologías de la Comunicación (2.007). *Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing,* León, España, Octubre/2.007.

II) Legislación:

a) Internacional:

1. Convención Americana sobre Derechos Humanos. Art. 9.

2. Pacto Internacional de Derechos Civiles y Políticos. Art. 15.1.

3. Declaración Universal de Derechos Humanos. Art. 11.2

4. Convención sobre los Derechos del Niño. Art. 40.2.

5. Código Penal de Paraguay. Arts. 188 y 189.

6. Código Penal de Colombia. Arts. 269 – G y 269 – H.

7. Código Penal de España. Art. 248 incs. 1º y 2º.

8. Ley de delitos informáticos de Brasil Nº 12.377:

– modificatoria de los arts. 154 A – y 154 B – del Código Penal de Brasil.

9. Ley de delitos informáticos de Perú Nº 30.096:

– incorporación del art. 9 del Código Penal de Perú.

b) Nacional:

1. Constitución Nacional – Ley Nº 24.430. Arts. 18 y 75 inc. 22.

2. Código Penal Argentino – Ley Nº 11.179. Art. 2.

3. Ley de delitos informáticos de Argentina Nº 26.388:

– Art. 1: modificatorio del art. 77 del Código Penal Argentino.

– Art. 2: modificatorio del art. 128 del Código Penal Argentino.

– Art. 3: modificatorio del epígrafe del Capítulo III, del Título V, del Libro II del Código Penal Argentino.

– Art. 4: modificatorio del art. 153 del Código Penal Argentino.

– Art. 5: incorporación del art. 153 bis del Código Penal Argentino.

– Art. 6: modificatorio del art. 155 del Código Penal Argentino.

– Art. 7: modificatorio del art. 157 del Código Penal Argentino.

– Art. 8: modificatorio del art. 157 bis del Código Penal Argentino.

– Art. 9: incorporación del inc. 16 del art. 173 del Código Penal Argentino.

– Art. 10: incorporación del 2º párrafo del art. 183 del Código Penal Argentino.

– Art. 11: modificatorio del art. 184 del Código Penal Argentino.

– Art. 12: modificatorio del art. 197 del Código Penal Argentino.

– Art. 13: modificatorio del art. 255 del Código Penal Argentino.

– Art. 14: derogación del art. 78 bis y del inc. 1º del art. 117 bis del Código Penal Argentino.

4. Proyecto de ley D. 4643/2.010 sobre suplantación de identidad:

– Art. 1: incorporación del art. 139 ter del Código Penal Argentino.

5. Proyecto de ley S. 2257/2.011 de suplantación de identidad:

– Art. 1: incorporación del art. 157 ter del Código Penal Argentino.

6. Proyecto de ley S. 1312/2.012 de suplantación de identidad:

– Art. 1: incorporación del art. 138 bis del Código Penal Argentino.

III) Jurisprudencia:

1. CNC Penal. Sala VII. "Castellini, Alfredo J. y otros". (Sentencia de fecha: 30/03/2005).

2. CNC Penal. Sala IV. "T., C. R. y otro". (Sentencia de fecha: 02/07/2.007).

4. CNA Comercial. Sala D. "Bieniauskas, Carlos c/ Banco de la Ciudad de Buenos Aires". (Sentencia de fecha: 15/05/2.008).

5. CNA Criminal y Correccional. Sala VI. "G.R. y otro s/ procesamientos". (Fallo de fecha: 03/08/2.010).

6. CFC Penal. Sala III. "C. P. A. s/ recurso de casación". (Sentencia de fecha: 16/06/2.015).

7. CNC Penal. Sala II. "Coronel, Orlando". (Sentencia de fecha: 05/10/2.004).

8. CN Criminal y Correccional. Sala III. "Iglesias, Carlos M.". (Sentencia de fecha: 04/06/1.992).

9. SCJ Mza. Sala II. "Fiscal c. Russo Beraldo". (Sentencia de fecha: 19/08/1.997).

10. C Criminal y Correccional Nº 24. "M. s/ Hurto". (Sentencia de fecha: 19/07/1.995).