UNIVERSIDAD DE CHILE
ESCUELA DE POSTGRADO
FACULTAD DE DERECHO

ALCANCE INFRACCIONAL DE LAS BOTNETS UTILIZADAS PARA LA COMISIÓN DE DELITOS CONFORME A LA ACTUAL LEGISLACIÓN CHILENA

MEMORIA PARA OPTAR AL GRADO DE
MAGISTER EN DERECHO Y NUEVAS TECNOLOGIAS

DANIC MALDONADO CÁRCAMO

Director de Tesis
Daniel Álvarez Valenzuela

Codirector de Tesis
Salvador Millaleo Hernández

SANTIAGO DE CHILE
MARZO, 2017

INDICE

RESUMEN

La presente tesis, tiene por objeto dar a conocer una visión general, respecto del alcance infraccional que posee la utilización de códigos maliciosos que, para este caso en particular, se centró en la utilización de botnets, para la comisión de delitos en el ámbito informático.

En ese contexto, se presentan importantes desafíos desde lo técnico para generar contramedidas que sean eficientes a la hora de mitigar las amenazas en este campo, pero también existe otro desafío muy relevante que dice relación con la problemática que se presenta al juzgador al momento de la persecución penal, a la delincuencia del mundo informático.

En esa misma orden de ideas, se hace preciso considerar la normativa vigente que establece sanciones para aquellas acciones que atenten contra sistemas transaccionales, y los datos contenidos en éstos, dado que ya se han cumplido dos décadas que dicha normativa no ha sufrido ninguna actualización, lo que favorece que determinadas acciones no puedan ser perseguidas adecuadamente porque no cumplir el tipo penal, o bien, no puedan ser castigadas porque derechamente no existe norma para tales efectos.

Considerando el reciente lanzamiento de la política nacional de ciberseguridad, y la adhesión de Chile, al convenio de Budapest, marcaran sin duda, un verdadero punto de inflexión, a fin de subir los actuales estándares a niveles internacionales, así como la generación de redes que permitan unificar los esfuerzos en materia de persecución penal de los delitos informáticos, considerando que su alcance no reconoce fronteras, por lo que, de no mediar un trabajo mancomunado a nivel de cooperación internacional, y la homogeneización de los cuerpos legales, no se podrá dar una lucha férrea, a los delitos informáticos a nivel global.

INTRODUCCION

Desde el principio, la humanidad se vio obligada a satisfacer en primer lugar, sus necesidades más básicas, sin duda, se las debió ingeniar para poder utilizar lo que la naturaleza ofrecía para su propio beneficio, y poco a poco comenzaron a desarrollar sus propios inventos, que de alguna manera fueron constituyendo el desarrollo de la técnica como medio también de sobrevivencia, lo que de alguna manera fue decidiendo el destino de la humanidad, hasta la invención de la agricultura que en definitiva cambió los destinos de la economía mundial, pasando de una economía con mercado a una economía de mercado.

En la actualidad, podemos observar que la tecnología diariamente está generando en nuestras vidas, cambios vertiginosos, gracias a su continuo y cada vez más rápido desarrollo. Una muestra de ello, es la gran red de redes, que se ha transformado en una verdadera autopista por donde transitan miles y miles de paquetes de información que están al acceso de un sólo clic, probablemente muchos de los desarrollos tecnológicos que hoy conocemos, en algún momento de nuestra historia, se encontraban en el plano de la ciencia ficción, pero que hoy en día se han convertido en parte de la realidad.

Probablemente, quienes dedicaron gran parte de su vida, a la invención de nuevas tecnologías para ser dispuesta al servicio de la vida humana, lo hicieron sobre la premisa de que ellas serían utilizadas sólo para fines que vayan en beneficio de toda la sociedad, sin embargo, es muy probable que no hayan considerado una dimensión negativa respecto de la utilización de las mismas, para fines que van en contra del orden establecido y que finalmente terminan causando algún daño a la sociedad.

En ese sentido, y como es de conocimiento general, no sólo se ha utilizado el ingenio para la creación de tecnología para propósitos positivos, sino también, hoy en día existe una verdadera industria dedicada al desarrollo de tecnología que busca derechamente quebrantar los marcos normativos existentes en las

naciones, para la obtención de algún tipo de reditúo que únicamente va en directo beneficio de unos pocos, pero que en la ejecución de los mismos, pasan a lesionar los derechos de otros.

Actualmente, podemos observar un crecimiento importante en términos de la utilización de la tecnología para fines relacionados con la delincuencia tradicional, la guerra electrónica o el ciberterrorismo, en ese sentido, las naciones se han visto obligadas a generar un espacio para la discusión y el análisis, apuntada a intentar enfrentar esta nueva forma de quebrantamiento del orden establecido a todo nivel, ya que hace algunos años nos encontramos frente a la presencia de la denominada delincuencia informática.

La presente tesis, se centra en el análisis, desarrollo y utilización de aplicaciones con fines maliciosos en términos de su funcionamiento, y cómo se han transformado en una amenaza muy poderosa en el último tiempo, de las cuales pareciera ser que existen medidas de mitigación sólo en los casos más sencillo, sin embargo, existen incluso en el mercado otras soluciones informáticas, que sencillamente gozan de mecanismos que las hacen prácticamente indetectables e indestructibles, produciendo daño en términos de seguridad, la pérdida de información, dinero e incluso la puesta en riesgo de aquellos servicios que resultan vitales para la vida humana. Específicamente nos centraremos en la utilización de Botnets para la comisión de delitos.

Desde la dimensión técnica, se buscará explicar en qué consiste una Botnet, los tipos existentes, y cómo funcionan, de tal manera de poder comprender su operatoria desde el punto de vista técnico, de tal manera de lograr una comprensión adecuada de este tipo de desarrollo que posee como objetivo principal su utilización para fines maliciosos.

Por otra parte, se plantea poder conocer el alcance infraccional que puede alcanzar la utilización de una Botnet, de acuerdo al marco normativo existente en nuestro país, sin antes por supuesto de someter a un análisis del estado del arte, respecto de la misma área pero a nivel internacional, de tal manera, de poder hacernos una idea del estado situacional, y ver cómo opera el control vía el derecho de esta nueva y cada vez más desarrollada área del crimen.

Por último, a partir del cruce de la dimensión técnica y la dimensión normativa existente, poder conocer el escenario al cual nos enfrentamos en materia del avance tecnológico desarrollado con fines criminales en la actualidad y la importancia de regular y desarrollar políticas que permitan mitigar o bien controlar en parte este fenómeno creciente, siempre con miras a proteger el acceso a la información y la privacidad de las personas.

DESCRIPCIÓN DE LOS OBJETIVOS DEL PROBLEMA DE INVESTIGACIÓN

Objetivo General

Conocer el alcance infraccional que posee la utilización de botnets, en la comisión de delitos informáticos y computacionales, conforme la legislación vigente en nuestro país y la casuística.

Objetivos Específicos

Conocer que es una *Botnet* desde su perspectiva técnica y su incidencia en la criminalidad informática.

Conocer el marco infraccional en el uso de las botnets, en la comisión de delitos tanto informáticos como computacionales.

Obtener una aproximación del fenómeno tanto desde lo técnico y lo legal, aplicado a un caso real, que permita vislumbrar la actual realidad en la que nos vemos enfrentados.

CAPITULO I

1. LAS BOTNET EN EL CONTEXTO DE LA DELINCUENCIA INFORMÁTICA

1.1. Generalidades

En la actualidad, para nadie es un misterio que la informática se ha introducido prácticamente en todas las áreas del quehacer humano, y conforme se va desarrollando la tecnología es posible apreciar que también ha ido modificando la forma en la que se venían haciendo las cosas tradicionalmente. La baja de los costes tanto en el hardware como el software, en conjunto con la masificación del acceso a internet, han generado un espacio propicio no sólo favorable para afianzar el proceso de democratización de la información sino para el desarrollo de un verdadero nicho para la realización de acciones de carácter lesivas.

Por otro lado, el desarrollo económico mundial ha impulsado la creación de tecnologías cada vez más compactas, atrás han quedado esos inmensos aparatos que carecían de toda opción de portabilidad, y con capacidades de almacenamiento bastante limitadas. En la actualidad nos encontramos frente a una realidad que ha cambiado vertiginosamente y la miniaturización de la parte física de los elementos computacionales, así como el aumento de la capacidad de almacenamiento es cada vez más común, viniendo a favorecer la consolidación de la denominada sociedad de la información[1], la que está produciendo día a día volúmenes gigantescos de conocimiento que demandan mayor espacio de almacenamiento, encontrándonos en la era del bigdata.

La carretera indiscutible por donde transita toda la información disponible, es claramente Internet, y existiendo además cierta apariencia de anomia en la

[1] El término «Sociedad de la Información», fue acuñado por el sociólogo y profesor japonés Yoneji Masuda, quien la definió como: «crece y se desarrolla alrededor de la información y aporta un florecimiento general de la creatividad intelectual humana, en lugar de un aumento del consumo material». [Masuda, 1994]

misma, genera una sensación de libertad total, pero que algunos han comprendido como un espacio para el libertinaje, ya que es posible acceder a cualquier tipo de información tanto como para hacer el bien, pero también para hacer el mal. A lo largo de la historia de la humanidad, es posible observar episodios terribles que han atentado contra la sociedad civilizada. Eso de alguna manera nos da entender que la maldad pareciera ser inherente al ser humano, y que independiente de los diferentes mecanismos de control existentes, siempre hay y habrá quienes estén dispuestos a quebrantar ese orden acordado para el tranquilo desarrollo de una vida en sociedad.

En ese sentido, la informática no ha quedado exenta de aquellas acciones que se apartan de las reglas. Probablemente porque ofrece la posibilidad de llevar a cabo acciones de carácter delictivas, gozando de niveles de anonimato bastante altos, y además pudiendo estar a kilómetros de distancia de la víctima al momento de la ejecución de un hecho punible, lo cual representa además cierto nivel de seguridad, debido a que el riesgo de exposición para el delincuente informático, es bastante bajo. Por eso la delincuencia informática ha presentado un crecimiento explosivo en todo el mundo, porqué en sus inicios estuvo motivada mayormente por personas que más bien eran autodidactas, quienes sin comprender muy bien los principios propios del quehacer informático, y mediante el ensayo y el error, lograron sortear la poca o nula seguridad de las primeras décadas del desarrollo tecnológico.

1.2. ¿Qué es una *Botnet*?

Actualmente el término *Botnet*, está siendo usado de manera recurrente entre los oficiales de seguridad, dado que han sido identificadas entre las amenazas más importantes que se presenta para la gran red de redes en el último tiempo, enmarcándose dentro de las amenazas persistentes avanzadas. Existiendo un mercado creciente, que ofrece el desarrollo de herramientas específicas

conforme a los requerimientos que formulen aquellos que se dedican a perpetrar acciones de carácter delictivo, y que para dichos fines utilizan la tecnología existente. Al parecer su capacidad, de hacerse invisible frente a las barreras de protección ya sean físicas o lógicas, está dada fundamentalmente por el conocimiento y el coste asociado al desarrollo de la misma.

En general cuando se habla de una *Botnet*, en la literatura es posible apreciar que se hace alusión a una palabra compuesta, por una parte por la palabra *Bot*, correspondiente al diminutivo de *Robot*, y por otra parte por la palabra *Net*, que hace alusión a *Network*, palabra proveniente del inglés, que hace referencia a una red, la cual corresponde a un conjunto de elementos organizados para un propósito determinado, en términos prácticos una *Botnet* es en sí, una especie de ro*bot* diseñado para operar sobre una red, la cual contiene una serie de instrucciones específicas para ejecutar de acuerdo a lo que requiera el *bootmaster* o administrador.

En el mundo informático, los virus han existido desde muchísimos años atrás, sin embargo, la utilización de *botnet*s para tomar control de grupos de computadores, se hizo presente recién en el siglo XXI, y en términos más coloquiales se les ha acuñado como el control remoto de los ciberdelincuentes, dado el poderío que éstas poseen. Debido a que físicamente es muy complejo poder tener acceso a sistemas computacionales que sean atractivos, la solución entre las barreras físicas que separa al ciberdelincuente de su objetivo final, es justamente la utilización de una *Botnet*.

Desde lo técnico, básicamente una *botnets*, está compuesta por dos partes, la primera de ellas, corresponde al panel de control, desde donde es posible operar o administrar aquellas acciones que se desea que ésta ejecute. Y la segunda parte corresponde al servidor, el cual corresponde al programa

informático que posee las instrucciones necesarias para la conexión entre los equipos infectados, y el centro de control administrado por el ciberdelincuente.

Los daños provocados por la utilización de *botnets* en Internet, es hasta ahora difícil de precisar de manera exacta, sin embargo, las estadísticas existentes dan cuenta de que su utilización ha generado serias complicaciones, principalmente en términos técnicos, así como la pérdida de información de suma importancia para grandes empresas e instituciones públicas en general. Lo cual, trae aparejado un desgaste importante que se traduce en pérdida de dinero con la finalidad de revertir los problemas generados por la utilización de éste tipo de solución informática dañina.

Cuando se habla de Malware[2], siempre hace referencia a desarrollos que poseen un propósito lesivo, toda vez que, su utilización implica el acceso a un determinado sistema de tratamiento de información, evidentemente sin que el propietario de éste, haya manifestado su voluntad, o esté en conocimiento de dicho acceso, ahora bien, refiriéndonos puntualmente a la materia de análisis de la presente investigación, y que corresponde a las *botnet*s, es posible apreciar algunas características principales respecto de su funcionamiento, y que son necesarias describir de manera somera, con la finalidad de mejorar la comprensión en relación al alcance que éste tipo de aplicaciones posee, en relación al presente, y futuro en el marco del desarrollo tecnológico actual del mundo entero.

1.3. Características de una *Botnet*

En términos generales, este tipo de código malicioso, el cual se enmarca dentro de los denominados Malware, poseen varias características que hacen de este tipo de herramientas, sean tan popular por estos días, y que de seguro lo

[2] La palabra **malware** es una abreviatura de «malicious software», y se refiere a todo programa informático diseñado para realizar acciones no deseadas o perjudiciales para el usuario legítimo de una computadora.

seguirán siendo por muchos años más, dado que su concepción está fundada en la denominada informática distribuida.

a. Capacidad de distribución

Las *botnet*s en su concepción tecnológica, aprovechan para su propagación la gran red de redes, y por lo mismo no reconoce un espacio específico, sino su límite está dado fundamentalmente por la distancia hasta donde haya podido llegar internet. Lo cual complejiza su detección desde el punto de vista técnico, así como también, su persecución desde lo judicial, debido a que muchos de los ataques pudiesen estar siendo realizados desde fuera del territorio nacional.

b. Multifuncionalidad

Una *Botnet*, en su programación inicial puede haber sido desarrollada con un determinado propósito, quizás una tarea básica, pero su composición modular, permitiría desde el comando y control central, efectuar actualizaciones con la finalidad de cambiar totalmente su propósito inicial, o bien agregarle nuevas funcionalidades, por lo tanto, la acción más difícil es la infección de una determinada máquina para que se pueda convertir en *zombie*, y pase a formar parte de una red *botnet*. Por lo tanto, es dable señalar que, una *botnet*, no posee un único propósito concreto y que no pueda ser modificado en el tiempo, al contrario, puede ir variando constantemente los objetivos para lo que fue programado.

c. Complejidad

En la literatura relacionada con las *botnets*, es bastante común leer que, poseen una complejidad bastante alta, considerando que sólo para su desarrollo, se utilizan diferentes tipos de lenguajes de programación, y diferentes mecanismos de control central, lo cual viene a configurar un escenario bastante complejo de administrar, por lo tanto, a la luz de los antecedentes, es mucho más

complicado que los malware tradicionales que pudiesen comprometer la seguridad de la información o derechamente dañarla en un sólo acto, a diferencia de una *botnet*, que a partir de la infección de una máquina, se mantiene en el tiempo, esto se asemeja a como si un desconocido pudiese ingresar a mi computadora todas las veces que quiera de manera física cuando el propietario no esté sentado frente al computador, en cambio en este caso, lo hace de manera remota desde cualquier parte del planeta, y sin que siquiera se hayan activados los sistemas de seguridad.

1.4. Usos principales de las *Botnet*

Antes que todo, es preciso señalar que, la informática distribuida ha estado presente, desde ya hace unas décadas, y es muy probable que la creación de las *botnet*s haya nacido a partir de dicha concepto, claramente no obedecían a las funciones a las que se dedican en la actualidad, como toda tecnología siempre busca convertirse en una solución frente a problemáticas que se puedan presentar a nivel tecnológico, sin embargo, siempre existe la posibilidad cierta, de que sean utilizadas con fines criminales.

En términos generales, en sus inicios muchas de estas herramientas sirvieron para generar una red de computadores como por ejemplo para la utilización de un telescopio, dado que para aumentar su capacidad de procesamiento requería de una gran capacidad de máquinas, situación que mediante este tipo de aplicaciones era posible que personas comunes y corrientes pudiesen facilitar sus computadores conectados a través de una *botnet* para aprovechar su procesador y así aumentar la capacidad de los mismos al momento de utilizar un telescopio por parte de alguna comunidad científica.

En relación al desarrollo de una *botnet*, es dable señalar que, existen variados métodos partiendo por los diferentes lenguajes de programación existentes,

tales como: PHP, Python, C/++, Perl y Java, pero independiente del tipo de lenguaje de programación utilizado para su creación, es posible identificar algunas etapas bastantes comunes en el flujo de vida útil de este tipo de redes.

a. Lo primero que debe hacer el *botmaster* o administrador de una red *botnet*, es planificar los objetivos que perseguirá su malware, así como también el mecanismo mediante el cual comandará y controlará la misma, incluso existen en algunos casos más desarrollados y avanzados que hasta pueden definir el área geográfica donde va a operar la *botnet*, de tal manera que, no salga de la zona programada, como mecanismo de control, cuando se trata de algún ataque muy sofisticado y con un blanco muy específico, cómo un territorio determinado, ya sea una ciudad, o un país, y así con ello evitar que se propague fuera de los límites iniciales establecidos conforme al objetivo de ataque.

b. En un segundo paso, deberá contar con un malware, para poder infectar las máquinas que convertirá como parte de su red, en este caso tendrá tres opciones, la primera estaría por el desarrollo de una *bot* propia, la segunda por el arriendo, y la tercera por la compra de una, hoy en día, existe un mercado que no podría ser definido de incipiente, pero claramente, cada vez va tomando mayor protagonismo, dado que, conforme se desarrolla el mundo de internet, mayor interés se va desarrollando en las posibilidades que ofrece para quienes les gusta hacer dinero fácil a partir de la utilización de la tecnología como un medio para la comisión de delitos, y en gran parte estimulados por motivaciones de índole económicas.

c. El tercer paso, deberá definir una estrategia para poder esparcir su *botnet*, para ello existen variados métodos; entre los que se pueden apreciar las típicas vulnerabilidades que pueden presentar algunos sitios web, así como también la distribución de spam, y quizás lo más usado en el caso de

objetivos menos sofisticados y menos ligados al mundo tecnológico, es el concepto de ingeniería social, la cual consiste en términos bien generales, en crear un ambiente muy similar a las condiciones reales en las que suele operar la víctima, en acciones rutinarias como las transacciones en un banco, el cobro por algún monto adeudado, o bien alguna información de algún suceso mediático y relevante que pudiese estar ocurriendo ya sea a nivel nacional o internacional, lo cual generalmente va en algún tipo de archivo adjunto a un correo electrónico, y la victima frente al contenido que se le ofrece y sin mediar mayor análisis, dan clic y sin darse cuenta ha descargado el *bot* en su máquina, la cual inmediatamente intentará establecer contacto con su comando central, sin que los mecanismos de seguridad del equipo de la víctima, haya sido capaz de alertar dicha situación.

Es dable precisar que, el desarrollo de las *Botnet*, en sus inicios no fue concebida como una herramienta para ser utilizadas en acciones que atenten con los derechos establecidos como se ha podido apreciar en la última década en donde la criminalidad cibernética ha aumentado considerablemente mediante la utilización de sofisticadas herramientas, que claramente están muy distante del conocimiento que poseen las personas que se convierten en víctimas, por lo que, frente a ello quedan en una total indefensión una vez que ya han sido infectados.

Los ciberdelincuentes utilizan las *botnet*s, para infectar una gran cantidad de equipos, y estos equipos contaminados conforman una red conocida como red *zombie*, dado que cuando un equipo ha sido infectado, pasan a formar parte de la red que controlada quien administra una determinada *botnet*.

En la actualidad las *botnets*, poseen varios objetivos, ya sean aislados uno de otro, o bien, algunos que son requisitos para realizar otras acciones, en ese sentido podemos indicar aquellas acciones más comunes que figuran tras el desarrollo de una herramienta de la naturaleza de la presente investigación.

Tabla 1

Usos principales de una Botnet

Servicios de Envío	Una de las funcionalidades que poseen las *Botnet*, está el envío de spam, software espías, o virus en general.
Acceso indebido para robar información	Otra funcionalidad importante, es la de robar información privada y personal, así como también información sensible, como número de tarjetas bancarias, usuarios y claves de acceso a cuentas bancarias, entre otras.
Denegación de Servicio DDoS	En general los ataques de denegación de servicio (DDoS), es bastante común como mecanismos de protestas, o bien sencillamente para dar de baja determinados servicios, con lo cual colocan en jaque el funcionamiento de determinados servicios, lo cual puede ser tanto desde el territorio nacional como internacional, ya sea sólo con el objetivo de protestar, o bien podrían eventualmente solicitar un rescate a cambio de liberar los portales web atacados.
Fraudes electrónicos en general	En último tiempo, se ha utilizado bastante para abultar o aumentar las visitas a determinados sitios web, lo que sin duda, provoca que se aumenten los cobros por concepto de publicidad, por mencionar alguno, este fenómeno es conocido como: "fraude clic".

En la presente tabla se puede apreciar aquellos usos más comunes en la actualidad, en la que son empleadas las *botnet*.

1.5. Tipos de comandos y control de una *Botnet*

Para poder administrar una *Botnet*, es necesario contar con un cliente, mediante el cual finalmente se podrá establecer contacto con todos aquellos equipos computacionales que forman parte de una determinada red *botnet*. En términos simples, cuando hablamos de una red *botnet*, nos referimos a todos aquellos equipos que fueron infectados, los cuales serán controlados mediante la *Botnet* por parte de su administrador. Dichos equipos son conocidos comúnmente como *zombies*, algunas veces también son llamados *drones*.

Existen variadas formas de administración de una *botnet*, pero nos enfocaremos en aquellas más tradicionales o las que comúnmente son utilizadas por los delincuentes informáticos, para llevar a cabo acciones con propósitos delictivos, entre las cuales encontramos los siguientes comandos y control:

a. IRC (*Internet Relay Chat*)

Es un protocolo de comunicación, creado en la década de los ochenta, y que posee como finalidad principal establecer comunicación entre dos o más personas, a través de mensajería escrita. Su nombre corresponde a la abreviación de *Internet Relay Chat*, ésta forma de comunicación goza de una popularidad importante a nivel internacional. En términos prácticos, para poder entablar una conversación con otra persona, en primera instancia es necesario contar con una aplicación del tipo IRCd (Servidor de IRC), el cual nos permitirá gestionar los canales de conversación. En dichos canales, para identificarse es necesario que un usuario siempre comience su nombre de usuario con un & o #. Un aspecto importante que favoreció su popularidad, es que este tipo de aplicaciones son distribuidas de manera gratuita.

Ahora bien, cuando este tipo de aplicaciones es utilizada para comunicarse con los equipos *zombies*, estos pasan a conformar una verdadera red privada, y mediante un determinado canal definido por su administrador, es posible establecer la comunicación entre éste y las máquinas infectadas, evidentemente no existirá una comunicación como tradicionalmente se realiza a través de este tipo de aplicaciones, sino más bien, las máquinas infectadas, serán agregadas al canal que ha establecido el administrador de la misma, quien mediante comandos, le indicará las instrucciones a las máquinas infectadas y el *bot*, que se encuentra alojado en la máquina infectada, tomará ese comando, lo interpretará, lo procesará y ejecutará la instrucción recibida, conforme a la programación inicial para lo cual fue diseñada, por ejemplo; efectuar tareas de capturas de pantallas de lo que el usuario esté realizando, grabar voz, o bien hacer un video utilizando la cámara web que disponga el equipo infectado.

En la actualidad, el uso de este tipo de aplicaciones para propósito de índole fraudulentos, está bajando su uso, probablemente porque una de las desventajas que presenta, es que los comandos que son enviados a las máquinas infectadas, viajan sin cifrar, lo que sin duda, deja una puerta abierta para su rastreo por parte de los equipos encargado de hacer cumplir la ley de cada país.

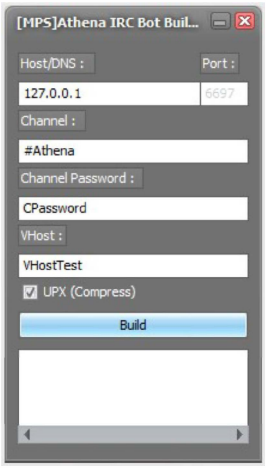

Figura 1. Comando y Control de la botnet, denominado Athena, vía IRC.

b. Panel Web

Otra forma que ha ganado bastante protagonismo en este último tiempo, para poder administrar una *botnet*, es la utilización de un panel de acceso vía web, una de las primeras ventajas que podríamos visualizar, sería la de evadir los cortafuegos , dado que en general este tipo de elementos, están diseñados para permitir la conexión web, por lo que aprovechan esta situación para que mediante este protocolo el *bot*, se pueda comunicar con su comando central, lo cual de alguna manera dificulta la posibilidad de ser detectadas. Así también, el protocolo HTTP, permite cifrar el tráfico, lo que viene a facilitar en parte el anonimato del administrador de una *botnet*.

A continuación, un acceso a un panel de control central mediante web:

Figura 2. Comando y control de una botnet vía web.

c. Programas Peer to Peer

Otro tipo de administración de una *botnet*, es también mediante programas peer to peer[3], la cual presenta una diferencia respecto de la arquitectura del tipo cliente-servidor, como son las otras anteriormente descritas, que poseen un control central, justamente en el caso de las aplicaciones del tipo peer to peer, desaparece este concepto de centralización, ya que no existen los clientes o servidores fijos, en definitiva las máquinas son consideradas todas exactamente iguales, y se comunican con aquellos equipos que se encuentran registrados en su lista. Por lo tanto, quien administra la *botnet*, puede en el momento que desee, utilizar cualquiera de las máquinas *zombies*, como comando y control, por ejemplo; para efectuar alguna actualización o enviar algún comando, lo cual se traduce en una verdadera ventaja, ya que al operar bajo esta dinámica también dificultaría su neutralización. Ahora bien, a pesar de su ventaja comparativa respectos de las demás formas de control y comando, esta no se ha masificado quizás como se podría pensar, debido fundamentalmente por su complejidad que presenta en su mantención y distribución.

[3] Panda Cloud Internet Protección, ***¿Qué es Peer – to – Peer (PSP)?***, «Las tecnologías 'peer to peer' (P2P) hacen referencia a un tipo de arquitectura para la comunicación entre aplicaciones que permite a individuos comunicarse y compartir información con otros individuos sin necesidad de un servidor central que facilite la comunicación.»

1.6. El negocio tras las *Botnet*

Tal como hemos podido analizar, hoy en día las *botnet*s definitivamente están siendo desarrolladas con fines para la comisión de delitos ya sean «computacionales» o bien «informáticos», y en ese mismo sentido, su crecimiento puede obedecer a dos situaciones por un lado podría estar dada por el arrendamiento y, por otro lado, por la venta de este tipo de herramientas.

Hoy en día las *botnet*, representan un verdadero negocio, es posible encontrar verdaderas empresas dedicadas al desarrollo de las mismas, en la actualidad, se puede arrendar una *botnet*, para enviar correos masivos cerca de los USD$2000 dólares por mes. En definitiva, su precio está dado por la cantidad de equipos infectados, la mayoría de estos programas maliciosos, provienen de países de habla inglesa. Existen *botnet* más pequeñas que bordean los USD$700 dólares. Existió una red denominada *Shadow*, la que fue creada y liderada por un ciberdelincuentes holandés, alcanzando a convertirse en una de las *botnet* que fue vendida en alrededor de cuarenta mil dólares americanos.

Actualmente e independiente sí se arrienda o se vende, los propósitos pueden ser variados, desde un ataque DDoS, envío de spam, instalación de software publicitario y malicioso, robo de datos confidenciales, *phishing, pharming, spam* de búsqueda, entre otras.

CAPITULO 2

2. ESTADO SITUACIONAL DE LA CRIMINALIDAD INFORMÁTICA

2.1. Generalidades

La utilización de la tecnología en hechos criminales, se ha visto incrementada a partir del desarrollo de código malicioso cada vez más sofisticado. Hoy en día, ya no es como en los inicios donde prácticamente participan personas que no tenían formación formal en el ámbito tecnológico, y que sus actividades se enmarcaban en un especie de aprendizaje por ensayo y error, pero en la actualidad la actividad criminal en el ámbito cibernético exige mayor entrenamiento y conocimiento en diferentes aspecto, como plataformas informáticas, sistemas operativos, lenguajes de programación, bases de datos, entre otros, por lo que exige profesionales o expertos en dichas materias para el desarrollo de códigos maliciosos que son empleados para la cibercriminalidad, por lo que, se han abierto verdaderos mercados que demandan aplicaciones cada vez más sofisticadas para la comisión de delitos, entre las que se cuentan las *botnet*, como herramientas sofisticadas y de alto poder.

Evidentemente, cuando se convirtió en una realidad, la posibilidad de estar conectados desde casi cualquier punto del planeta, lo cual estuvo fundamentalmente dado por la necesidad imperiosa que experimentó la comunidad científica de finales de la década de los sesenta, cuando se enfrentaban a la disyuntiva de cómo poder compartir la información obtenida a partir de sus investigaciones, lo cual sirvió como base para el desarrollo de lo que hoy conocemos como la gran red de redes. Es muy probable que en sus inicios no se haya vislumbrado los alcances a los que llegaría hoy en día, y menos que daría paso a un nuevo espacio para el desarrollo de actividades criminales. Fue así como en la década de los setenta, ya se comenzaron a

conocer algunas instrucciones no autorizadas a diferentes computadoras conectadas en entre la red de los científicos, donde se vieron enfrentados a grandes desafíos para su detección, tal es el caso donde el físico Clifford Stoll[4], debió dedicar largas horas y muchos meses, para detectar las intromisiones en el laboratorio donde trabajaba, con la finalidad de obtener evidencias que permitiera establecer la identidad y responsabilidad que le cabía a quien se encontraba accediendo sin la autorización a la información de muchos servicios tanto públicos como privados en Estados Unidos, y que posteriormente era vendida a otras personas en diferentes países, en algunos casos incluso correspondían a materias que se encontraban bajo reservada o derechamente secretas. En dicha época, sin duda existían muchos menos avances en el ámbito de la informática forense[5], lo cual claramente hacía mucho más difícil la tarea investigativa. Esto es una muestra de que la criminalidad cibernética se desarrolló prácticamente apenas existieron las redes que permitieron enlazar cientos de computadoras alrededor del mundo.

A partir del desarrollo sistemático no sólo de internet, sino de la tecnología en general, los esfuerzos han estado destinados al desarrollo de aplicaciones que han permitido la automatización de cientos de procesos y también ha venido a cambiar la forma en que se hacían las cosas tradicionalmente, dando paso rápidamente a mayores niveles de confianza, conforme se iban utilizando las distintas herramientas tecnológicas que son puesta a disposición de la sociedad, sin embargo, eso ha ido cambiando dado que cada vez los usuarios que se ha convertido en víctimas de algún delito informático, su sensación de seguridad en la red disminuye.

---

[4] Se recomienda la lectura del libro "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage", escrito por Clifford Stoll, un físico estadounidense, astrónomo, experto en computadores, quien participó en la captura del hacker Markus Hess durante los años 1986 y 1987, cuando trabajaba en el Lawrence Berkeley National Laboratory en California.

[5] Se estima que desde el año 1984, la Oficina Federal de Investigación, más conocida por sus siglas en inglés FBI, inició el desarrollo de aplicaciones para el desarrollo de pericias en el ámbito informático.

El desarrollo de una solución informática involucra altos costes, ya sea por el equipamiento físico que pueda requerir, así como lo relacionado con los programas propiamente tal, por lo que muchas veces los esfuerzos están enfocados a dar cumplimiento a los objetivos que persigue dicho desarrollo, pero no siempre se consideran todos los aspectos relativos a la seguridad, probablemente porque no se ha tomado conciencia de la real dimensión de la criminalidad en el ámbito tecnológico, o bien porque los costes de aumentar la seguridad presenta montos en algunos caso bastante altos, si se consideran partidas adicionales que busquen minimizar las vulnerabilidades, siendo justamente esas brechas las que aprovechan quienes se dedican a realizar acciones delictivas utilizando para ello medios tecnológicos.

En ese sentido, también es posible apreciar en algunos casos, la ausencia de una estandarización mínima que permita mitigar en parte determinados ataques, pudiesen ayudar bastante, muchos de ellos, están dirigidos a los usuarios comunes y corrientes, dado que muchas de las brechas utilizadas, van por la vía del engaño o bien se aprovechan del descuido de la víctima, por lo tanto, es de vital importancia la existencia de estándares que permitan contar con un piso en términos de la seguridad informática, y que incluya necesariamente programas de educación a los usuarios. Es dable señalar que, existen registros de los primeros fraudes a bancos en países como Estados Unidos e Inglaterra, a fines de la década de los setenta, donde se aprovecharon justamente de las vulnerabilidades que presentaban los sistemas informáticos de los bancos de esa época.

Conforme al avance de la tecnología, es posible apreciar que los criminales informáticos, dependiendo de las motivaciones que posean, han ido desarrollando técnicas que les permiten cumplir sus actos ilícitos, cada vez de manera más sofisticada, y en ese sentido el derecho se ha hecho cargo en

tratar de establecer cierta categorización general a la multiplicidad de acciones que pueden ejecutarse a través de Internet, y que son de carácter lesivas para sus víctimas. En ese sentido, es posible encontrar literatura que plantea tópicos como el fraude electrónico, el sabotaje informático y el espionaje informático.

En términos generales, es posible apreciar que el actual escenario fundamentalmente se encuentra altamente motivado por el ánimo de lucro. En esa misma lógica podríamos también esgrimir que existen dos grandes grupos de ciberdelincuentes, aquellos que más bien que son autodidactas, y que no poseen una formación formal respecto de la tecnología pero que con práctica diaria y la constante participación con sus homólogos en diferentes partes del planeta, van adquiriendo conocimientos que les permiten realizar determinadas acciones, pero podríamos decir que de alguna manera podrían constituir aquel grupo menos perjudicial en esta cadena delictiva. Dado que existen aquellos que poseen los entrenamientos formales y con niveles altísimos de conocimiento, por lo tanto, son capaces de crear herramientas altamente sofisticadas que permiten hacer prácticamente de todo en el mundo criminal ligado a la tecnología, y que además cuentan con la posibilidad cierta incluso de no ser detectados, es justamente este último grupo que más nos debiese preocupar, toda vez, que constituyen un verdadero mercado para proveer de soluciones informáticas que permiten llevar a cabo desde cualquier parte del mundo, algún acto criminal en el ciberespacio.

2.2. Situación Internacional

En el contexto internacional, las grandes compañías orientadas a proveer soluciones informáticas y que de alguna manera apuntan sus esfuerzos a tratar de prevenir y en otros casos derechamente a reparar el daño causado

provenientes de múltiples amenazas que colocan en riesgo la seguridad de la información que se mantiene bajo procesos informatizados en todo el mundo.

Actualmente es posible conocer la existencia de aquellos países más comprometidos en términos del alojamiento de *botnet*. A continuación una lista confeccionada por Kaspersky Lab[6], que da cuenta de la realidad mundial en términos de aquellos países en los que se han detectado mayor cantidad de víctimas de tipo de soluciones informáticas utilizadas en la criminalidad informática, destacándose la utilización de *botnet* en ataques de denegación de servicio.

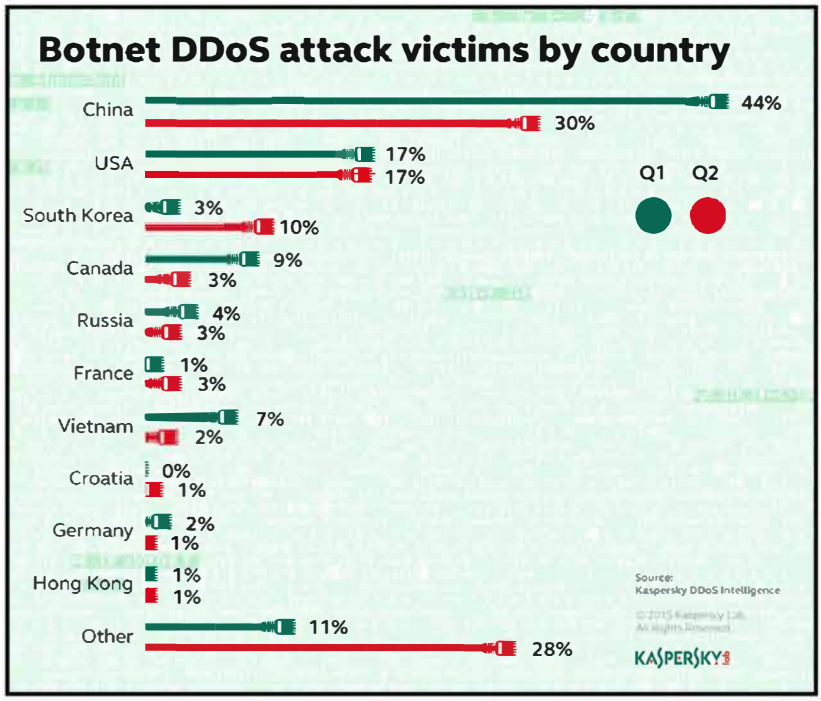

Figura 3. Cuadro que muestra aquellos países con mayor cantidad de ataques de denegación de servicio, donde se utilizaron Botnets, para tales propósitos.

[6] Karpersky, es una de las compañías más importantes en el desarrollo de software para diferentes sistemas, en especial es conocido por su antivirus. La cual es de origen Ruso.

Del mismo modo la organización internacional Spamhaus[7], posee como objetivo principal el monitorear fundamentalmente la actividad de *Botnet* a nivel mundial utilizada para el envío de *spam*[8], lo cual se traduce en una vía altamente viable al momento de convertirnos en víctimas, toda vez, que no existe una preocupación por parte del usuario tradicional, a la hora de discriminar entre aquellos remitentes seguros y aquellos que no lo son, no representándose la posibilidad que se podrían convertirse en víctimas de algún delito informático con dar sólo un clic. Por una parte, esta situación podría estar dado por el desconocimiento de la actividad delictual en el mundo cibernético, o bien por gozar de una excesiva confianza frente a la tecnología, por lo cual ven determinados servicios como inofensivos.

Por lo anterior, se hace indispensable que quienes prestan determinados servicios vía web, adviertan a sus clientes los peligros a los que pudiesen verse enfrentados, sino mantienen una actitud alerta, y constantemente informados respectos de las noticias ligadas a la criminalidad cibernética.

A continuación, una gráfica proporcionada por la organización internacional Spamhaus, donde se puede apreciar a fecha cinco de diciembre del año dos mil quince, los altos números de *botnet*, utilizadas para estos fines y los países más afectados por este tipo aplicaciones.

---

[7] Spamhaus, es una organización internacional sin fines de lucro, fundada en 1998, y con sede en Ginebra, Suiza y Londres, dedicada al control de spam a nivel mundial.

[8] Corresponde a correos electrónicos no solicitados, a menudo anuncios, que se envían a través de una red informática a muchos destinatarios. http://www.yourdictionary.com/spam#websters

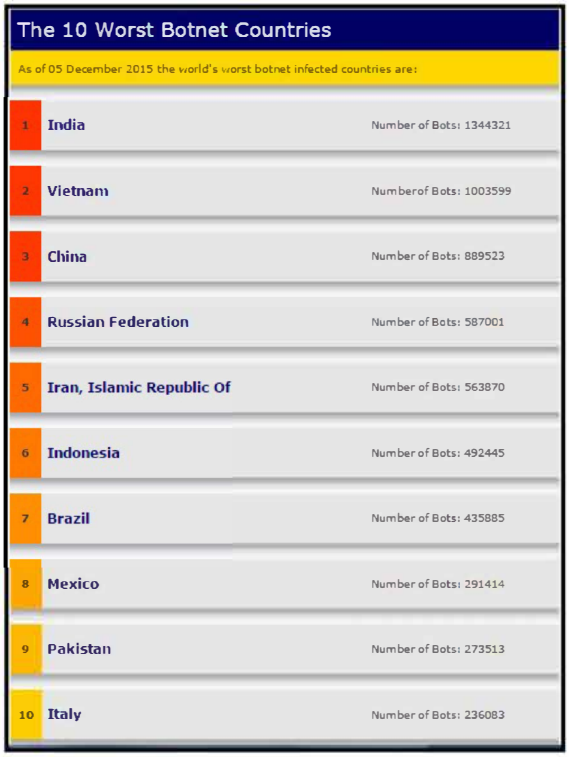

Figura 4. Cuadro que muestra los diez peores países que presentan ataques con *botnet*.

Del mismo modo la Asociación Nacional de Publicista[9], la cual representa a más de seiscientos ochenta empresas de las mil marcas más importantes del mercado mundial, quienes además invierten un total aproximado de doscientos cincuenta millones de dólares americanos en publicidad anual, y que también se ven afectados por el uso de *botnet*, tal como muestra el siguiente gráfico:

[9] ANA (Association of National Advertisers), con asiento en Estados Unidos.

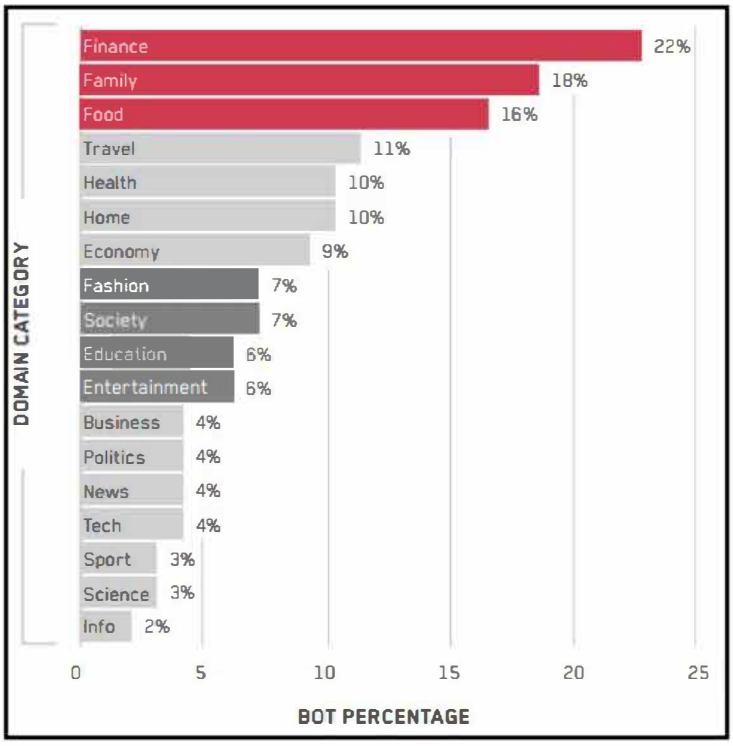

Figura 5. Afectación por *botnet*, separados por rubro de servicio. Fuente: ANA (Association of National Advertisers), The *Bot* Baseline – Fraud in Digital Avertising.

En la gráfica, es posible visualizar que aquellos dominios más afectados, corresponden aquellos relacionados con el ámbito financiero, con un 22 por ciento, le siguen aquellos relacionados con el ámbito familiar, con un 18 por ciento, y el ámbito relacionado con los alimentos, con un 16 por ciento, siendo los tres grandes rubros más afectados con *botnet* que son utilizadas con la finalidad de obtener dividendos económicos, como por ejemplo; el aumentar a través de la utilización de dichas herramientas las visitas a un determinado video publicitario, lo que finalmente se traduce en un mayor desembolso de dinero por parte de las compañías al momento de publicitar sus productos, por supuestas visualizaciones, que finalmente han sido incrementadas de manera fraudulenta. Por lo que estiman que, durante el año 2015, perdieron aproximadamente unos 6.3 millones de dólares por la utilización de *botnet* para defraudar en al área de la publicidad y marketing.

En lo relativo al sabotaje y al espionaje informático, las grandes compañías ligadas al desarrollo de soluciones de tipo informáticas para contrarrestar la creciente expansión de herramientas cada vez más sofisticadas en el ámbito criminal, ya sea buscando obtener algún dividendo o bien causar algún tipo de daño, realizan enormes esfuerzos para poder generar cierto nivel de contención de las amenazas que surgen a cada minuto a nivel mundial, sin embargo, lo indicadores nos hablan de un crecimiento exponencial del cual no se vislumbra un decrecimiento a pesar de todos los esfuerzos realizados a nivel mundial en el ámbito de la seguridad informática.

En la misma línea, dentro de las grandes herramientas desarrolladas altamente sofisticadas, y que dieron mucho que hablar, y por sobre todo respecto de su alto nivel en términos de su capacidad técnica para no ser detectada, como fue Stuxnet y Flame[10]. Hoy en día las autoridades en diferentes partes del mundo han comenzado a preocuparse por este tipo de amenazas, que podrían incluso producir más allá que simplemente un daño económico, sino también pudiesen afectar infraestructura sensible, que finalmente podría llegar a costar vidas humanas, por lo que es necesario aunar esfuerzos para combatir, mitigar o evitar la comisión de delitos, mediante la utilización de medios informáticos.

Hoy sólo basta con una conexión a internet, y con una simple búsqueda nos encontraremos con sitios que ofrecen soluciones del tipo *botnet*, y con precios en algunos casos muy accesibles, evidentemente su costo de alguna manera está directamente relacionado con la capacidad que tenga una determinada *botnet*, tal como se puede apreciar en las siguientes impresiones de pantallas, que dan cuenta de la oferta de las mismas.

[10] Los dos virus más poderosos desarrollados con el fin de ser utilizados en ataques relacionados con la ciberguerra.

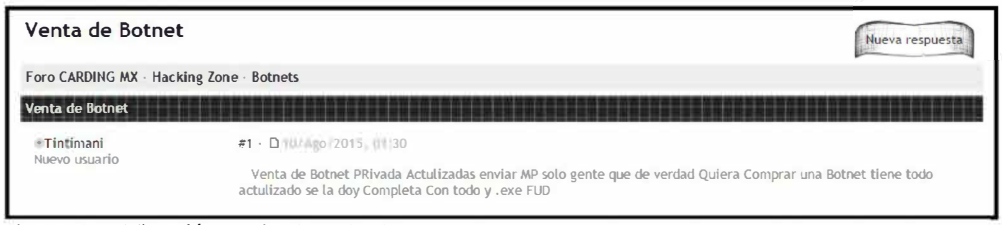

Figura 6. Publicación venta de *Botnet*.
Fuente: http://cardingmx.mforos.com/2106562/11536820-venta-de-botnet/

Pero en general, aquellas herramientas más sofisticadas y orientadas derechamente a la criminalidad cibernética, provienen de verdaderas empresas que han nacido justamente a partir de la existencia de demanda en el campo criminal y que fundamentalmente busca obtener dividendos de índole económicos, por lo que Internet, se ha transformado en la plataforma por excelencia para publicitar sus productos y particularmente bajo la red TOR[11], lo que claramente proporciona seguridad en términos de la privacidad, evitando con ello que las entidades persecutoras en los diferentes países puedan establecer su ubicación y con ello perseguir judicialmente a los responsables.

Cabe hacer presente que, en el caso de las empresas que poseen como principal función dentro de sus operaciones, la de prestar servicios orientados a la detección de diferentes tipos de *malware*, siempre puede existir un gran número de amenazas que no sean detectadas, o bien que son detectadas una vez que ya han cumplido con el objetivo para el cual han sido diseñadas, por lo tanto, no es posible hablar de un cien por ciento de seguridad cuando hablamos de tecnología, si bien es cierto, podemos subir los estándares con el fin de mitigar en parte las amenazas, pero siempre existirá alguna debilidad que pueda ser explotada, en muchos casos corresponden principalmente al usuario, bajo la modalidad denominada ingeniería social[12].

---

[11] La red de Tor, es un grupo se servidores que operan como voluntarios y que permite a las personas navegar de manera anónima. https://www.torproject.org/about/overview.html.en

[12] La ingeniería social, según lo describe Christopher Hadnagy, en su libro «Ingeniería Social el Arte de Hacking Personal», corresponde a: «El acto de manipular a una persona para que lleve a cabo una acción que – puede ser o no – lo más conveniente para cumplir con cierto objetivo. Este puede ser la obtención de la información, conseguir algún tipo de acceso o lograr que se realice una determinada acción.»

Desde el punto de vista internacional, es posible apreciar que la actividad criminal ligada a la utilización de aplicaciones que prácticamente son capaces de hacer de todo en un computador, a miles de kilómetros de manera remota y automatizada, y que además presenta crecimientos exponenciales que acentúan aún más la amenaza latente respecto de convertirnos en víctimas de un delito del ámbito informático, sino se desarrollan determinados protocolos que vengan a favorecer las buenas prácticas, lo cual contribuirá a minimizar los riesgos.

El ciberespacio[13], no sólo genera preocupación en lo relativo a los delitos cibernéticos y/o computacionales, que más bien se encuentran circunscrito a materias de orden de seguridad interna de un país, sino también, acciones ligadas al ciberterrorismo o la ciberguerra[14], lo que involucra necesariamente las fuerzas armadas de cada nación, por lo que, la mirada debe ser muchísimo más amplia cada vez, con el objetivo de someter a análisis la problemática de manera pormenorizada, evaluando desde la infraestructura crítica hasta aquellas situaciones cotidianas que nos pudiesen afectar, debido que también este tipo de aplicaciones maliciosas están siendo utilizadas en actos de ciberterrorismo, o derechamente como armas en el campo de la ciberguerra, de ahí la necesidad de contar con instrumentos adecuados que permitan abordar la problemática, en ese contexto, se puede apreciar que muchos países cuentan con una política nacional de ciberseguridad, por lo que existen normativas internas robustas que permite castigar de una manera más drástica en el caso de la utilización de estas herramientas para fines terroristas por ejemplo. Además, se deberá contar con equipos altamente entrenados en dichas áreas para que puedan combatir este tipo de actos, de lo contrario, se estará colocando en riesgo la seguridad de un país, sino cuenta con los medios

[13] El diccionario de la Real Academia Española, define el Ciberespacio como: «Ámbito artificial creado por medios informáticos.»

para defenderse frente ataques asociados al ámbito cibernético, y que sin duda, existen casos en donde ha significado verdaderas catástrofes.

En esa misma línea, es interesante hacer mención al estudio realizado por la Organización de los Estados Americanos, en conjunto con el Banco Interamericano de Desarrollo[15], que muestra que tan preparados se encuentran los países latinoamericanos, frente a los ataques relacionados con el cibercrimen, pudiéndose observar diferentes niveles de madurez en cada uno de los países analizados, y por lo tanto, existe una disparidad bastante considerable entre ellos, que claramente favorece la proliferación de la criminalidad cibernética, en algunos países se aprecian débiles marcos regulatorios en materia penal, así como también existe ausencia de una política nacional de ciberseguridad, en lo particular, los estudios de esta naturaleza, vienen a reflejar la realidad de los países en materia de delitos informáticos, en general se aprecian cambios, pero no con la misma velocidad que presenta el desarrollo de la tecnología, es importante destacar el esfuerzo, pero sin duda, queda mucho por hacer, tanto a nivel de los gobiernos, de las empresas, organizaciones, y personas en general, de tal manera de poder dimensionar la magnitud de este nuevo espacio virtual, que ha dado paso al desarrollo de actividad criminal, lo cual implica necesariamente un esfuerzo doble por parte de los países de tal manera que sea factible mitigar la utilización de la tecnología con fines delictuales.

---

[14] El ciberespacio, fue declarado por The Economist (19), como el quinto dominio para la guerra, después de la tierra, el mar, el aire y el espacio.

[15] El informe de reciente publicación «Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?» a cargo del Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), se busca conocer los niveles de seguridad en los países latinoamericanos y caribeños. La conclusión en general a la que se llegaron, es que una gran mayoría de los países de la región aún están poco preparados para contrarrestar las amenazas del cibercrimen.

2.3. Situación Nacional

En el caso de nuestro país, no se encuentra ajeno a la realidad que se presenta a nivel internacional, y más aún cuando es una de las economías que presenta los mejores indicadores en el cono sudamericano, contando con un excelente índice en materia tecnológica, en especial lo relacionado con el acceso a internet, lo cual nos sitúa como líderes indiscutido en la región, alrededor de setenta por ciento de la población tiene acceso a la gran red de redes, por lo tanto, existe un espacio propicio para acciones ligadas a la delincuencia informática.

Para una mejor comprensión, y como una forma de dimensionar el fenómeno de la criminalidad cibernética en nuestro país, se solicitó datos estadísticos tanto a la Fiscalía Nacional del Ministerio Público, como a la Brigada Investigadora del Cibercrimen Metropolitana de la Policía de Investigaciones de Chile, para conocer en términos de cifras los delitos ligados al espionaje y sabotaje informático[16], los que se pasarán a detallar a continuación.

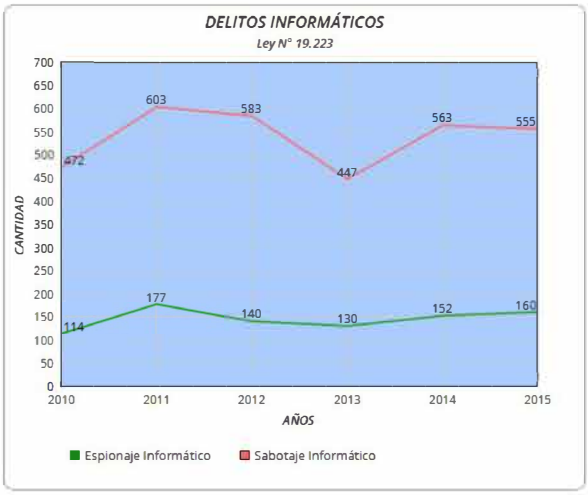

Figura 7. Delitos Informáticos, (Sabotaje y Espionaje) Ley Nº 19.223.
Fuente: Fiscalía Nacional del Ministerio Público

[16] Es dable precisar, que la Ley 19.223, no realiza una distinción literal de los términos espionaje y sabotaje, más bien, dichas acepciones fueron introducidas por los tribunales.

Tal como se puede apreciar en el gráfico anterior, quien lleva la delantera en términos de frecuencia, son aquellas acciones correspondiente al sabotaje informático, fundamentalmente está dado por los accesos indebidos a sistemas de tratamiento de información, así como los datos contenidos en ellos, produciendo derechamente la inhabilitación para su acceso o bien destruyendo o modificando los datos que se encuentren almacenados en los sistemas vulnerados, lo cual finalmente produce un daño de magnitudes para la víctima, y obviamente sin su consentimiento, y en muchos casos sin que este último, pueda siquiera advertir que está siendo víctima de este tipo de delitos.

En la gráfica, es posible apreciar que existen algunos puntos altos, generalmente este tipo de situaciones está dado por la explotación inicial de alguna vulnerabilidad que posteriormente es controlada o erradicada desde diferentes vías, ya sea por la aplicación de una medida paliativa o derechamente por una de índole correctiva para subsanar la problemáticamente del punto de vista técnico. En otros casos, se logra estancar los índices, mediante la persecución penal, ya que en muchos casos, proceden a efectuar la denuncia respectiva mediante los canales formales para tales efectos, y de esa manera se da origen por parte del Ministerio Público, a una investigación que posee como objetivo establecer la dinámica de los hechos de origen delictivos y así poder individualizar el o los responsables, a fin de que por un lado paguen a la sociedad el daño causado, y por otro lado, busca neutralizar la amenaza cibernética para que no continúe con los fines para los cuales había sido desarrollada.

De la misma gráfica, se puede desprender que existen cifras bastantes altas para este tipo de delito que cada día presenta nuevas variables, que hace que el fenómeno no desaparezca sino más se transforme dado que se van desarrollando nuevas técnicas. Y finalmente es posible mitigar en parte o

atacar determinado fenómeno, lo que, en definitiva en algunos casos, hace que las cifras logren reducirse, pero en una mirada al largo plazo, siempre es posible apreciar que posee una tendencia clara hacia el alza, por lo tanto, se encuentra en la misma dirección que los indicadores a nivel internacional.

En relación con aquellas acciones constituyentes de delitos, más comunes en el ámbito de los delitos computacionales, los cuales más bien corresponderían a determinadas acciones delictivas tradicionales pero que finalmente con el avance tecnológico, utilizan dichos medios para concretar determinadas acciones de carácter delictivas. A fin de visualizar la tendencia en dicha área, específicamente aquellas acciones rotuladas bajo el delito de estafa y otras defraudaciones que se comenten utilizando mayoritariamente la técnica conocida como ingeniería social.

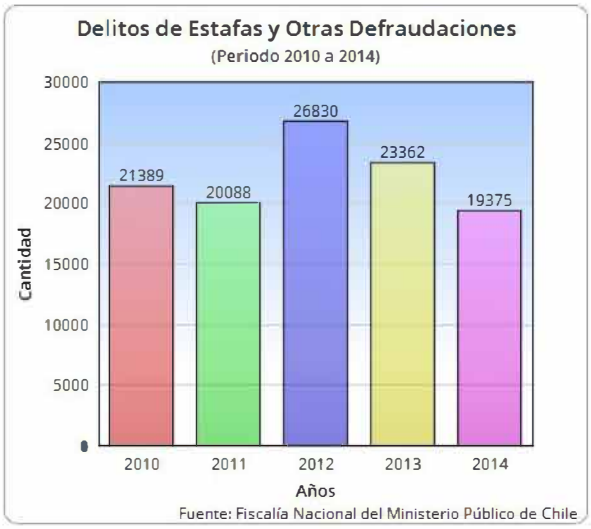

Figura 8. Delitos de Estafas y Otras Defraudaciones
Fuente: Fiscalía Nacional del Ministerio Público de Chile.

En la gráfica precedente, es posible apreciar cifras bastante considerables, lo que da cuenta que, en definitiva, la tecnología es utilizada como un instrumento en la comisión de delitos tradicionales como es el caso de las estafas y otras defraudaciones. En ese sentido, es posible ratificar que claramente la mayor

motivación para la utilización de la tecnología posee un fuerte énfasis en la obtención de dividendos de índole económicos. Y muy en especial, que quién comete el delito puede estar a miles de kilómetros de su víctima, detrás de un grupo delictivo altamente organizado y con la tecnología que le permite llevar a cabo estafas por importantes cantidades de dinero en muy poco tiempo, aprovechándose del anonimato que ofrece la red de internet.

Otro aspecto importante, es la publicación de información de carácter privada, que haya sido obtenida ya sea de manera lícita, o bien a través de algún medio tecnológico, y que posteriormente por diversas motivaciones son publicadas principalmente en redes sociales, con la finalidad de causar algún tipo de daño a su propietario. En muchos casos las publicaciones de información personal, va asociada a dichos ya sean de carácter injuriosos o calumniosos.

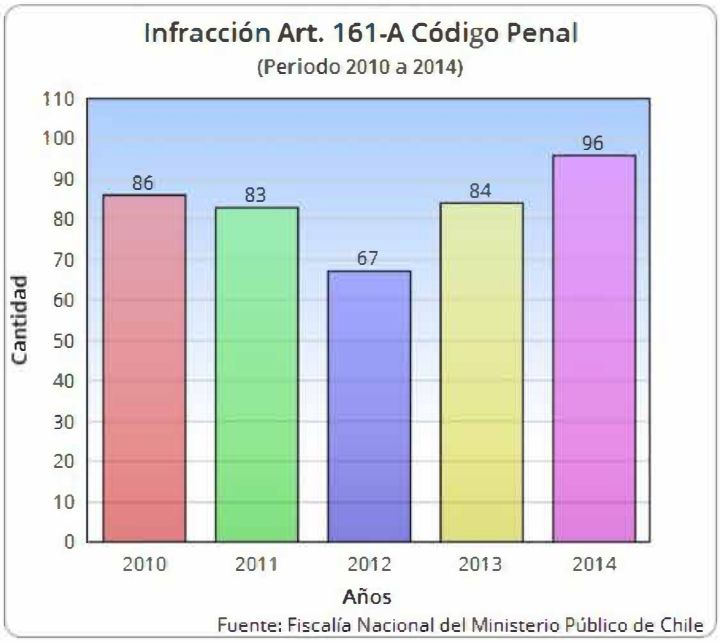

Figura 9. Infracción Art 161-A y B del Código Penal
Fuente: Fiscalía Nacional del Ministerio Público

En ese sentido, podemos apreciar que existe más menos una constante en términos de la cantidad de casos que se presentan por años, en el año 2013 y

el año 2015, se ve un leve incremento que nos da una clara tendencia con lo que se puede apreciar hoy en día, donde se está masificando, y que en general busca causar algún tipo de daño a la imagen o reputación de una persona.

Del mismo modo, en los mismos tópicos considerados para la consulta a la Fiscalía Nacional del Ministerio Público de Chile, se procedió a solicitar aquellos datos que posee la Brigada Investigadora del Cibercrimen Metropolitana, pudiéndose obtener los siguientes datos:

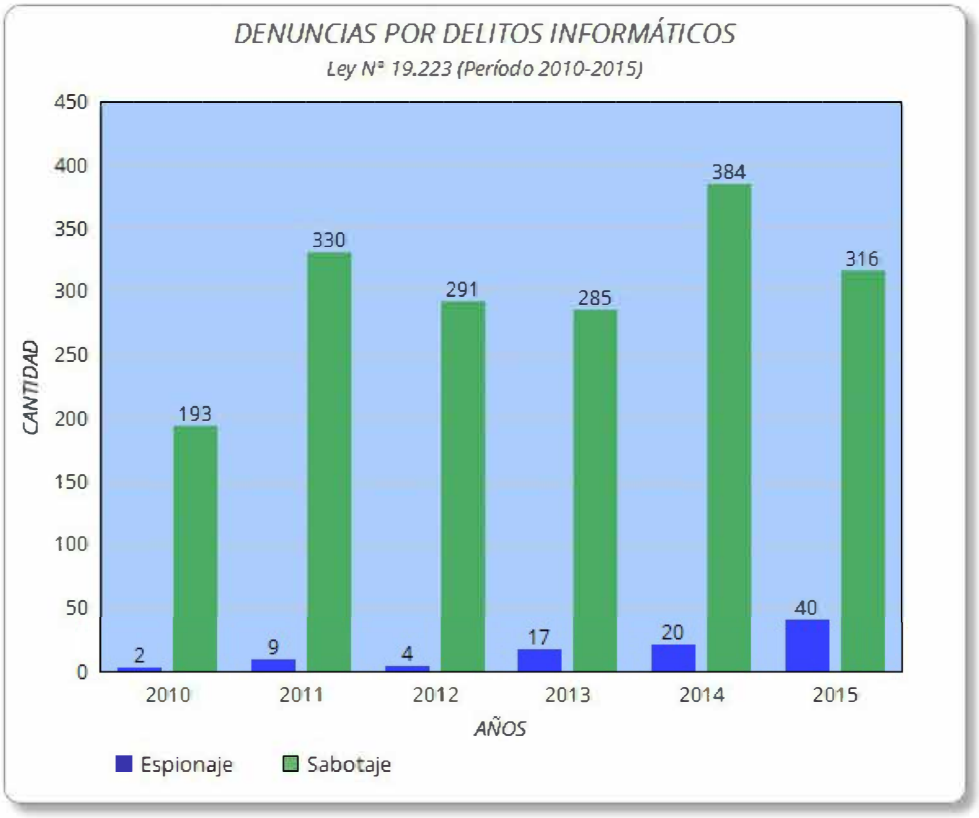

Figura 10. Denuncias cursadas en la Brigada Investigadora del Cibercrimen Metropolitana de la Policía de Investigaciones de Chile, durante el periodo comprendido entre el año 2010 al 2015, específicamente asociadas con los delitos informáticos.

En relación al gráfico precedente, y a los datos contenidos en el, se pueden efectuar algunas precisiones a fin de favorecer la comprensión del comportamiento de los mismos. Lo primero que se puede observar es que

aquellas acciones relacionadas a espionaje informático, presentan cantidades bastante bajas, pero con una clara tendencia de crecimiento. En relación aquellas acciones asociadas al sabotaje informático, se aprecian cifras bastante altas, con leves oscilaciones en algunos años, pero claramente para aquellos valores más bajos, en ningún caso se podrían hablar de una disminución de dichas acciones delictivas.

Figura 11. Denuncias cursadas en la Brigada Investigadora del Cibercrimen Metropolitana de la Policía de Investigaciones de Chile, asociadas a delitos contra la vida y la privacidad de las conversaciones, Art 161-A y B, del Código Penal.

Del mismo modo, en aquellas acciones relacionada con la creación de perfiles falsos, que buscan publicitar información personal de sus víctimas, con la finalidad de desprestigiarlas, todo a través de la utilización de redes sociales, o páginas web que permiten la publicación de manera gratuita, se aprecia un incremento importante, año a año, por un lado el incremento está dado porque muchas personas han tomado conocimiento que es posible denunciar una situación de esta naturaleza, y por otro lado, porque cada vez, es más utilizada como una forma para tomar venganza en contra de otro.

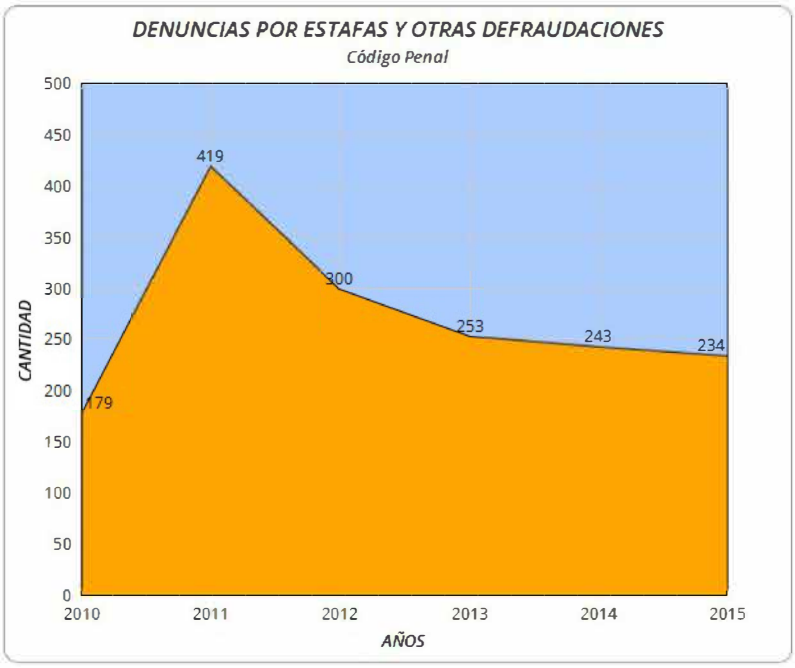

Figura 12. Denuncias cursadas en la Brigada Investigadora del Cibercrimen Metropolitana de la Policía de Investigaciones de Chile, asociadas a delitos relacionadas con Estafa y Otras Defraudaciones, contempladas en el Código Penal.

En el caso de aquellas denuncias por estafas y otras defraudaciones, se aprecia, un incremento importante durante el año 2011, el cual estuvo dado fundamentalmente por aquellas actividades ligadas al *pharming y phishing*, pero que posteriormente fueron disminuyendo producto de la persecución penal, por las campañas efectuadas por parte de la banca, y también porque se fueron aumentando los estándares de seguridad, dado que al inicio de este fenómeno eran bastante precarios. Posteriormente, es posible apreciar una leve disminución año a año, sin embargo, dicha disminución no es de gran impacto, dado que cada vez aparecen nuevas formas de estafas, como, por ejemplo: arriendo de casas de veraneo, venta de dispositivos electrónicos, entre muchas otras formas de engaños, que utilizan como medio de comisión las redes sociales o páginas web donde es posible publicar diferentes tipos de avisos de ventas de todo tipo de productos.

Figura 13. Denuncias cursadas en la Brigada Investigadora del Cibercrimen Metropolitana de la Policía de Investigaciones de Chile, asociadas a delitos relacionadas con Estafa y Otras Defraudaciones, contempladas en el Código Penal.

Respecto de la infracción estipulada en el artículo 36-b, de la Ley General de Telecomunicaciones, no se aprecian indicadores significativos, conforme se puede apreciar en el gráfico precedente, probablemente por un desconocimiento del mismo, dado que la interceptación de comunicaciones, se asocia más a la captura de la señal satelital de las cableras.

Es importante consignar, que si bien estos datos son bien decidores, y de alguna manera nos muestran una tendencia de crecimiento en lo referido a la criminalidad cibernética, también existen ausencia de estudios o recogidas de datos que permitan dimensionar de manera precisa el fenómeno, fundamentalmente porque muchas empresas que sufrieron algún episodio asociado a un delito de origen cibernético, desisten de iniciar una acción legal, en primer lugar porque eventualmente podría significar algún tipo de descredito

por poseer alguna vulnerabilidad, por lo tanto, esa mala fama podría también verse reflejada en la pérdida de clientes, que finalmente se traduce en pérdidas económicas, y esto no sólo ocurre en el ámbito nacional, sino que es una tendencia también observable a nivel internacional. Del mismo modo, existen algunos casos que rehúsan a efectuar una denuncia porque consideran que las penas asociadas a este tipo de delitos son demasiadas bajas, y más aún si el ataque es muy sofisticado, y es realizado desde fuera del territorio nacional, es muy difícil que exista siquiera la posibilidad de identificar al imputado y menos que se le persiga judicialmente, lo cual al final del día, opera como un desincentivo para iniciar algún tipo de acción penal, lo cual va generando que quienes están detrás de determinados ataques sigan en la impunidad total.

Es dable señalar que, los datos señalados precedentemente, tanto del Ministerio Público de Chile, como los de la Policía de Investigaciones de Chile, corresponden únicamente a una muestra, dado que también existen cifras negras, que no permiten visualizar la problemática de manera precisa, fundamentalmente porque existen muchísimos casos en que los afectados sencillamente no desean denunciar, aduciendo a diferentes razones, y por otro lado la clasificación en los sistemas de las instituciones involucradas en el quehacer penal, únicamente lo hacen conforme a la tipificación existente para los delitos, por lo tanto, si quisiéramos establecer de manera exacta cuantos afectados existen por *phishing*, no es posible, porque finalmente quedan registrados bajo el delito de estafas y otras defraudaciones. Son muchos los países, que consideran que su sistema de estadísticas policiales es insuficiente para registrar los delitos cibernéticos. Las tasas de delitos cibernéticos registrados por la policía se corresponden con los niveles de desarrollo del país y con la capacidad policial especializada más que con las tasas de delincuencia existentes.

CAPITULO 3

3.1 ANÁLISIS NORMATIVO DE LOS DELITOS INFORMÁTICOS

3.1.1 Generalidades

Prácticamente desde de los inicios de la informatización de diferentes procesos tanto en el ámbito público como en el privado, comenzaron a reportarse incidentes relativos a instrucciones no autorizadas, probablemente por la escasos mecanismos de seguridad que presentaban las primeras soluciones informáticas, las cuales comenzaron hacer aprovechadas por quienes poseían algún interés en la información que se almacenada en un determinado sistema de información, por otra parte, en el caso de que dichas intromisiones fueran advertidas, tampoco existía la capacidad técnica para efectuar una pericia, ya que no se contaba con los lineamientos o estándares para tales efectos, situación muy bien explicada por Clifford Stoll, quien fuera administrador del centro de cómputo del Lawrence Berkeley National Laboratory, en California, en la década de los setenta, quien debió enfrentarse a un sin número de intrusiones, por lo que se vio obligado a desarrollar determinados controles para ir recopilando información que le permitiera conocer quien estaba al otro lado de la red computacional, y que estaba accediendo a sus datos sin su consentimiento.

Nuestro país en materia económica ha experimentado avances significativos según indicadores internacionales nos sitúan entre las siete economías más libres del mundo[17], convirtiéndose en el líder indiscutible de Sudamérica, debiéndose fundamentalmente por la existencia de un estado de derecho, con un gobierno reducido, con énfasis en la búsqueda constante para mejorar las regulaciones internas, y por supuesto la apertura de la economía que presenta

[17] Miller, T., Kim, A. (2016). «2016 Index of Economic Freedom», 12, 484.

el país, han favorecido tanto al desarrollo como al crecimiento del mismo, lo que sin duda, ha fomentado una serie de avances y en especial la incorporación de soluciones relacionadas con el ámbito tecnológico, lo cual ha venido a cambiar la forma en que se venían haciendo las cosas, prueba de ello, es que nuestro país presenta excelentes índices no sólo en términos de acceso a internet, sino también a nivel sudamericano lidera en términos de la velocidad del acceso.

Ese mismo escenario de crecimiento vertiginoso de la tecnología, viene a presentar no solamente nuevas oportunidades en términos de desarrollo y crecimiento para la nación, sino también trae aparejado un sin número de acciones que podrían atentan contra los derechos de las personas, fundamentalmente los relacionados con la vida privada, entonces a partir de ello, nace la necesidad imperiosa de regular por la vía legal determinadas acciones delictivas llevadas a cabo con la ayuda de la tecnología y que son factibles gracias a la existencia de internet, a partir de esta interconexión que cubre casi todo el globo terráqueo. La disciplina que se hace cargo de su regulación desde lo legal, se conoce como la rama del derecho informático, lo cual surge a consecuencia de un cambio brusco en un muy breve plazo de tiempo, no dándose de la manera tradicional en que generalmente nace una rama jurídica, por lo que en sus inicios existió de alguna manera ciertas discrepancias respecto de la autonomía del derecho informático, ya que constituía una rama atípica. Ya que frente a la ausencia de este muchos recurrían a otros cuerpos normativos como el derecho civil.

Pero como no todo puede ser resuelto por la vía civil, se requería contar con una rama autónoma del derecho. Y en ese contexto, podemos encontrar que existen en muchos países, incluyendo el nuestro, organismos en donde se estudia lo relacionado con la informática y el derecho, todo ello viene a reforzar más aún la idea del derecho informático como una rama jurídica autónoma del

derecho. Lo que sí está totalmente claro es que el derecho informático, es más que necesario porque nuestro país posee una alta informatización, y por ende se hace indispensable para poder mantener una debida protección en la utilización de la misma, y en especial buscar proteger el derecho a la intimidad, porque a partir de la dependencia de la tecnología pudiese generarse grandes problemas frente a la inexistencia de controles sobre la misma, y de esa forma asegurar su utilización bajo relativa normalidad, porque también no es menos cierto, que la regulación legal no es la única forma de control en lo relacionado con la informática.

Con el desarrollo tecnológico que ha experimentado el país en las últimas décadas, ha traído innumerables beneficios, en especial lo relacionado con el acceso a la información, pero, así como presenta cosas positivas, también trajo aparejado la posibilidad de llevar a cabo acciones de carácter delictivo. En algunos casos se tratan de acciones tradicionales, las cuales ya se encuentran tipificadas, como, por ejemplo: la estafa. En el mismo sentido, se comenzó a experimentar situaciones que derechamente estaban dirigidas a los sistemas computacionales y los datos contenidos en estos, lo cual requirió de una tipificación especial para aquellas situaciones.

En este capítulo se pretende conocer el trabajo de aquellos organismos internacionales, como es el caso de la Organización de las Naciones Unidas y del Consejo de Europa, y de esa manera poder conocer sus esfuerzos para perseguir la criminalidad cibernética en general. Por otra parte, se procederá a revisar tanto la normativa internacional como nacional en esta materia, de tal manera de poder conocer el marco regulatorio respecto de la utilización de código informático diseñado para la comisión de diferentes tipos de delitos, y que presentan índices de crecimiento exponencial, y no se vislumbra una disminución en un horizonte de mediano plazo.

3.2 Organismos Internacionales frente a la delincuencia informática

3.2.1 Organización de las Naciones Unidas

Es dable destacar a nivel de las organizaciones de índole intergubernamentales que operan a nivel universal, que no se han quedado inmóviles frente a las acciones delictivas relacionadas al ámbito cibernético, más aún cuando una de sus principales características de este fenómeno, es que no reconoce fronteras, por lo mismo, las Naciones Unidas, lleva ya varios años realizando estudios respecto de la criminalidad cibernética, con la finalidad de coordinar una acción a nivel global que permita su combate de manera mancomunada, así como también generar conciencia respecto del tema, de tal manera que cada nación participante lleve a cabo acciones para mitigar este flagelo.

En ese contexto, el año 2010 se llevó a cabo el 12° Congreso de Las Naciones Unidas, sobre Prevención del Delito y Justicia, el cual tuvo como tema central el análisis respecto de la utilización de la ciencia y la tecnología en actividades de índole delictual, esto justamente debido a la relevancia que ha adquirido en las últimas décadas la expansión de la tecnología y el crecimiento del fenómeno de la cibercriminalidad a nivel mundial. Entre las preocupaciones abordadas se encuentra la incertidumbre del alcance del delito informático y computacional, dado que, si bien es cierto, existe preocupación a nivel internacional por este fenómeno, también no es menos cierto, que las estadísticas que dan cuenta de la actividad ilícita, también presenta serias deficiencias, siendo muy difícil encontrar detalles pormenorizados del tipo de delito, detenidos, o enjuiciamientos, existiendo más bien cifras globales que dan cuenta de la problemática. Del mismo modo, existen cifras desconocidas, ya sea porque los afectados no denuncian, o por desconocimiento cuando se tratan de persona naturales, o bien porque, si inician acciones legales, podría repercutir en una publicidad negativa, o bien en la pérdida de ingresos cuando se trata de personas jurídicas.

Otro aspecto que formó parte de dicha discusión está dado por la dimensión transnacional que posee la criminalidad cibernética, en ese sentido se plantea la necesidad imperiosa de desarrollar canales formales que favorezcan una respuesta eficiente y eficaz, entre los países, dado que como consecuencia del principio fundamental de la soberanía nacional, ningún país puede desarrollar actividades de investigación en otro, sin el debido, consentimiento o autorización del mismo, de ahí que se hace necesaria la homologación de normativa legal, y de directrices que permitan la persecución legal de acciones delictivas asociada al cibercrimen, y que permitan disminuir los niveles de impunidad existes en la actualidad.

Otro de los esfuerzos, tiene relación con lo indicado en el párrafo anterior, en lo relativo a la estandarización de los enfoques jurídicos nacionales, dado que en algunas oportunidades se ha dado el caso que del país desde donde se ha originado un determinado ataque cibernético, dicha acción no se encuentre tipificada como un delito, pero que, si está categorizado como tal en el país de destino del ataque, lo cual impediría su persecución. Eso más bien, desde lo jurídico, pero también existen limitaciones en lo técnico, ya que en muchos países no existe obligatoriedad para que la empresa prestadora de servicios asociado a internet, mantenga los debidos registros que permitan desarrollar diligencias investigativas posteriores.

De ahí que cobre vital importancia la estandarización de las normativas legales en los países. Lo cual va de la mano con el establecer canales formales que vengan a facilitar la cooperación internacional en la persecución penal de los delitos asociados al cibercrimen, ya que lo contrario, si no existen canales que permitan obtener información de manera rápida entonces es posible que se pierda información importante desde lo técnico dado la volatidad que presenta la evidencia digital.

Otro aspecto importante que han considerado, es que si bien es cierto, en muchos casos el ciberdelincuente actúa de manera aislada, también existen otros ataques muchos más lucrativos, que son ejecutados por verdaderas organizaciones altamente estructuradas, y con una definición clarísima respecto de las funciones que debe cumplir cada miembro que forma parte de dicha organización. Esto entonces, obliga a que la mirada deba ser distinta cuando actúa una banda organizada, para lo cual no sólo se debe contar con buenas normativas legales, sino un equipo a la altura de la situación que permita en la medida de lo técnico el esclarecimiento de los hechos y por supuesto la identificación de quienes están detrás de dicha acción punible.

Del mismo modo, la Organización de las Naciones Unidas, en cada reunión proceden a evaluar aquellos compromisos que fueron adquiridos por sus miembros en la sesión anterior, de tal manera de que cada país, de cuenta de aquellos avances en esta área. Evidentemente, dichos avances sobre todo en lo relacionado con la modificación o creación de normativa que apunte a la persecución de actividades ilícitas ligadas al ámbito cibernético, va mucho más lento de lo que se requiere, más aún cuando el fenómeno a regular presenta cambios extremadamente vertiginosos.

Uno de los esfuerzos significativos que se puede visualizar por parte de la ONU, en relación a los delitos informáticos, es la categorización que esta organización realizó respecto de los delitos informáticos, pudiéndose apreciar cinco categorías, específicamente las que se señalan a continuación:

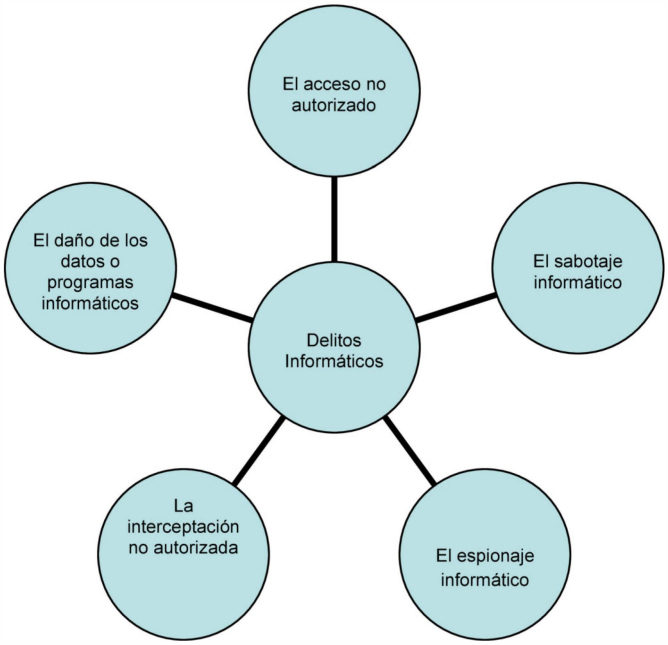

Figura 11. Clasificación de los Delitos Informáticos, por las Organización de las Naciones Unidas.

Esta clasificación se obtiene del Manual de las Naciones Unidas, para la prevención y control de delitos informáticos, publicada el año 1994, en dicho estudio es posible obtener que alrededor del 90% de los delitos realizados mediante la utilización de un medio informático fueron llevados a cabo por personal de las mismas compañías, y que sólo un 23% habría sido ejecutado desde el exterior. Lo cual se condice con los estudios llevados a cabo, por importantes empresas ligadas al mundo de la seguridad informática, donde el cliente interno juega un rol importante a la hora de perpetrar algún ataque de índole cibernético.

3.2.2 Consejo de Europa

El convenio de Budapest sobre Cibercrimen, surgió a partir de una propuesta del Consejo de Ministros del Consejo de Europa[18] durante el año 2001, el cual posee como objetivo principal convertirse en un tratado de carácter internacional que viene hacer frente a las distintas acciones delictuales que se están suscitando alrededor del mundo, lo cual demandaba una solución que permitiera aunar los esfuerzos al momento de perseguir criminalidad cibernética.

Por otro lado, dicho convenio no sólo busca ser una especie de guía para la armonización de las leyes nacionales relacionadas con los delitos ligados al mundo cibernético, sino también viene a exigir aquellos países que lo suscriban, procedan a establecer como delito aquellas conductas tales como el acceso indebido, la pornografía infantil, el fraude electrónico entre otros delitos, todo ello, como una forma de homogenizar la legislación interna de cada uno de los países adscritos, de tal manera de dotar de una herramienta eficaz que permita la persecución penal, y por sobre todo mejorar los actuales niveles de coordinación existente entre países para poder perseguir el crimen cibernético.

Dicho tratado entró en vigencia el 1º de Julio de 2004, y constituye el primer convenio penal con inspiración universal destinado a luchar contra el ciber crimen. Inclusive, hasta la fecha, el Convenio es el único instrumento internacional vinculante sobre la materia y sirve como guía para que los países puedan desarrollar una legislación interna integral contra el delito cibernético, además de servir como un marco para la cooperación internacional entre los Estados partes de este tratado.

---

[18] El Consejo de Europa es una organización de origen internacional que se encarga de articular la cooperación de los países europeos, en materias que buscan estandarizar diferentes aspectos legales, en ámbitos tales como; y no se debe democracia, delincuencia, derechos humanos, entre otros. 23.NOV.015. Es dable hacer presente, que el Consejo de Europa, no es lo mismo que el Consejo de la Unión Europea.

Es posible apreciar, que el nacimiento de dicho convenio no sólo habría sido motivado por las actuales condiciones criminales ligadas al ámbito tecnológico, sino según lo expresado por Susan W. Brenner[19], correspondería a un esfuerzo que comenzó veinte años antes con un estudio de la Organización para la Cooperación y Desarrollo Económicos (OCDE) sobre la posibilidad de estandarizar las legislaciones nacionales sobre ciber crimen.

En el año 2001, Alemania, Reino Unido, España, EE.UU. y Canadá se convirtieron en signatarios de dicho convenio, habiéndolo ratificado todos ellos entre 2006 y 2011, salvo Canadá, cuya ratificación aún permanece pendiente. Actualmente treinta y un países lo han ratificado, encontrándose abierto a la firma de otros países invitados a formar parte de dicho convenio.

En el caso de Chile, cabe señalar que, aún no se ha adherido a este Convenio, sin embargo, se encuentra en estudio del mismo, existiendo altas probabilidades de que se sume a dicho convenio, en un muy breve plazo.

En general, se podría decir que el convenio de Budapest, representa sin duda, un avance en términos de la creación de una política que permita aunar los esfuerzos en pos de la estandarización de las legislaciones de aquellos países que deciden adherirse para la persecución de los delitos informáticos, más aún considerando la dimensión transnacional de dicha criminalidad. Evidentemente no ha estado exento de críticas por parte de la doctrina[20], para mayores detalles respecto de la situación de nuestro país, en relación a dicho convenio, se recomienda la lectura de Juan Carlos Lara, Manuel Martínez y Pablo Viollier.

---

[19] Brenner, Susan W. La Convención sobre Cibercrimen del Consejo de Europa. Revista Chilena de Derecho y Tecnología. Vol. 1 Nro. 1 (2012). Pp. 266.

[20] Para una Para un análisis de la conveniencia o no de la suscripción del Convenio de Budapest por parte de nuestro país, se sugiere la lectura del artículo "Hacia una regulación de los delitos informáticos basada en la evidencia", de Juan Carlos Lara, Manuel Martínez y Pablo Viollier, en la Revista Chilena de Derecho y Tecnología. Vol. 3 N° 1 (2014). Pp. 101-137.

Dentro de la clasificación en términos de acciones constituidas como delitos es posible apreciar lo siguiente:

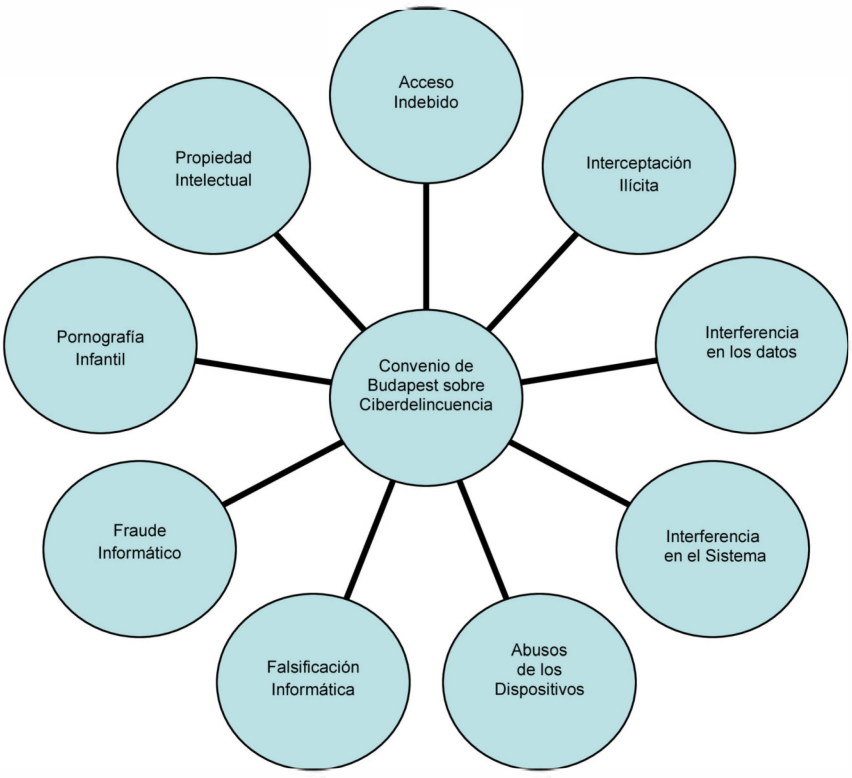

Figura 15. Delitos considerar por el convenio de Budapest, ligados al mundo cibernético.

3.3 Derecho Comparado

Se hace del todo necesario, adentrarse en el estudio respecto de aquellos cuerpos normativos existentes en otros países, para ver cómo se aborda la misma problemática, como una forma de poder obtener conclusiones con la mayor cantidad de información posible. Dado que nuestro país ha realizado esfuerzos para dar soluciones de manera reactiva, no existiendo acciones que busquen concienzudamente un mejoramiento de la norma de manera

mancomunadas entre todos los actores, y menos que exista una articulación adecuada entre normas que se relacionen ya sea directa o indirectamente con acciones delictivas en un ambiente cibernético, más aún cuando la tecnología presenta un crecimiento exponencial en su utilización en nuestro país.

La opción de adherirse al convenio de Budapest, es una oportunidad interesante de estudiar, dado que posee justamente un énfasis importante en dichas temáticas, y considerando la dimensión transnacional de este tipo de delito, permitiría la armonización de aquellas normativas relativas al derecho penal interno en lo relativo a los delitos informáticos, así como también generar un canal mucho más expedito y real para la puesta en práctica de la cooperación internacional. Dado que hoy en día, aún nos encontramos al debe, ya que no existen canales expeditos para la coordinación internacional en materia de este tipo de criminalidad, en ese sentido, considerando que internet, posee una expansión global, y que los fenómenos también evolucionan con gran rapidez por lo que se hace necesario respuestas de la misma manera frente a la persecución en términos penales, ya que en la actualidad si bien es cierto, es posible efectuar un requerimiento a algún país a través de Interpol, existen muchísimas respuestas en donde se indica que en el país de destino de la consulta, no existe obligatoriedad de respaldar el tipo de información requerida o bien una determinada acción no se encuentra tipificada como delito. Dentro de este convenio es posible apreciar por ejemplo el establecimiento como delito el fraude electrónico, situación que nuestra actual legislación no contempla.

Del mismo modo, se hace necesario efectuar una revisión a la situación jurídica que presentan algunos países en materia de delito informático, para de esa manera proceder a su comparación con la normativa nacional, de tal manera de establecer ya sean sus similitudes o ventajas que pudiesen contener, y de

alguna manera pudiesen resultar útiles para el mejoramiento de nuestra propia norma. Para lo cual se plantean como caso de revisión los países de España, Alemania y Estados Unidos.

3.3.1 España

En el caso español, es posible apreciar que no poseen una norma específica para aquellas acciones delictivas ligadas al mundo cibernético, sino más bien, introdujeron en su propio código penal aquellas conductas que fueron tipificadas como delitos y donde se haya utilizado para su comisión algún medio tecnológico, o bien se haya atentado contra un determinado sistema de información o sobre los datos que este sistema mantenga almacenado, no apreciándose, de manera tácita en dicho cuerpo normativo, alguna referencia específica sobre los conceptos de delitos informático o cibercrimen, sino más bien, dichas incorporaciones se encuentran enfocada en proteger la privacidad, y castigar a quienes descubran y revelen información sin el consentimiento de su propietario, por diferentes medios, entre los cuales se consideran aquellos medios de origen tecnológico.

Principalmente bajo el Título X, correspondiente a delitos contra la intimidad, del domicilio, del Código Penal español, se aprecia el artículo 197, el cual establece acciones relacionadas tanto con el espionaje como sabotaje informático. Adicionalmente, es posible apreciar, que en el caso, que quien comete el delito fuese parte de un grupo criminal o bien corresponda a una organización criminal, entonces se deberá aplicar las penas superiores en grado establecidas, a diferencia de nuestro país que no hace una diferenciación respecto de la calidad de quienes lleven a cabo las acciones delictivas en grupo o se hayan organizado para tales efectos.

Dentro de las modificaciones es posible apreciar que durante el año 2010, mediante la Ley N° 15/2010, incorporaron a su Código Penal, en su artículo 183 ter, la figura conocida como “child grooming”, la cual consiste en términos generales, en una forma de abuso sexual de carácter impropio, que consiste en la exposición de menores a actos de significación sexual, a través de diferentes aplicaciones que operan vía internet, que para el caso de nuestro país, se encuentra tipificado en nuestro Código Penal, en el artículo 366 quárter, como abuso sexual impropio.

Así mismo es posible apreciar que, más que la tipificación de delitos de carácter informáticos propiamente tal, se visualiza un esfuerzo importante en la protección del bien jurídico correspondiente a la integridad y confidencialidad de la información independiente del soporte en la que esta se encuentre, y más bien incluyeron aquellos relacionados con los medios tecnológicos. Del mismo modo, es posible inferir que han excluido de la discusión el daño físico que pueda sufrir un equipo computacional, no formando parte de los delitos asociados al área informática.

Otro aspecto diferenciador, en el caso de español, es que no definieron cómo delito cualquier tipo de acceso indebido, sino más bien, la protección apunta directamente hacia la privacidad de los datos, por lo tanto, lo que se castiga no es el acceso propiamente tal, sino la mal utilización de la información obtenida mediante un acceso indebido. Por lo que es posible, visualizar que los esfuerzos están dirigidos a la protección de la información, más que al acceso indebido propiamente tal.

3.3.2 Alemania

En el caso alemán, tampoco quedaron ajenos respecto de aquellas acciones donde la tecnología comenzó hacer utilizada con fines delictivos, por lo que

cuando se vieron enfrentados a esta situación, procedieron a definir e incorporar directamente en su Código Penal, las sanciones para aquellos que lleven a cabo acciones ya sea relacionadas con espionaje o sabotaje informático.

En su código penal, es posible apreciar en el artículo 202a, número 1, que se establece como delito el acceso no autorizado a datos, por lo que es posible inferir que existe también un enfoque en la protección de la privacidad, bastante importante.

Aunque en opinión de algunos expertos, reconocen el esfuerzo de Alemania en la incorporación de un número importante de nuevos preceptos penales, pero que sería inferior a las existentes en Estados Unidos, para la misma materia, ya que no sanciona el mero ingreso no autorizado. En el mismo artículo, número 2, indica de manera precisa que dicha protección apunta específicamente a datos contenidos o transferidos mediante soporte electrónico o magnético, en ese sentido se aprecia una amplitud respecto del tipo de medio utilizado para almacenar o transmitir información, lo cual proporciona una amplia cobertura incluso para medios tecnológicos que aún no se hayan creado, considerando el avance vertiginoso que presenta la tecnología.

En la misma materia, en su artículo 303a, se contempla la alteración de datos, entre las acciones penalizadas está el cancelar, inutilizar o alterar datos, incluso se encuentra tipificada la tentativa, lo cual guarda relación con el sabotaje informático. Del mismo modo, en su artículo 303b, se estipula como punible la destrucción de bases de datos, deterioro, inutilización, eliminación o alteración de un sistema.

Otro aspecto interesante es lo indicado en su artículo 263a[21], relacionado con la estafa informática, sin duda todo un reto, dado que necesariamente debía tratar de encontrar una similitud a los requisitos que requiere una acción engañosa en el caso de una estafa tradicional, esto es, engaño, error, disposición patrimonial y perjuicio, para estar en presencia del hecho ilícito, sin embargo, determinaron que existiendo perjuicio patrimonial ya sea a través de la manipulación de una base de datos, la utilización de datos ya sean completos o incompletos, o mediante la utilización de datos no autorizados, entonces estaría en presencia de una estafa informática.

3.3.3 Estados Unidos

En el caso de Estados Unidos, es posible apreciar que existen varias disposiciones legales federales que definen aquellas facultades que poseen los organismos persecutores, para llevar a cabo investigaciones ligadas a los delitos informáticos, en especial lo relacionado con la obtención de evidencias informática. En general, son leyes que hablan respecto de las comunicaciones electrónicas en general, del mismo modo existen leyes especiales que hablan sobre la seguridad nacional y demás infracciones que ligadas a la propiedad intelectual.

Es dable hacer presente, que Estados Unidos, en el año 1994, introdujo una modificación a la Ley de Fraude y Abuso Informático (Computer Fraud and Abuse Act) del año 1986, la cual fue aprobada por el Congreso, fundamentalmente por los cambios vertiginosos que ha experimentado la tecnología en general. Esta ley constituye una base importante para hacer

[21] Artículo 263a. Estafa por computador del Código Penal Alemán. «1. Quien con el propósito, de procurarse para sí para un tercero una ventaja patrimonial antijurídica, en la medida en que él perjudique el patrimonio de otro, por una estructuración incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado de datos, o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso, será castigado con pena privativa de la libertad hasta cinco años o con multa.»

frente al flagelo de la delincuencia informática. Adicionalmente existen otras normativas también de carácter Federal, en la misma línea como: la Ley de Ejecución y Restitución de Robo de Identidad de 2008 (Identity Theft Enforcement and Restitution Act, ITERA), la Ley de Privacidad de Comunicaciones Electrónicas (Electronic Communications Privacy Act, ECPA).

Dentro del Acta de Fraude y Abuso Computacional, se establecen las sanciones para quienes utilicen algún tipo de código malicioso, realizando una diferenciación entre aquellas personas que se dedican a la creación de códigos maliciosos, para los cuales se estableció un castigo de hasta diez años en prisión federal más una multa. Ahora para quienes únicamente su acción estuvo dada por la distribución de un determinado código malicioso, se estableció una sanción que va desde una multa hasta un año en prisión. Del mismo modo, es posible apreciar que no existe una definición de un tipo de virus en particular, sino más bien, se encuentra enfocado al acto de la utilización de un determinado código con fines delictuales.

En ese contexto, la ley presenta representa una regulación de los virus hablando en términos muy generales (computer contaminant), sin que se refiera a un determinado código dañino, sino a toda forma de instrucción que tenga como objetivo contaminar bases de datos, modificar, destruir, transmitir, alterar los datos para el normal funcionamiento de una computadora, un sistema o bien una red informática.

De manera supletoria, existen otras leyes que permiten la persecución de delitos ligados al mundo informático, nos referimos a las leyes más bien de índole tradicional, que en algunas ocasiones también ha servido para perseguir delitos del tipo informático, como, por ejemplo: La Ley de Espionaje Económico (Economic Espionage Act, EEA), vigente desde el año 1996, con el fin de

proteger los secretos comerciales, y tratando de evitar con ello la apropiación indebida de la misma.

Por último, la Ley de Comunicaciones Almacenadas (Stored Communications Act, SCA), prohíbe la obtención o modificación, deliberada y no autorizada, de una comunicación electrónica en almacenamiento electrónico. La prohibición no se aplica a los proveedores de servicios de Internet, sino a los mensajes de texto.

3.4 Derecho Nacional

Tal como se ha dicho desde el inicio, nuestro país no ha estado ajeno al flagelo de la utilización de herramientas tecnológicas como medio de comisión para delitos ya sea de origen informático o computacional, y que se relacionan con la acción penal pública, puntualmente se podría efectuar una diferenciación entre dos tipos de delitos que se presentan en la práctica, el primero correspondería a los delitos informáticos, los cuales cuentan con un marco normativo que establece aquellas acciones que son constituyente de delitos, pudiéndose observar una especie de subdivisión en dos grandes áreas, una correspondería al sabotaje informático y la otra al espionaje informático, situación que si bien es cierto, no está descrita o definida en la ley, pero que ha sido introducida por los propios tribunales.

Por otra parte, podemos encontrar una serie de acciones delictivas que corresponden a delitos tradicionales que comúnmente son ejecutados en el mundo real, pero que ahora producto del avance tecnológico, también es posible realizarlas a través del mundo cibernético, los cuales comúnmente son denominados como delitos computacionales, que en definitiva corresponden a acciones delictivas tradicionales que son llevadas a cabo aprovechándose de la

existencia de tecnología que facilita la comisión de las mismas, fundamentalmente aprovechándose de las posibilidades que ofrece hoy en día la red de internet, tales como: estafa, usurpación de nombre, entre otros.

En ese sentido, si la acción punitiva que se cometió se enmarca dentro de lo estipulado en la Ley 19.223, entonces estaremos en presencia de un delito informático. Ahora bien, si se trata de algún delito computacional entonces se aplicarán otras regulaciones existentes en el marco de la normativa nacional, dado que una *botnet*, puede ser utilizada tanto para cometer un delito informático como uno de índole computacional, en general, es transparente al tipo de delito ya que por las funcionalidades que ésta presenta sirve para la obtención de información de todo tipo, y que por ende puede ser utilizada para todo tipo de delitos.

Para contextualizar el análisis respecto de la utilización de una *botnet* en actividades ilícitas, ya sea para la comisión de un delito informático o bien en uno de tipo computacional, se procederá a la revisión la siguiente normativa típicamente utilizada en nuestro país para la persecución penal, correspondiente a la Ley 19.223, en el caso de cuando se trata de delitos informáticos, y la infracción al Artículo 161-A y B, Estafa Residual Art 473, y el artículo 36 B, de la Ley General de Telecomunicaciones.

3.4.1 Ley N° 19.223, tipifica figuras relativas a la informática.

Lo primero que hay que señalar, es que Chile fue el primer país de Latinoamérica en sancionar los delitos informáticos; esta ley fue publicada el 7 de junio de 1993, la cual sin duda en sus inicios constituyó un avance importante para hacer frente aquellas acciones que se venían dando en términos de la delincuencia informática en nuestro país, ahora bien, conforme ha transcurrido el tiempo y producto de su sometimiento a revisión es que hoy

se plantea con mucha firmeza que requiere una mejora importante, ya que no contempla todas aquellas acciones de carácter delictivo en el plano informático, principalmente porque en la época en la que se promulgó, el uso de los computadores y de internet era aún muy limitado o bien derechamente porque requirió de un análisis aún mucho más profundo a la hora de su creación.

En ese aspecto a nivel mundial, se generó un desarrollo importante en lo relacionado con la regulación penal, en el caso chileno, no ha existido una modificación en el área desde el 7 de junio de 1993, fecha en que fue publicada la Ley 19.223, en donde se establecen aquellas figuras penales para quienes realicen acciones en contra de un sistema informático y sus datos que posea almacenado. Pero sin duda, ha generado una necesidad de reflexionar respecto de la forma en que se unen el derecho y el mundo de internet.

Con la finalidad de hacernos una idea, lo primero que debemos preguntarnos; ¿Qué son los delitos informáticos?, en términos muy generales cuando nos adentramos en la búsqueda de una definición, es posible apreciar que no existe una única respuesta, sin embargo, muchas de ellas presentan similitudes. Como es posible observar en la definición planteada por la Organización para la Cooperación y el Desarrollo Económico[22], «cualquier conducta ilegal, no ética o no autorizada, que involucra el procesamiento automático de datos y/o transmisión de los mismos». Otra definición similar la plantea el Departamento de Justicia Norteamericano, «sería cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática, sea esencial para su comisión, investigación o persecución». Del mismo modo, Castillo y Ramallo[23], plantean «como toda acción dolosa que provoca un perjuicio a personas o entidades, y

[22] OCDE es un organismo de cooperación internacional, fundada en 1960, actualmente está compuesta por treinta y cinco países, encontrándose su sede central en Francia, cuyo principal objetivo es coordinar la política económica y social, de aquellos países miembros.

[23] CASTILLO JIMENEZ, María Cinta, RAMALLO ROMERO, Miguel. El delito informático. Facultad de Derecho de Zaragoza. Congreso sobre Derecho Informático. 22-24 junio 1989.

en cuya comisión intervienen dispositivos habitualmente utilizados en la actividad informática».

Con la proliferación de conductas delictivas vinculadas al crimen informático, fue haciendo necesario la creación de normativa que permitiera criminalizar determinadas acciones que hayan tenido cabida en el espacio cibernético, lo cual sin duda, no ha sido fácil, por lo tanto, cada una de las definiciones que es posible conocer, corresponden a un una aproximación de un concepto en desarrollo, adoptada en principio por varios autores con el argumento de que una definición de esa amplitud permitiría el tratamiento de las mismas hipótesis de trabajo para distintas disciplinas y podría así usarse una misma definición en análisis penales, económicos, sociológicos, etc. La definición puede servir como una primera aproximación conceptual que puede resultar útil para delimitar qué conductas ilícitas o indeseables tienen alguna vinculación con la informática criminal; sobre todo, porque en los primeros años en que comenzaron estos nuevos ataques los códigos penales, se encontraban ante una realidad que no era posible anticipar de manera adecuada, incluso hoy en día es difícil establecer una única definición general, dada las múltiples formas existentes para la criminalidad cibernética.

En el caso nacional, Jijena Leiva, plantea no crear un cuerpo normativo nuevo, sino incorporar estas nuevas formas de comisión de delitos, en los cuerpos legales ya existentes, lo cual supone una transformación en el orden jurídico tradicional. De lo cual podemos desprender que este posee algunas particularidades y que estaría apuntando a un bien jurídico especial, y que indudablemente no encajaría en aquellos tradicionales. Por lo que podríamos decir que en la práctica se han establecido determinados tipos penales para aquellas acciones que atenten contra un sistema computacional y/o los datos que este contenga almacenados, haciendo una clara distinción por ejemplo de

un daño físico lo cual estaría excluido como un delito informático, discusión que se encuentra zanjada. Ahora respecto de aquellas acciones tradicionales y que simplemente hayan utilizado alguna solución informática para llevar a cabo su cometido, se enmarcarían dentro de los denominados delitos computacionales.

Hace más de dos décadas que en nuestro país, se viene investigando por parte de abogados especializados en el ámbito tecnológico, en relación al delito informático, y dentro de sus discusiones es posible apreciar que ha existido serias posturas en tratar de definir o diferenciar entre aquellas acciones netamente informáticas y aquellas que únicamente la informática sirvió como herramienta para la consumación de un hecho punible, nos referimos a los denominados delitos computacionales, al respecto es posible encontrar algunas definiciones tales como la propuesta por Jijena Leiva, quien se refiere a los delitos computacionales como: «todas aquellas hipótesis delictivas que permiten ser encuadrados dentro de los tipos tradicionales, ya sea que en ellas los medios informáticos solo han sido una específica herramienta de comisión, mientras que los delitos informáticos requieren una configuración distinta, en consideración a particularidades que ellos envuelven», situación que pareciera gozar de toda lógica, toda vez, que un computador en algún momento puede ser considerado como el medio y en otras como el objeto para la comisión de un delito.

Es de todo conocimiento, que la información en un bien inmaterial, y que posee asociado de manera intrínseca un valor, ya que la obtención y generación de la misma ha involucrado una inversión muchas veces de un alto coste, por ende requiere que se desarrolle en torno a ella una regulación adecuada para brindar protección al propietario de la misma, y de esa manera evitar que sea tomada por un tercero sin la debida autorización, y no sólo por el coste que implicó la recolección de dichos datos, sino y quizás lo más importante asegurar

la privacidad de dicha información, en especial aquellos datos que revisten características de sensibles.

Los delitos informáticos constituyen un verdadero fenómeno, del cual aún no es posible siquiera vislumbrar su alcance, lo cual supone una problemática importante porque claramente se trata de una delincuencia distinta a la tradicional, y que tiene alcance mundial, aunque incluso algunas acciones correspondan a delitos tradicionales, en donde únicamente se utilice como medio de comisión la tecnología, como son los denominados delitos computacionales. Esta nueva variante de delito informatizada nos presenta varias aristas complejas que hacen un tanto difícil su tratamiento, examinando sólo algunas que nos permitirá definir un marco de análisis sobre la problemática en general, y no busca pretender que sean las únicas existentes.

Una de las problemáticas, es que al ser informático nos presenta inmediatamente una complejidad importante, dado que posee una mezcla de varias técnicas, como lenguajes de programación cada uno con sus propios códigos, diseños de sistemas, componentes físicos, entre otros, como ya es sabido, presentan una obsolescencia muy rápida lo que complica tanto a quienes pretenden solucionar una determinada acción constituyente de delito desde lo técnico, pero también genera un problema para quienes se encargan de estudiar o crear leyes para determinados fenómenos, haciendo que muchas veces se llegue tanto desde lo técnico como del derecho con un remedio cuando ya la enfermedad desapareció o ya se convirtió en una verdadera pandemia, incluso quizás ni siquiera sirva para el rebrote de una nueva variante de una acción delictiva en el mundo cibernético.

Otro aspecto importante, es que su uso no está limitado sólo a las grandes empresas, con cientos de especialistas capaces de comprender su

funcionamiento e incluso aplicar medidas para mitigar posibles acciones delictivas, sino que es transversal a toda la sociedad, desde su uso doméstico en casa, en colegios, instituciones públicas, empresas, fuerzas armadas, de orden y seguridad. Por lo que, no será posible que la sociedad en general pueda cuidarse de eventos de esta naturaleza, toda vez, que cada día cientos de funciones están siendo desarrolladas de manera computacional, lo cual se enmarca dentro de un proceso natural de innovación y desarrollo de la tecnología en sociedades en vías de desarrollo o bien ya desarrolladas.

Del mismo modo, la tipología en la que opera la red, donde todos de alguna manera nos encontramos conectados, independiente desde el lugar donde nos ubiquemos geográficamente, habrá alguien que estando físicamente en otro continente podría atacar y vulnerar la seguridad informática de otro sujeto ubicado en otro continente sin ningún inconveniente. En otras palabras, este tipo de delito no reconoce una determinada área geográfica, sino que sencillamente no reconoce fronteras ni países, por lo que, claramente es difícil definir determinadas regulaciones cuando estas podrían estar siendo realizadas fueras del territorio nacional, lo cual dificultaría enormemente su persecución.

En la misma línea, el conocimiento en materia tecnológica, que ha cimentado la denominada cibercultura[24], posee también una arista que facilita la comisión, una porque la tecnología irrumpió en nuestro país de manera bastante rápida, y se encontró con una generación que se encuentra fuera de los denominados nativos digitales. Por lo tanto, más bien tomó conocimiento de lo básico para poder operar, pero desconociendo totalmente aquellos riesgos a los que se podrían ver expuestos. En general, las personas poseen una alta comprensión de aquellas situaciones de carácter delictivo en el mundo real, pero desconocen

[24] Derrick de Kerckhove. «La piel de la cultura. Investigando la nueva realidad electrónica», Barcelona, Gedisa. editorial.1999

e incluso les cuesta imaginar que se puedan convertir en potenciales víctimas en un escenario de origen cibernético, en definitiva, se podría decir que internet llegó, pero no traía manuales que ayuden a estar preparado para los crímenes informáticos, en especial cuando nuestros datos están almacenados en un medio computacional.

Existen algunos autores, tales como: Chomsky y Dieterich, 1999, pág 162, que plantean que a partir de la década de los ochenta se experimentó una verdadera revolución en términos tecnológicos, lo cual ha venido a darle vida a la denomina cultura cibernética, y que sería la primera cultura realmente universal en la historia del hombre.

Todo lo anterior, configura un escenario tremendamente complejo para el ámbito jurista, ya que tratar de tipificar una determinada acción con tan alta diversidad tecnológicas, que podría llevar a definir una tipificación quedé respuesta únicamente a un determinado fenómeno y quedemos corto frente a una nueva forma de comisión, permitiendo que su persecución penal sea infructuosa o incluso imposible, cimentando un camino propicio para que los delincuentes cibernéticos puedan operar en total impunidad.

Y este tipo de acciones delictivas requiere un ordenamiento jurídico, acorde a las actuales exigencia de la sociedad, porque tienen un impacto directo en ella, he incluso sus consecuencias pueden ser devastadoras, tanto en términos personales para un determinado individuo como para un país entero, cabe recordar el incidente acaecido en Estonia el año 2007, donde un grupo activista mantuvo en jaque al país por varios días, llevando a cabo una operación de denegación de servicio que mantuvo paralizada a los principales sitios web de dicho país, en especial aquellos relacionados con la banca, y tan sólo porque se había anunciado el traslado de una estatua de un líder soviético hacia otro lugar

del país, lo cual generó dicha molestia y por ende terminó con un país paralizado desde el punto de vista de la operación en el mundo cibernético.

En términos económicos, existen reportes que permiten evidenciar que el coste promedio del cibercrimen ha aumentado en aproximadamente un doscientos por cientos[25], en otros casos se afirma que las ganancias obtenidas por acciones asociadas al cibercrimen están muy cercanas a las ganancias obtenidas por el narcotráfico, sin embargo, el cibercrimen es más silencioso y a nivel social no posee el mismo castigo, ya que ser una persona ligada al mundo delictual informático, supone que posee conocimiento alto respecto de la operatoria de lo tecnológico, por lo que, más que condenarlo goza de una suerte de admiración incluso por parte de sus propias víctimas. No así un traficante de droga del cual se tiene una mirada mucho más lapidaria por parte de la ciudadanía, toda vez, que ve a ese personaje, como un sujeto con un desarrollo carente en muchos aspectos y que producto de su entorno terminó inmerso en una actividad ilícita y finalmente es visto como una lacra para la sociedad ya que claramente está destruyendo la vida de muchas personas.

Por tanto, hoy en día se encuentra acuñado el concepto de criminalidad cibernética, ya que en sus inicios probablemente como todas las cosas, comenzó de manera muy incipiente y más bien se centró en el aprovechamiento de brechas de seguridad en el campo de la informática que fueron explotadas por personas que vieron una oportunidad, de obtener un dividendo económico fundamentalmente y que en algunos casos quienes estaban detrás de alguna acción en la mayoría al menos en sus orígenes no contaban con una formación oficial en el ámbito de la informática, siendo más bien verdaderos autodidactas y que habían invertido mucho tiempo en

[25] http://www.hamiltonplacestrategies.com/sites/default/files/newsfiles/HPS%20Cybercrime2_0.pdf

desarrollar verdaderos experimentos muchas veces jugando al ensayo y error, pero no sólo existen ataques externos, también los ataques internos son bastante recurrente y además cuentan con el conocimiento propio de la actividad interna, lo que favorece su comisión, siendo éste último, justamente el que posee más incidencia y quizás trae mayores problemas para quienes lo sufren.

Por lo que, hoy en día nos vemos enfrentados a un problema mucho mayor, que requiere de una intervención importante de varios campos, y en especial desde lo jurídico, como una forma de avanzar en la criminalización de determinadas acciones de índole informáticas que presentan crecimientos sustantivos, toda vez, que se favorecen a partir del anonimato que ofrece Internet, así como también de regulaciones ya sea inexistentes o deficientes en los países, por lo que la coordinación internacional y el desarrollo de normativas legales adecuadas es de carácter urgente y necesario.

En el caso chileno, la normativa, al ser revisada se puede apreciar que las figuras penales definidas, están dirigidas a proteger los sistemas de tratamiento de información, así como también los datos contenidos en ellos, siempre y cuando ese ataque haya sido con la utilización de la tecnología, ya que si alguien destruye físicamente un servidor que contiene un determinado sistema y por dicha acción resulta dañada la data existente en dicho medio computacional, no constituirá un delito informático, sino más bien un simple delito de daño, dicha discusión se encuentra totalmente zanjada en nuestro país.

En relación a los delitos computacionales, es preciso señalar, que este tipo de acciones, más bien corresponde a aquellas que tienen cabida en el mundo real, pero que con el avance de la tecnología y el cambio en la forma que se venían

desarrollando las cosas, también se han visto afectada por la delincuencia informática, nos referimos por ejemplo a: la estafa, la usurpación de nombre, entre otros, y que su diferencia fundamental con los delitos informáticos propiamente tal, es que estos utilizan la tecnología únicamente como medio para poder concretar el hecho delictivo.

Respecto de la estafa, es un tanto complicado en la actualidad, dado que una acción de phishing y pharming[26], no se enmarcarían estrictamente dentro de dicho delito, por cuanto, un ataque de esa naturaleza implica contar con las credenciales válidas para acceder a un sistema computacional, pero en definitiva por lo masivo del fenómeno, los tribunales se vieron obligados a perseguir dichas acciones a través del delito de estafa y otras defraudaciones, no existiendo una normativa específica que hable del fraude electrónico y del abuso de dispositivo.

A continuación, se detalla la normativa que finalmente sirve a la hora de perseguir penalmente alguna acción ya sea de carácter informático o computacional.

Artículo 473 del Código Penal

Uno de los delitos de mayor ocurrencia en los últimos años, corresponde a estafas, en donde para su comisión se ha visto involucrada algún medio tecnológico, utilizando para dichos fines variadas técnicas informáticas, fundamentalmente la denominada *SCAM*[27], mediante la cual les permite la

---

[26] **Pharming**, «es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado anteriormente.»

[27] **Scam**, es una técnica utilizada fundamentalmente para intentar obtener datos sensibles para posteriormente utilizarlos, y obtener algún tipo de dividendo económico, utilizando como vía de distribución el correo electrónico, los que generalmente llevan inserto algún enlace, que permite redireccionar a la víctima a una página web fraudulenta.

obtención de credenciales válidas, para concretar acciones fraudulentas cómo el *Phishing*[28], sin embargo, no es que no requiriendo vulnerar ningún sistema con una técnica alta que finalmente caben en la denominada ingeniera social, pudiéndose observar principalmente perfiles en redes sociales falsos que ofrecen todo de tipo de productos que finalmente nunca llegan a los compradores, ofertas de trabajos fraudulentas, herencias fraudulentas, gestión de visa de trabajos, premios falsos, entre otros.

Respecto de todos aquellos delitos más tradicionales, pero que utilizan como medio de comisión la tecnología, más bien conocidos como delitos computacionales, no poseen una normativa específica que trate de manera especial cuando estos son llevados a cabo de manera cibernética, fundamentalmente la problemática que es posible apreciar aquí es que nuestra legislación no contempla el fraude electrónico.

En este artículo, se puede apreciar que existe una definición genérica, que no establece una forma específica de engaño, por lo tanto, cuando mediante ingeniería social, una tercera persona desconocida, utilizando determinada tecnología, logra engañar a su víctima, y producto de dicha situación la otra persona entrega sus credenciales válidas, y por lo tanto, se cumplan tanto los elementos del tipo penal, esto es, engaño, error, disposición patrimonial y perjuicio, estaremos en presencia de la denominada estafa residual, es cómo lo han estado considerando los tribunales, a pesar de que existen detractores toda vez, que se entiende que las máquinas no pueden ser engañadas, ya que para poder ingresar a una cuenta bancaria a través de su modalidad en línea, se requiere contar con las credenciales válidas para tales efectos, por lo tanto, no se puede aplicar el concepto de engaño tal como se hace con una persona.

---

[28] **Phishing**, es una técnica utilizada para la comisión y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña u otra información de carácter sensible)

En lo especifico, este artículo no establece la forma de engaño, por lo tanto, podría ser cualquier mecanismo que permita engañar a una persona, incluso con la utilización de tecnología, sin embargo, dicho engaño es a una persona, quien finalmente entrega las credenciales válidas para ingresar a una plataforma bancaria o bien a una casilla de correo electrónico, los que posteriormente serán utilizados para ingresar a un determinado sistema transaccional con el fin de materializar la acción delictiva, pero en general, la máquina no es susceptible de ser engañada, más bien el engaño está en la utilización de perfiles falsos, o páginas que simulan ser de un banco, y que finalmente por descuido de los usuarios, no se toman unos minutos para corroborar la veracidad de dichos sitios, entonces proceden a facilitar las credenciales válidas para acceder a sus cuentas por ejemplo, por lo tanto, quien resultó engañado es una persona y no la máquina.

Otro aspecto fundamental, que no contempla la ley es el abuso de dispositivos, ya que una tecnología puede ser modificada o utilizar derechamente una determinada tecnología para la comisión de un delito cibernético, como en este caso la interceptación de datos que finalmente me permiten cometer un delito tradicional como es la estafa, como por ejemplo la utilización de tecnologías del tipo *raspberry pi*,[29] instaladas en cajeros automáticos, que permiten realizar análisis de paquetes de datos que se ingresan al cajero automático por parte de los usuarios, no existiendo ninguna posibilidad de parte del usuario de percatarse que le están capturando sus datos.

[29] Pequeño computador, que posee variadas capacidades de memoria, y soportes de dispositivos periféricos.

3.4.3 Infracción artículo 161 A y B del Código Penal

Otra situación bastante común es la creación de perfiles falsos en diferentes redes sociales, los cuales poseen diferentes motivaciones, pero que fundamentalmente buscan desprestigiar a sus víctimas, ya sea por la vía de la injuria o la calumnia, si bien es cierto, dichas acciones no corresponden al ámbito penal, pero lo que si se encuentra tipificado como delito es la acción de publicar información personal de un tercero sin su debido consentimiento, razón por la cual es posible cursar la denuncia respectiva para iniciar el proceso de judicialización.

El artículo 161-A y 161-B, del código penal, dice relación con la publicación de imágenes, información personal, videos, muchos de los cuales han sido obtenidos desde un entorno privado aprovechándose de la cercanía que suele tener el victimario de su víctima, lo cual se materializa ya sea por descuido o bien por la utilización de tecnología más avanzadas como es el caso de una *botnet*, la cual permite la obtención de información de manera remota, que finalmente terminan siendo publicitados a través de alguna red social, o bien en algún portal web que permita subir información de manera gratuita, en ese tipo de casos y que no son menores, conforme a la estadísticas existentes, la mayoría de dichas acciones estarían enmarcadas dentro de la infracción establecida en nuestro código penal, en dicho artículo es posible apreciar que dicha normativa está tipificada finalmente como una falta, por lo tanto, en la práctica sólo se le aplicará una multa, la cual están graduadas de entre 50 a 500 unidades tributarias mensuales, a la persona que se encuentre ya sea en un recinto particular o bien en lugares de libre acceso al público, sin existir de por medio, la debida autorización de la víctima, y por cualquier medio, en este sentido es interesante observar que la norma, una vez más, no se casa con ningún tipo de forma en particular de captar determinada comunicación o información de carácter privada, dado que usa la expresión «por cualquier

medio», en ese sentido podemos visualizar que es bastante amplia dicha situación, pero en definitiva permite proteger en caso de que un tercero, haya logrado obtener información personal de otra persona sin su consentimiento. Quizás lo que, si debiese definirse adecuadamente que tipo de información es susceptible de ser perseguida penalmente, dado que no siempre se trata de información de carácter sensible y quizás derechamente debiese ser tratada por la vía civil, cómo una forma también de descongestionar el sistema, y así poder centrar los esfuerzos en aquellos delitos de mayor impacto social.

Del mismo modo, es posible apreciar en dicha norma, que no sólo establece la forma de obtener la información privada, donde se utilizan una gran gama de verbo rectores que permiten especificar una gran cantidad de acciones que se encuentran definidas. Adicionalmente es posible apreciar que también se sanciona a quien haga mal uso de dicha información, como lo es la publicación en cualquier medio a disposición de los demás, sin la autorización de su propietario.

Por otra parte, esta norma, define una infracción mayor, si es que la persona que obtiene la información, finalmente termina siendo el mismo que procede a publicarla a través de cualquier medio, pero fundamentalmente en Internet, ya que existe una serie de sitios web que ofrecen la posibilidad de publicar información sin ningún coste asociado, además considerando el nivel de anonimato que ofrece Internet, hace mucho más fácil y propicio la comisión de delitos de esta naturaleza.

Ahora respecto de la norma, si bien es cierto, permite iniciar la acción penal, no constituye una solución integra, dado que si bien es cierto, el marco el regulatorio lo que busca es restituir el bien jurídico lesionado, no soluciona del todo su problema, dado que la publicación en cuestión sigue manteniéndose en

portales web, situación que si se trata de un portal web nacional, entonces el tribunal competente podría ordenar la baja del contenido que está produciéndole un problema a la víctima, no corre la misma suerte si se trata de un sitio web que se encuentra fuera del territorio nacional, lo que complejiza el dar de baja determinado contenido, y además obliga a gestionar directamente por parte del afectado, no existiendo un camino muy expedito para ello, dado que nos vemos enfrentados a variadas barreras, ya sean idiomáticas, tecnológicas, legales o sencillamente por desconocimiento de parte de la víctima en relación al manejo de la tecnología en cuestión.

3.4.4 Ley General de Telecomunicaciones Art.36 B.

En general, muchas de nuestras actividades cotidianas que eran llevadas a cabo de manera analógica, han estado migrando hacia al mundo digital, por lo que ha transformado desde ya hace un buen tiempo, en un espacio propicio para la comisión de diferentes delitos, lo que ha implicado leves movimientos en términos de normativa penal, que ayuden a perseguir acciones que atenten contra las comunicaciones. En ese sentido, es bastante común observar casos donde un tercero a logrado obtener ya sea correspondencia electrónica o bien aquellas realizadas vía alguna red social, y que posteriormente proceden a divulgar.

Por lo que es posible invocar el artículo 36–B, cuando se trate de la difusión pública o privada de cualquier comunicación que haya sido obtenida sin el consentimiento de su propietario. En el presente artículo de la Ley General de Telecomunicaciones, no se aprecia una especificidad respecto del tipo de tecnología tampoco, por lo que se podría entender como cualquier comunicación, dentro de esta tipificación podría estar, aquellas personas que comienzan a operar como una cablera y transmiten desde su casa contenidos por los cuales no han pagado los derechos pero obviamente cobran por la señal

a sus abonados, para lo cual cuentan con los códigos necesarios para descifrar determinada comunicación y de esa manera apoderarse de un contenido que no les pertenece.

3.5 Análisis de Caso por Delito Informático

Se analizará la sentencia del Octavo Juzgado de Garantía de Santiago, RIT 9186-2013, RUC 1300971941-K, resuelta por el Juez don Sergio Córdova Alarcón, Juez Titular, la cual dice relación con un código malicioso que fue distribuido a través de internet denominado "minerva.exe", cuando recién se descarga dicho archivo, no emite ninguna señal que permitiese advertir la existencia de una intervención en un computador, sin embargo, al ser sometido a pruebas en un ambiente controlado, se observa actividad permanente de dicho código, en primer lugar identifica los computadores para posteriormente distribuirse aprovechando su configuración, e inmediatamente comenzaba a conectarse al sitio web http://jokerkode.blogspot.com, para efectuar una descarga del código malicioso, que se ubicada en el directorio /2012/12/santuario-9.html, y dentro de su codificación e invisible a ojos del usuario normal, existían parámetros de conexión que recogía el código, para poder acceder al servidor público de IRC, o conversaciones tipo chat instantánea ubicada en diversas fuentes extranjeras, bajo el dominio irc.objects.net, canal #brigada, puerto de conexión N° 9000. El código informático, una vez sometido a revisión, se estableció que mantenía patrones característicos a los códigos maliciosos de este tipo, implementando para su operación llamadas a funciones del sistema operativo de la familia Microsoft Windows. Es por ello que permite ejecutar múltiples funciones de acuerdo a las actualizaciones vinculadas a las operaciones que permiten dichas librerías. En este sentido, es posible indicar que el código permite realizar las siguientes funciones:

a. Valores de sistema operativo: obtención de hora, fecha, dirección IP local,

nombre de cuenta Messenger, ruta de directorio temporal de Windows, país, versión del sistema, unidades, entre otras.

b. Procesos de ejecución a través de comandos: ejecución de archivos, listado de carpetas y archivos, listado de procesos en ejecución, obtención de fondo de escritorio, captura de pantalla, descarga de archivos, conexión a servidor FTP (servidor de archivos), captura de webcam, recepción de mensajes del atacante, activación de micrófono y transmisión de archivo de audio, eliminación de archivo, captura de teclado, entre otros.

c. Métodos de comunicación: conexión a FTP para subir y descargar archivos, descarga de archivos desde una URL, recepción de instrucciones a través de IRC.

En relación a los archivos materia de análisis es posible aseverar que éstos corresponden a un virus informático el cual hacer pertenecer a una *Bot* Net a sus víctimas. Su funcionamiento es silencioso y el usuario de los equipos computacionales no detecta operación alguna.

Tal como se explicó anteriormente, y en términos generales a la vez, se observó durante el período de análisis forense, que éste virus es contralado remotamente a través de un servidor de IRC público, el cual mediante ciertos códigos de configuración permiten acceder al canal #PDI con la información contenida dentro del mismo virus y la página web jokerkode.blogspot.com.

En dicho canal se detectó cerca de 330 equipos infectados, usuarios que utilizan nombres aleatorios asignados por una función propia del virus, lo que permite en definitiva que mantenga una conexión constante con ese medio de comunicación. Esto no quiere decir que las víctimas puedan escribir o ver lo que

está sucediendo, sino más bien, están a la espera de instrucciones del programador del virus.

El intercambio de información entre el delincuente informático y sus víctimas es por medio de un servidor FTP, el cual a través de instrucciones ordena a los computadores infectados subir archivos y él por su parte los descarga y elimina rápidamente. Además, dentro de estas funciones, se incluye la ejecución de otros virus alojados en servidores nacionales, lo que permite descargar un archivo con las contraseñas almacenadas en los diferentes navegadores web que tienen las víctimas.

Se considera que el nivel de peligrosidad del código malicioso es elevado ya que su creador mantiene constante revisión de los equipos infectados a través de instrucciones que operan directamente sobre los equipos comprometidos, con la cual obtiene información relativa a impresiones de pantallas, donde logran recopilar información sensible que les permite posteriormente acceder a otros servicios que pudiese tener la víctima a través de internet.

Tal como se puede apreciar, este tipo de virus, está diseñado en términos de programación para que sus víctimas, mediantes la utilización de un programa antivirus, no pueda siquiera advertir la posibilidad de que un tercero desconocido tomó control de su computador, y está obteniendo información de todo tipo, que pudiese ser sensible y perjudicial de salir de la esfera de privacidad de su propietario.

En este caso participaron tres personas ligadas al mundo de la informática, quienes mediante dicha herramienta pudieron lograr infectar alrededor de

trescientas computadoras[30], mediante el cual permitía el envío de un correo electrónico de manera masiva el cual contenía un archivo adjunto del tipo PDF, el cual con sólo darle clic permitía la instalación de la *botnet*, con la cual finalmente lograban tomar control de la máquina.

El método utilizado para llevar a cabo la operación, se centró en la utilización de ingeniería social[31], específicamente procedieron a utilizar como fallada un correo que supuestamente provenía de la Empresa Equifax, el que hacía alusión que quien lo recibía mantenía una deuda impaga atribuible a un parte, y que para mayores detalle debía abrir el archivo de extensión PDF, que daba cuenta de dicho comunicado, al abrir dicho archivo efectivamente el documento contenía información personal de la persona que recibía dicho correo electrónico, por lo que de alguna manera la daba cierto nivel de confianza, sin embargo, la sola acción de dar clic en dicho archivo comenzaba la instalación de este virus en la máquina donde se recibió el correo, proceso que evidentemente no podía ser advertido por el receptor del mensaje. Posteriormente, dicho virus podía mantenerse activo y conectado a través de internet, pero específicamente de IRC, donde cada uno de los equipos infectados pasaba a ser esclavos de parte de los creadores de dicho virus, conformando una denominada red *botnet*. El administrador de dicha *botnet*, podría impartir a través de los canales de conversaciones del IRC diferentes instrucciones sobres las máquinas que previamente ya habían sido infectadas. Dentro de los afectados existieron personas comunes y corrientes, pero también existieron medios de comunicación como canales de televisión, o incluso autoridades políticas, lo que sin duda, generó una preocupación, toda vez, que quedó demostrado que es posible utilizar dicha tecnología con

[30] Informe Forense Informático N° 208/13, elaborado por el Subcomisario Andrés Godoy Pérez, perteneciente a la Brigada Investigadora del Cibercrimen Metropolitana.

propósitos que se alejan de los márgenes establecidos por la normativa legal.

Conforme a los antecedentes vertidos a partir de la investigación, doña Alicia Gemma Rosende Silva, Juez Titular 8° Juzgado de Garantía de Santiago, estableció para los imputados en esta causa, la pena de: "Quinientos cuarenta y un días de presidio menor en su grado medio", así como la suspensión de cargo u oficio público por el mismo plazo de la condena, junto con el comiso de las especies incautadas, por su participación en la calidad de autores en el delito consumado de espionaje y sa*bot*aje informático, en calidad de reiterado, cometido durante el año 2013.

Por otra parte, se estableció que los culpables, concurrieron los requisitos señalados en el artículo 4 de la Ley N° 18.216, se concede a los sentenciados el beneficio de la remisión condicional de la pena, fijándose el plazo de quinientos cuarenta y un días de observación por la sección correspondiente de Gendarmería de Chile; dejándose constancia para los fines pertinentes en el evento de revocación de beneficio que registran haber estado sujetos a la medida cautelar de arresto domiciliario nocturno entre 22:00 horas de cada noche hasta las 06:00 horas del día siguiente, desde el 19 de noviembre del año 2013 hasta el 19 de marzo del año 2014.

Del mismo modo, se eximió a los condenados del pago de las costas, toda vez que aceptaron el juicio abreviado inmediato, aceptando también con ello, los hechos de la acusación y renunciando a su derecho a un juicio oral, el cual impondría una carga económica mayor para el Estado.

---

[31] La ingeniería social es un término más bien utilizado en el ámbito de las ciencias políticas, y fue llevado al campo de la informática por un reconocido hacker llamado Kevin Mitnick. Es muy común encontrar una definición clásica que dice que consiste en la manipulación inteligente de la tendencia natural de la gente a confiar.

Tal como se puede apreciar en la sentencia, se enmarca dentro de lo que la Ley, hoy establece para tales efectos, sin embargo, no existe posibilidad de que la pena sea superior, ya sea porque actuaban como una organización con una estructura clara, reunida para la comisión del delito, y tampoco existe la posibilidad cierta de una condena mayor, cuando los participantes poseen entrenamiento formal en el campo informático, lo cual debiese tener un peso superior, toda vez, que los imputados podían representarse claramente el alcance de sus actos, más aún cuando prestaban servicios para entidades bancarias donde manejaban los datos de todos los clientes, y menos que crearon dicha *botnet*, con la finalidad clara de cometer un ilícito.

CAPITULO 4

CONCLUSIONES

El desarrollo explosivo que ha experimentado el ciberespacio, especialmente por la extensión física que presenta la gran red redes, más conocida como Internet, la que prácticamente alcanza a casi todo el planeta, permitiendo llevar a cabo, millones de operaciones, desde aquellas más cotidianas hasta aquellas más complejas, sin necesidad de moverse de la comodidad de la casa o la oficina. En términos prácticos, estamos frente a una nueva forma de hacer aquellas cosas que tradicionalmente se venían realizando directamente en el mundo real, existiendo una interacción impensada a nivel social, que ha cruzado transversalmente todo el quehacer de la sociedad humana, estamos en plena era de la conectividad, y que cada vez se acentuará con más fuerza a partir de la Internet de las cosas.

Es indiscutible, que el ciberespacio presenta una expansión vertiginosa a nivel mundial, estado del cual, nuestro país no se encuentra ajeno. Los índices nos ubican dentro de los países que lideran a nivel sudamericano con la mayor cantidad de usuarios conectados a internet, lo que sin duda, también representa una mayor exposición al riesgo de convertirse en potenciales víctimas de algunas situación que podrían lesionar la tranquilidad emocional o patrimonial de una persona, toda vez, que esa maldad presente en el mundo real, se ha traspasado al mundo virtual, por lo que, el avance tecnológico también presenta una faceta negativa, constituyendo una oportunidad para aquellos que se dedican a delinquir.

En ese contexto, la aparición de diferentes tipos de códigos maliciosos, capaces de realizar muchísimas operaciones específicas, tales como: la extracción de información sensible, grabación de audio, o tomar una fotografía, todo de manera remota sin que al ojo del usuario pueda ser detectado, e incluso, en

desarrollos muchos más sofisticados, ni siquiera los sistemas de seguridad instalados para la protección de un sistema computacional, pueda advertir la presencia de un código malicioso, que esté operando sin el consentimiento del propietario, sobre un dispositivo computacional que haya sido infectado.

En esa línea, es muy común escuchar expresiones tales como: virus, *malware*, troyanos, gusanos, *botnet*, entre otros. En ese contexto, las *botnet*, representa una herramienta sofisticada desde lo técnico, que se destaca por su capacidad de distribución, multifuncionalidad, complejidad, las que fundamentalmente son utilizadas, para realizar denegación de servicio, obtención de credenciales válidas para posteriormente acceder de manera indebida a un sistema transaccional, ya sea para robar información, distribuir virus o códigos malignos en general. En la actualidad, es posible adquirir una *botnet*, a partir de varios miles de dólares, las que se enmarcan dentro de las denominadas amenazas persistentes avanzadas, orientadas justamente al sabotaje y espionaje informático, información que posteriormente podría ser utilizada para la comisión de algún delito ya sea informático o computacional.

Respecto de los códigos maliciosos, independiente del nombre que pudiera llevar, más bien su identificación dice relación con su forma de operar, pero finalmente su desarrollo es justamente para llevar a cabo, algún tipo de acción sin el consentimiento del propietario. A algunos de ellos, únicamente con la finalidad de causar algún tipo de daño en los archivos o en el sistema operativo del usuario afectado. Pero en su mayoría, poseen fines más bien criminales, y buscan obtener alguna recompensa ya sea económica, o bien lesionar o dañar la imagen de alguna persona, utilizando para ello, las redes sociales para la publicación de información comprometedora de la víctima. La cibercriminalidad ha crecido en cifras considerables. Según el último estudio de las Naciones Unidas, Chile alcanza cifras verdaderamente preocupantes, considerando que

nuestro país posee alrededor de un setenta por ciento de usuarios de internet. En términos generales, a la revisión de las estadísticas correspondientes tanto a las denuncias como las respectivas órdenes de investigar, dan cuenta de una curva que claramente va creciendo de manera exponencial, donde se pueden apreciar leves disminuciones muy puntuales, pero en general, el crecimiento es sostenido en el tiempo. Los indicadores, se ven favorecidos, fundamentalmente por dos fenómenos, el primero dice relación con que muchas personas dedicadas a la actividad delictual, han decido migran al espacio cibernético, ya que les reporta mayor seguridad para llevar a cabo sus acciones, e incluso gozan de un menor reproche social, toda vez, que su actividad supone un esfuerzo intelectual para la comisión de los mismos, y por otro lado, la baja penalidad que actualmente existe en la legislación, para este tipo de acciones.

La actividad en el mundo cibernético, representa sin duda, una nueva dimensión que requiere contar con mecanismos sólidos de protección, toda vez, que a través del mismo se llevan a cabo variadas transacciones que pudiesen afectar a una persona, de manera importante tanto a nivel patrimonial cómo a nivel personal, y que hoy día el actual marco normativo, no da respuesta de manera adecuada a las nuevas exigencias existente en el ámbito del crimen informático, por lo tanto, dejan en una especie de estado de indefensión a quienes se convierten en víctimas de ciberdelincuentes, debido fundamentalmente, porque no todas las acciones que son llevadas a cabo a través del ciberespacio y que buscan obtener algún provecho a través de acciones criminales, están tipificadas como tal, incluso la sola acción de iniciar un proceso judicial, no asegura que el responsable vaya a reparar su acción antisocial.

Tal como se dijo anteriormente, el marco regulatorio en nuestro país, relacionado con los delitos informáticos, no da respuesta de manera eficiente a los actuales escenarios a los que nos vemos enfrentados en materia de cibercriminalidad, primero porque exige un tipo de dolo especial, ya que no exige que se lleve a cabo la acción propiamente tal, sino además exige que se establezca la animosidad que tuvo el autor de las mismas, al momento de su comisión. Otro aspecto importante, es que frente a estos nuevos medios de comisión como es Internet, no esté tipificado de manera correcta lo relacionado con el fraude o estafa electrónica, utilizando de manera inadecuada la figura de la estafa actual, ya que no aplicaría a una máquina, dado que en términos práctico no puede ser engañada, más bien se accede introduciendo las credenciales válidas, ya que al que engañaron previamente fue al usuario. Así como tampoco, existe una normativa que establezca el abuso de dispositivos como una acción constituyente de delito, por lo tanto, hoy en día una persona podría ser detenida con tecnología como, por ejemplo, para vulnerar un cajero automático, pero el sólo porte de dichos elementos tecnológicos no constituye delito, si aún no los han utilizado.

En ese sentido, es posible apreciar esfuerzos significativos de alcance internacional, como los impulsados por las Naciones Unidas, que buscan justamente generar un espacio de discusión respecto del fenómeno a nivel mundial, y de alguna manera conforme a los compromisos adquiridos por los países miembros, quienes llevan a cabo estrategias a nivel local, justamente para luchar contra el crimen de origen informático. Otra acción muy significativa en el combate de la cibercriminalidad, lo representa el convenio de Budapest, impulsado por el Consejo de Europa, el cual busca justamente entre los países miembros estandarizar la normativa penal en materia de aquellos delitos que se lleven a cabo el espacio cibernético, planteando la persecución para la pornografía infantil, el fraude electrónico, acceso indebido, propiedad intelectual, y muchos otros. Los organismos internacionales han comprendido

que es necesario llevar a cabos esfuerzos mancomunados entre países para el combate de la delincuencia informática, a partir de los alcances de este fenómeno, el cual claramente es transfronterizo, y por lo mismo, dificulta su persecución, por no existir homogeneidad a nivel de su penalización a nivel global. Del mismo modo, se requiere contar con una coordinación a nivel mundial, que dé respuesta de manera eficiente a la hora de preservar la evidencia informática o bien que facilite la obtención de información para un proceso de investigativo posterior, de tal manera que no se diluya una investigación, todo porque el ataque en sí, operó fuera del territorio nacional.

A nivel de derecho comparado, en el caso como España, Alemania, Estados Unidos, es posible observar regulaciones muchísimas más específicas, y con penas muchos más altas, dependiendo los niveles de importancia de los sistemas comprometidos. En el caso español, se aprecia una definición importante, que hace referencia a los grupos criminales u organizaciones criminales, a los cuales se le aplicará penas superiores, situación que en nuestro país no se aprecia una diferencia, entre si una persona actúa sola, o bien se reúne con otros para formar una organización con fines criminales para operar a través de la red. Nuestro marco regulatorio, no hace un alcance de esa naturaleza. En el caso alemán, se aprecia también una gran diferencia, ya que no procedieron a crear una ley especial, sino más bien, introdujeron directamente las figuras relativas al aspecto informático en el código penal. En lo medular es posible destacar la existencia de la figura de la tentativa, lo cual guarda relación con el sabotaje informático, en esa misma línea, es dable destacar, la existencia de una definición relativa a la estafa electrónica, donde determinaron que existiendo perjuicio patrimonial, ya sea a través de la manipulación de una base de datos, la utilización de datos sean completos o incompletos, o mediante la utilización de datos no autorizados, entonces se estaría en presencia de una estafa informática, situación que difiere de nuestra realidad local, que no contempla el fraude o estafa electrónica como un delito.

En el caso de Estados Unidos, su normativa contempla penas de hasta diez años de cárcel en una prisión federal, más multa en el caso de aquellos que desarrollan códigos maliciosos, y una pena diferente para aquellos que únicamente lo distribuyan, como penas de multa, y a lo más un año de cárcel. Muy distinto a lo que ocurre en nuestro país, donde no existe una diferenciación entre quien crea y quien distribuye un determinado código malicioso, lo cual claramente está enfocado en hacer una diferenciación entre una persona con un nivel avanzado en términos técnicos y que utiliza su conocimiento a sabiendas en actividades de carácter ilícitas, no así aquel que únicamente toma un determinado código malicioso, y que busca obtener algún provecho para sí mismo, pero que no posee las condiciones para llegar a programar uno.

Otro aspecto más que relevante, y que podría constituir un camino real para el desarrollo de acciones coordinadas respecto del flagelo de la criminalidad cibernética, es justamente el desarrollo de la Política Nacional de Ciberseguridad, lo cual constituirá un hecho histórico en nuestro país, ya que permitirá definir estratégicamente aquellas acciones en materia de seguridad en el mundo cibernético, lo que además se traducirá en un impacto importante en la definición de estándares mínimos de seguridad, y por otra parte, obligará a la adecuación de los actuales cuerpos legales a dar respuesta más efectiva al fenómeno, por lo tanto, se debiese ver un cambio más que importante en la política criminal existente en esta materia, y el modo en que estamos haciendo las cosas como país.

Es muy común escuchar, que muchas personas creen que Internet, es un espacio que no posee ninguna restricción y que se podría hacer de todo, probablemente sea una concepción errada de la idea central que profesa la gran red de redes, que busca proteger el derecho al acceso de la información, pero que requiere necesariamente también proteger el derecho a la intimidad, lo que nos hace pensar, que debe asegurarse un equilibrio necesario entre ambos

derechos. El ciberespacio, debe necesariamente seguir siendo libre en términos de favorecer el proceso de democratización de la información, y de paso asegurar su consideración como derecho humano, situación que nos obliga a establecer niveles de protección adecuados en su uso. Lo mismo, debe ocurrir en el caso del Estado, donde debería estar delimitado claramente hasta donde podrá condicionar nuestro actuar en la red, sin atropellar nuestros derechos. Se hace necesario, la existencia de una potente coordinación a nivel internacional, liderada por algún organismo principal que actúe como un articulador frente a acciones que sean constituyente de algún tipo de delito de esta índole, para justamente evitar la impunidad, cuando el hecho punible, ocurra fuera del territorio nacional o incluso afecte a más de un país a la vez, lo cual debiese tender a la estandarización de la normativa legal, que por un lado fortalezca la protección a la intimidad, pero siempre con la posibilidad cierta de poder obtener datos que permitan identificar a un delincuente en el mundo virtual, y por ende la obtención de pruebas que den cuenta de un determinado acto ilícito ya sea un delito informático, computacional, o alguna acción que pudiese enmarcarse dentro de actividades ligadas al ciberterrorismo o ciberguerra, que podrían amenazar la tranquilidad de toda una nación.

Bibliografía

- Schiller, C. & Binkley, J. (2011). *Botnets: The Killer Web Applications.* Estados Unidos, Syngress Publishing.
- Clifford, S. (2000). *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*, Estados Unidos, Pocket Book.
- Kaspersky Security Bulletin 2015: Overall Statistics For 2015.
- Spamhaus. (2016). *The 10 Worst Botnet Contries.* Recuperado de https://www.spamhaus.org/statistics/botnet-cc/.
- White Ops and the Association of National Advertisers (ANA) 2016*, The Bot Baseline: Fraud in Digital Advertising*. Recuperado de https://www.google.cl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjlj5fy74fQAhVJgpAKHQozCUcQFggaMAA&url=http%3A%2F%2Fwww.ana.net%2Fbotfraud&usg=AFQjCNHDan_yk3XTWa7NJgkXJ_jc1LyHRw.
- No se aprecia el nombre del creador del sitio, (2013), recuperado de http://cardingmx.mforos.com/2106562/11536820-venta-de-botnet/.
- Hadnagy, C. (2011), *Ingeniería Social el Arte de Hacking Personal,* España, Anaya Multimedia.
- Banco Interamericano de Desarrollo (BID); Organización de los Estados Americanos. (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? (1). Recuperado de https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/.
- Ley N° 19.223. Diario Oficial de la República de Chile, Santiago, Chile, 07 de junio de 1993.
- Miller, T., Kim, A. (2016). «*2016 Index of Economic Freedom», 1, 484.*
- Naciones Unidas. (1993). *Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos.* Nueva York, Naciones Unidas.
- Brenner, Susan W. (2012) *La convención sobre Cibercrimen del Consejo de Europa. Revista Chilena de Derecho y Tecnología. Chile.*
- Convenio sobre Cibercriminalidad, Budapest, publicado el 01 de julio de 2004.

- Romina Moscoso Escobar. (2014). La Ley 19.223 en general y el delito de *hacking* en particular. Revista Chilena de Derecho y Tecnología, 3, 224.
- Malware: Fighting Malicious Code. Skoudis E., Zeltser L., 2003.
- Legal Issues in Botnet Mitigation. ENISA Report, to appear, 2011.
- Magliona, C. (1999). *Delincuencia y Fraude Informático: Derecho comparado y ley No. 19.223.*
- Wilson, C. (2008) «*Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*», recuperado de http://www.fas.org/sgp/crs/terror/RL32114.pdf.
- *Ranking Connectivity Scorecard*, (2013), Estados Unidos, recuperado de http://www.connectivityscorecard.org/countries/
- Revisión sobre la actividad TI en Chile, (2013), Chile, recuperado de http://www.acti.cl/files/ACTI-IDC-Indicador-Actividad-TI-en-Chile-2013.pdf
- El panorama de malware en América Latina en el 2013: pronóstico para el 2014, por Dmitry Bestuzhev, Noviembre 2013, recuperado de http://latam.kaspersky.com/Malware2013LatAm
- Indicador de la Sociedad de la Información (ISI) everis/IESE, 2012, recuperado de http://es.scribd.com/doc/87371891/Indicador-de-la-Sociedad-de-la-Informacion-ISI-everis-IESE