UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
DEPARTAMENTO DE CIENCIAS PENALES

# La Ley 19.223 a 26 Años de su Promulgación

Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

Susana Hiplan Esteffan

PROFESOR GUÍA:

Prof. Lautaro Contreras Chaimovich

SANTIAGO, CHILE

2019

# Resumen

Este trabajo de investigación para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, es un análisis pormenorizado a la legislación vigente en lo relativo a la criminalidad informática, particularmente a la Ley 19.223 del año 1993, que establece cuatro tipos penales.

En una primera parte, trata sobre el fenómeno global de la criminalidad informática; luego estudia la legislación penal comparada y las maneras de afrontar la criminalidad informática que otras legislaciones más vanguardistas en la materia han tenido; para luego enfocarse en la Ley 19.223 y hacer un análisis detallado de los cuatro tipos penales en ella contenidos, observando para esto, los tipos penales en toda su dimensión, tanto deontológica como ontológica.

Finalmente se analiza el último proyecto de Ley sobre la materia, presentado en Octubre de 2018 por el ejecutivo, a la luz del Convenio de Budapest sobre ciberdelincuencia, el cual nuestro país suscribe.

# TABLA DE CONTENIDO

# I. Primera Parte: Introducción.

## 1.1. Definiciones y nociones sobre informática.

Etimológicamente, la palabra *informática*, proviene del acrónimo francés *Informatique*, que a su vez se compone de dos palabras, “information” y “automatique”, es decir; Información automática. Este vocablo, que en la actualidad nos parece tan familiar, no siempre lo fue. La informática es conocida simplemente como “computación” en términos coloquiales y corresponde a la ciencia que estudia el procesamiento, almacenamiento y transmisión de datos digitales; es decir, aquellos que son producidos mediante computadoras. Para llegar al nivel de sofisticación informático actual, en que los ordenadores son parte indispensable de la sociedad actual, tuvieron que pasar un par de décadas.

Todo comenzó con la interconexión de los ordenares, con la finalidad de compartir y traspasar información, que tuvo su origen en la idea pionera de un pequeño grupo de científicos del MIT durante la década de los años 60. Esta interconexión de ordenadores comenzó mediante una red local que comunicaba estos aparatos entre dos universidades distintas del Estado de California (UCLA y Stanford), a través de redes físicas, y utilizando un lenguaje o código (también llamado protocolo) común. Esta primera red de ordenadores interconectados en tiempo real se llamó ARPANET[1]. Y su creación se atribuye a la

[1] ARPANET es una sigla que proviene del acrónimo ARPA, en inglés DARPA y que cuyo significado corresponde a *Advanced Research Projects Agency Network.*

necesidad que tenía ARPA (hoy renombrado DARPA)[2], de obtener una red estable y de conexión segura (que no fallara) ante la amenaza de un ataque militar de cualquier tipo contra los Estados Unidos, incluso nuclear.

Con el éxito que tuvo aquella primera interconexión de ordenadores, un par de científicos del MIT diseñaron una teoría de transmisión de datos de alta velocidad que pronto fue llevada a la práctica exitosamente, hecho que ocurrió en el año 1972, y que permitió la comunicación y transmisión de datos entre universidades y empresas, ganando rápidamente una amplia popularidad entre académicos, estudiantes y personal del mundo privado. Ya en el año 1972, se crearon los protocolos transparentes IP y TCP (los del ejército estadounidense eran lenguajes codificados), para en las siguientes décadas llegar a estandarizar todos los protocolos de comunicación entre ordenadores, crear la primera red en árbol (no lineal) de conexión informática, y para ya finalmente en la década de los 90, crear el primer "cliente web"[3] la World Wide Web, mejor conocida como WWW, y el primer servidor de internet[4]. Hechos ambos de magnitud revolucionaria. Gracias a ellos ya no era necesario tener programas específicos, sino que todos los programas (ahora con protocolo común) fueron unificados para acceder desde aquél mismo cliente.

Por supuesto, todos estos avances supusieron la paulatina y eventualmente potencial masificación que la interconexión de ordenadores ha tenido. Ya sabemos que partió de

---

[2] DARPA es el acrónimo de la *Defense Advanced Research Projects Agency,* organismo del departamento de defensa estadounidense, que se encarga de investigar nuevas tecnologías para el ejercito de dicho país.

[3] Por "Cliente" se entiende un programa computacional que se conecta a un servidor, que es una unidad física de almacenamiento de información, desde la cual extrae datos y los lleva hacia el denominado "host", (huésped) que viene a ser la unidad informática (computador, smarthphone, etc) que la solicita.

[4] Ambos desarrollados por el CERN, *Centro Europeo para la Investigación Nuclear*, durante la década de los 90.

manera lineal conectando un par de equipos entre dos universidades del Estado de California, y de a poco, es que hemos llegado a tener acceso a internet hasta en los lugares más recónditos del mundo. Hoy, se estima que alrededor de un 95 de la población mundial tiene acceso a la internet a través de un móvil.[5]

No fue sino hasta el comienzo del presente milenio, que la masificación de la utilización de las redes de transferencia de datos en tiempo real, alcanzó niveles de expansión exponenciales. El acceso a internet, ya no sólo desde ordenadores, sino que desde una variada gama de aparatos tecnológicos, es algo sin lo cual no podemos concebir nuestra cotidianidad. Hoy, los medios informáticos forman parte esencial de nuestro desenvolvimiento en la sociedad contemporánea. No sólo nos comunicamos y llevamos a cabo parte importante de nuestras relaciones interpersonales a través de soportes informáticos, sino que también realizamos transacciones bancarias, operaciones de compra venta, celebramos contratos de todo tipo con el sólo presionar un botón, y nos enteramos en tiempo real de acontecimientos que están sucediendo al otro extremo del globo. Incluso se han creado monedas cuyo único soporte es electrónico[6].

La masificación de internet es un fenómeno tecnológico de incidencia socio-cultural tal, que probablemente muchos años van a tener que pasar antes de que seamos capaces de darnos cuenta del real impacto que esta tecnología vino a significar para nuestra

[5] ITU ONU. (2016). La UIT pública las cifras de 2016 de las TIC. 18 de enero de 2017, de Organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación Sitio web: http://www.itu.int/es/mediacentre/Pages/2016-PR30.aspx

[6] Bitcoins, Chaucha, entre otras.

civilización. Se habla ya de un cambio de era, estamos hoy viviendo la Era Digital[7], era en la que la criminalidad ha traspasado las fronteras físicas y se ha desarrollado de manera paralela a los delitos tradicionales, trayendo consigo un nuevo universo en el que delinquir, nuevos bienes que el Ordenamiento Jurídico debe proteger, y la necesidad de crear un nuevo catálogo de delitos que tipifique aquellas conductas lesivas que se den en el orden digital.

### 1.2. Contexto e historia de la Ley 19.223.

El fenómeno digital ha conllevado que en la actualidad llevemos a cabo parte no despreciable de nuestra vida a través de internet; muchos de los aspectos de esta se ven traspasados al soporte digital, lo que implica por supuesto, tanto lo deseable, como lo indeseable. La criminalidad es un ejemplo muy claro de esto.

Con el devenir de los avances tecnológicos, viene aparejada la evolución del comportamiento que las personas tomamos frente a las nuevas tecnologías, así, se diversifica la cantidad de cosas que podemos hacer estando frente a una pantalla, incluyendo el catálogo de conductas que podrían potencialmente revestir caracteres de delito. Atendido esto, fue que durante el año 1993, la cámara alta de nuestro parlamento, aprobando una moción presentada por el senador José Antonio Viera Gallo, legisló sobre los

[7] Fuchs, C. (2008). Internet and Society: Social Theory in the Information Age. Austria: Routledge.

delitos informáticos, ya que según la moción del proyecto de ley, ya incluso en aquella época, no existía *"organización social compleja que pueda prescindir de la utilización de sistemas automatizados de tratamiento de la información*[8]" y según él mismo, el proyecto de ley tenía por finalidad *"proteger este nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales: la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan*."[9] De la primera cita de la moción del Senador Viera Gallo, podemos inferir que la utilización de sistemas informáticos interconectados a internet en unidades de trabajo, ya era imprescindible hace casi dos décadas y medias; así como también podemos inferir que el fenómeno de la criminalidad informática ya constituía una amenaza latente hacia estos sistemas. Ya decía el diputado *"si maliciosamente se destruye o altera el sistema de información de una AFP, de un banco, de Codelco, de cualquier institución grande del Estado, del Registro Civil, el perjuicio que se producirá será incalculable. En la práctica, estaremos en presencia de una forma más refinada de acto terrorista".*[10] El pasar del tiempo no ha hecho sino confirmar los temores del legislador.

La gestación del proyecto de la Ley 19.223 tiene su origen en la presentación de dos anteproyectos de ley que buscaban dar cabida en nuestra legislación a un nuevo tipo de bien jurídico protegido. A saber, "los sistemas informáticos" y la información en ellos contenida. Ambos proyectos, de extensión considerablemente mayor que la ley en rigor, no alcanzaron

---

[8] La historia de la Ley 19.223 está disponible en el enlace https://www.leychile.cl/Navegar?idNorma=30590

[9] Ibíd.

[10] Ibíd.

los trámites legislativos mínimos para poder discutirse y fueron simplemente retirados. Esto puede deberse, ya a que los legisladores de la época efectivamente creían que era innecesario tipificar tan extensamente sobre la materia, o pudo deberse a que debido a la complejidad de aquellos, los legisladores no llegaron a comprenderlos bien. Pudo incluso deberse a que no llegaron a vislumbrar que la criminalidad informática iba a convertirse en un fenómeno de lesividad y frecuencia de comisión muy similar al de la criminalidad común que opera en el mundo físico.

Es ya en el año 1993 que el diputado Viera Gallo presenta el proyecto que finalmente será promulgado como la Ley sobre la que versa este trabajo.

La Ley 19.223, tal y como da cuenta su fidedigna historia, fue un proyecto de Ley bastante discutido en lo relativo al establecimiento de tipos penales que no formaran parte del código penal, ni en la forma de nuevos artículos, ni en la forma de artículos ampliados o re redactados. Fue precisamente el punto recién tratado, aquél que convenció al senador Viera Gallo y a los demás parlamentarios que apoyaron la moción, de decantarse por la técnica de la ley complementaria, y no por la codificación, pues ante la sugerencia recibida por parte de algunos miembros de la comisión de añadir disposiciones relativas a la criminalidad informática, a tipos penales ya existentes en el código penal, decía el legislador *"para la historia de la ley, deseo reiterar lo dicho por el diputado informante, en el sentido de que el bien jurídico protegido con el proyecto es un sistema de almacenamiento de información, según la técnica de la informática, y no un método para cometer otros delitos. Eso fue lo que llevó a la comisión – como lo ha expresado el Diputado señor Espina- a optar*

*por una ley especial y no por incorporar los tipos al código penal, como proponía el Gobierno en un primer momento".*

Como es de inferirse de la anterior cita, en la época en que el Diputado Viera Gallo presentó su proyecto de ley, el desconocimiento sobre la criminalidad informática y sus características en nuestro país era tal, que no se entendía si la tipificación sobre ellos debía ser simplemente la misma que para el catálogo de delitos tradicionales, con la técnica de añadir algún acápite a artículos existentes, o incluso, si es que quizá no era necesario añadir nada, sino que bastaba someramente con una interpretación extensiva de los tipos tradicionales.

El diputado que presentó el proyecto, explica al introducir su moción legislativa, que en países como Estados Unidos, Francia, Alemania, Austria y Suiza, la legislación del ciber crimen había surgido en la forma de tipos penales específicos, tomando bajo el alero de protección del derecho penal, nuevos bienes; a saber, los sistemas informáticos per se y la información en ellos almacenada. Esta era entonces, la tendencia internacional.

Se observa del todo razonable este camino de acción, pues si bien la criminalidad informática es el traslado de la criminalidad tradicional al este nuevo ámbito en que también desarrollamos nuestra vida, el soporte informático en que desarrollamos esta parte, es mayoritariamente aquello que se ve atacado por los ciber delincuentes.

Fue tal el nivel de desacuerdo, que el mismísimo ejecutivo tuvo a bien sugerir una modificación llevada a cabo sobre el Código Penal, y el ministro de Justicia de aquella época, dijo no estar convencido de que la técnica legislativa escogida fuese la más adecuada.

Esta ley fue fruto de acaloradas discusiones en muchísimos ámbitos. Desde el cuestionamiento a si su promulgación era la manera más efectiva de atacar el fenómeno de la criminalidad informática, hasta la realización de indicaciones pormenorizadas a palabras específicas sobre cada uno de sus artículos. Fue sujeto de consulta a la Comisión de Constitución, Legislación, Justicia y Reglamento, y varias opiniones técnicas fueron consultadas. Finalmente, el día 7 de Junio de 1993, se promulgó la Ley 19.223 que "Tipifica figuras penales relativas a la informática." Con ella, Chile creó una ley simple y escueta que establece cuatro tipos penales que buscan sancionar el sabotaje al funcionamiento al sistema informático, el espionaje a estos sistemas y la revelación de información obtenida desde un sistema sin la autorización para hacerlo. Se tipifican de igual modo, conductas que atenten contra la protección de los datos contenidos en los sistemas informáticos, y es esta tipicidad objetiva, la que trae aparejadas las penas más altas, por considerarse los peligros relativos a la obtención y manejo de la información almacenada, los potencialmente más dañosos.

En un principio, esta ley se pensó como el primer paso hacia una legislación complementaria relativa al ciber crimen. Fue ideada como la puerta de entrada hacia la creación de un conjunto de normas que buscaran fortalecer la normativa relativa al ciber crimen en amplio espectro, fortaleciendo incluso leyes sectoriales tales como las de propiedad intelectual (siempre en su dimensión informática); sin embargo desde su promulgación, son comparativamente, pocas las veces en que se ha fallado en base a ella[11]. No ha resultado ser una norma de aplicación práctica extensiva, al punto de que incluso se le

[11] La base de datos jurídicos Vlex.com sólo registra 114 fallos que contengan al menos la mención de la citada normativa (al 5 de diciembre de 2016).

han propuesto modificaciones[12] a través de los años, aunque ninguna aún con éxito. Este hecho, es del todo factible de atribuir, entre otros factores, a la rapidez con que estas formas de criminalidad evolucionan, ya que van adquiriendo la misma sofisticación que los soportes materiales e inmateriales en los que operan. Y así, tenemos que una ley promulgada hace ya más de veinticinco años, probablemente ha quedado obsoleta, y las intenciones de que fuese la puerta de entrada hacia una legislación sofisticada y acorde a la evolución tecnológica, del todo abandonadas.

### 1.3. Evolución de la criminalidad informática.

La evolución que la criminalidad informática ha sufrido es fascinante y a la vez, aterradora. Implica dilemas terribles y desde su aparición, no ha podido ser detenida. Por "Cibercrimen", entendemos aquellas formas de criminalidad que se dan sobre y a través de un soporte informático conectado a la red. El informe técnico presentado ante la cámara de diputados de nuestro parlamento durante las discusiones previas a la promulgación de la Ley 19.223, describió a la criminalidad informática como *"Delitos que tienen notas o características especiales, no se requiere la presencia del autor del hecho en el lugar de la comisión, la manipulación puede hacerse a distancia, el delito no conoce fronteras y*

[12] Proyecto de Ley que tipifica figuras relativas a la informática presentado el 12 de febrero del 2015 en la cámara de diputados.

*cualquier persona o empresa que tenga un computador y un enlace telefónico puede ser víctima de un delincuente computista."*[13]

A su vez, Interpol divide el ciber crimen en 2 aristas[14]: *Advanced Cybercrime* que viene a ser el Cibercrimen organizado, o de alta tecnología, y que corresponde a sofisticados ataques contra sistemas informáticos conectados a la red, tales como aquellos perpetrados a gran escala durante el 2017, año que será recordado como *"aquél en que la ciber seguridad se tomó el escenario central en los medios alrededor de todo el mundo, año del que aprendimos que cualquier persona y cualquier compañía puede ser víctima de ciber crimen, desde los medios de comunicación, los medios de producción, las aplicaciones de viajes, los bancos, las plantas de producción eléctrica o las organizaciones de la salud. Los ciber criminales no demuestran compasión"*[15]

La otra arista en la que Interpol divide el Ciber crimen es la de mayor data, el *Cyber-Enabled Crime,* el cual corresponde a aquellos delitos del mundo fenomenológico que con obvias variaciones en su plataforma de comisión, han visto trasladado su comisión al ciberespacio, a saber, crímenes de orden financiero, crímenes en contra de menores de edad, atentados contra la libertad sexual e incluso, formas altamente sofisticadas de terrorismo, entre muchos otros.

---

[13] La historia de la Ley 19.223 está disponible en el enlace https://www.leychile.cl/Navegar?idNorma=30590

[14] Interpol. (2015). Cybercrime. 10 de diciembre de 2016, de Interpol Sitio web: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

[15] Nick Ismail. (2018). 2017 – the year that defined cybercrime. 27 de Agosto de 2019, de Bonhill Group Plc Sitio web: https://www.information-age.com/2017-year-defined-cybercrime-123470158; Traducción Libre.

Llegados al punto que el desarrollo de la tecnología ha alcanzado en nuestra civilización, llevamos tantos años escuchando términos como “hacking” que lisa y llanamente no cuestionamos su calidad delictual, mas no siempre fue así. De hecho, en sus orígenes, el hacking era simplemente un término que hacía referencia a modificaciones en los sistemas, sin que esta acción fuese relacionada con un efecto dañoso. Para entender esto, es menester remontarse a la década que vio nacer a la Internet, los años 60. Fue durante las primeras conexiones entre universidades, que científicos del MIT crearon maneras de modificar, reparar o mejorar las funciones de los programas informáticos que ellos mismos desarrollaban, sin la necesidad de rediseñarlos. Un “hack” era una manera ingeniosa de reparar un producto informático. La connotación negativa actual del término proviene de una década más tarde, cuando en 1970 un grupo de hackers descubrió los códigos necesarios para realizar llamadas de larga distancia internacional sin pagar, a través de teléfonos pioneros en largo alcance. Esta fue la primera vez que se habló de delitos informáticos.

Este hecho marcó un hito, puesto que enfrentó a las autoridades a una nueva realidad delictual para la cual no tenían herramientas ni maneras de hacer frente. Ese fue el punto de quiebre en que las autoridades de los Estados Unidos se dieron cuenta de que se encontraban frente a hechos que al parecer estaban fuera de los márgenes de la ley, pero para los cuales no existían herramientas legales que utilizar para hacerles frente.

Entrada ya la década los años 80, hizo su aparición el *worm*, programa informático desarrollado con finalidades de espionaje por científicos localizados en Alemania que entregaban la información a la KGB. Esto significó una dimensión a otra escala en términos de criminalidad informática. Ahora el blanco era la seguridad nacional.

A partir de la década de los 90, la criminalidad informática ya era un fenómeno conocido y al cual se estaba tratando de hacer frente. Ya en la moción de la Ley 19.223 el diputado Viera Gallo hacía mención a los países, en su mayoría desarrollados, que ya habían legislado tipos penales que hicieran posible la persecución de las nuevas formas de criminalidad informática. En aquella época, los métodos más empleados en la comisión de este tipo de delitos, eran el *Data Diddling*, que consistía en la alteración de datos; el *Trojan Horse*, que correspondía a un worm o gusano que estaba diseñado para inmiscuirse en un sistema informático y alterar su normal funcionamiento; eran, del mismo modo, frecuentemente empleadas las *Salami Techniques*, que entraban también a la categoría de delito financiero, pues eran programas que sustraían pequeñas cantidades de dinero desde distintas cuentas hasta juntar grandes cantidades en la cuenta del autor del hecho dañoso. Las *Trap Doors* consistían en generar interrupciones en el funcionamiento lógico de un programa, sin ninguna finalidad de beneficio personal, como si era el caso de las *Salami Techniques*. El *Data Leakage* es probablemente, el único delito informático que proviene de aquella época que ha aumentado exponencialmente su frecuencia de comisión, y que se ha visto aumentado a gran escala. Consistía en la utilización de trojan horses o worms para obtener sin autorización información almacenada en un sistema informático. Hoy se utilizan métodos de alta tecnología y sofisticación para obtener información almacenada en cualquier lugar del mundo, muchas veces protegida por enormes barreras de seguridad.

El catálogo de delitos informáticos frecuentes en 1993 no se agota en las formas de criminalidad recientemente descritas; hace ya veinte años la creatividad de los ciber delincuentes era digna de admiración. Según las definiciones que da interpol, los ciber

delincuentes sólo han ido avanzando en el desarrollo de sus técnicas y programas. Hoy se cometen los mismos delitos que en los años 90, pero de maneras muchísimo más sofisticadas, cuestión que no sólo es consecuencia de la lucha estatal contra el cibercrimen, sino que además lo es de la lucha contra el ciber crimen que algunos programadores han comenzado en contra a sus colegas de la vereda del frente, en algo que podríamos definir como una *auto tutela cibernética organizada*; Y es producto, del mismo modo, de la preocupación que este fenómeno ha levantado – con justa razón- entre los Estados del mundo, que se han adaptado diversas facciones, -aunque aún insuficientes- de su institucionalidad para poder hacerle frente.

1.4. Nociones de Derecho comparado sobre Ciber crimen.

El Ciber crimen corresponde a una forma de criminalidad distinta a los tipos contenidos en el catálogo de delitos tradicionales, lo cual por supuesto, implica que su tratamiento no puede ser el mismo que para el catálogo tradicional del Derecho Penal. Estamos ante la presencia de delitos que atentan contra otra clase de bienes jurídicos protegidos, cuyas características no podrían ser más disímiles a las de los delitos tradicionales. Sabemos ya que en los delitos informáticos, el autor del hecho dañoso no se encuentra en el lugar en que los hechos se desarrollan, ni tampoco, en el que producen sus efectos. Sabemos así mismo, que es menester que tanto el autor como la víctima tengan un sistema informático con acceso a la red, para que el delito pueda cometerse, y sabemos también que, con el avance de la tecnología en este campo, las formas de comisión van

adquiriendo niveles de sofisticación cada vez mayores. Un punto importantísimo que ha supuesto especiales aprietos para los legisladores, es el espacio temporal en que se desarrolla la comisión del delito. *"It is particularly worrying that the lenght of time for a cybercrime opportunity to turn into a cybercrime wave is now measured in hours and minutes rather than months and years."*[16] Por otro lado, la victimización que este tipo de delitos produce, alcanza a tomar tintes omnipresentes, y esto implica una serie de problemáticas a las que los gobiernos y los legisladores se ven enfrentados a la hora de idear el tratamiento penal que este tipo de delitos debe tener.

Hasta ahora, lo que los legisladores en el derecho comparado han hecho, es esperar a posicionarse frente a un hecho lesivo de características uniformes, y de alta frecuencia de comisión, para luego tipificarlo. Pero siempre está latente la posibilidad de formular una agenda pre-comisión, que trate de adelantarse a las nuevas potenciales formas de criminalidad informática, posibilidad que es observada con suspicacia por sectores de la doctrina.

Los Estados Unidos fueron el país en que nació la internet y en el que su uso doméstico se masificó. Son también, por supuesto, el país en que nació la ciber criminalidad. Se vislumbra del todo lógico que si fue en los Estados Unidos donde Internet se masificó, y donde el Cibercrimen tiene sus orígenes, es allí donde también comenzaron los primeros intentos por tipificar este tipo de conducta. En 1986, se promulga la primera ley federal llamada *Pronunciamiento sobre Abuso y Fraude Informático*[17]*,* que tipifica este tipo de

[16] Giddens, A & Sutton, J. (2010). Sociology: Introductory Readings. Cambridge: Polity Press.

[17] United States Code. Title 18 - Crimes and Criminal Procedure. Chapter 47 - Fraud and False

conducta y que puede ser utilizada en la mayoría de las conductas delictuales de este tipo, ya atentasen contra sistemas privados o gubernamentales. Esta acta fue ampliada en el año 1994, y en general prescribe un catálogo de delitos culpables ante las cuales el gobierno Federal está facultado por para aplicar extensamente el rigor de la ley. Ha resultado ser una herramienta efectiva para el combate contra el Cibercrimen a nivel federal.

El 5 de enero de 1988 entró en rigor la ley nº 88-19 de "Fraude Informático" en Francia. Esta es una legislación muy peculiar. Acoge una noción amplísima de "fraude informático" a la vez que aplica para delitos tradicionales del catálogo penal cuando estos presentan características informáticas y de virtualidad. *"La ley de reforma francesa se concibe materialmente como una vía para reprimir accesos abusivos a los sistemas informáticos y actuaciones ilícitas sobre los datos informatizados y su tratamiento, se produzca o no un perjuicio."* Tenemos por tanto, que en Francia, tanto como en Estados Unidos, el legislador se decantó por una formulación de tipos cuyo tratamiento es culposo, y no doloso.

En Francia, en gran medida producto de esta legislación, la totalidad de los ilícitos que utilizan un sistema informático como medio para la comisión del delito, así como también, aquellos que tienen como objetivo el ataque a un sistema informático, entran en la categoría de "fraude informático". La regulación francesa sobre la materia aporta una visión del tratamiento del fenómeno de la criminalidad informática muy distinta a la generalidad del resto, lo cual es observable sobre todo en el tratamiento que otorga al delito de estafa, en que el tratamiento que le da el Código Penal francés a este delito es extensible al fraude

---

Statements. Section 1029

informático de contenido patrimonial. Esta particularidad, que no se observa en otras legislaciones, se atribuye a la formulación del tipo de Estafa, que se centra en las "maniobras fraudulentas" y en el "perjuicio" en vez del "engaño" y el "error".

Gran Bretaña fue el siguiente país en legislar al respecto con el *Computer Misuse Act* de 1990, el cual fue el producto de un controversial caso sobre data leakage en el que incluso se vio envuelta la casa real[18]. El *Misuse Act* se compone de 3 secciones que establecen tipos penales que buscan penar el acceso a material contenido en un sistema informático, el acceso con la intención de realizar modificaciones a un sistema informático y, en tercer lugar, la modificación de material computacional[19]. El *Misuse Act* fue muy criticado desde su promulgación, y se le han realizado varias modificaciones. Pero a pesar de esto, ha sido utilizado como modelo por distintos países que inician su lucha contra el Cibercrimen. Su última enmienda data del año 2015, y su blanco son los *Serious Crimes,* aquellos que revisten mayor lesividad.

La Legislación neerlandesa de delitos informáticos, conocida como *Computer Crime Act* entró en rigor el día primero de Marzo de 2016. Con anterioridad a esa fecha, los Países Bajos eran un paraíso para los Hackers. Esta ley fue objeto de un largo debate sobre la factibilidad de la información almacenada en un sistema informático de ser o no un bien en el sentido penal de la palabra. El parlamento holandés estimó que no lo era, pues cuando se es privado de un bien, dejamos de tener su posesión, y en el caso de los datos almacenados

[18] Caso *R v Gold & Schifreen.*

[19] Computer Misuse Act. (http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences/enacted)

que son objeto de data leakage o hacking, esto no ocurre (cuestión que al presente año 2019, y teniendo en cuenta las nuevas formas delictuales informáticas, es muy discutible).

Esta ley fue el producto de un trabajo de 3 años de estudio y discusión, y entre otras cosas, establece tipos para las ofensas contra la confidencialidad, la integridad y la disponibilidad de sistemas computacionales, además de interceptación ilegal e interferencia en los datos de un sistema computacional. Por otro lado, trata también de delitos tradicionales pero relacionados a sistemas computacionales, como grooming, suplantación de identidad y robo de datos personales, entre muchos otros. Es, de las legislaciones analizadas, la más extensa. *"It should also be observed that the Netherlands has been a frontrunner in cybercrime legislation in some respects, particularly with its provisions on procedural law dating from the Computer Crime Act of 1993"*[20], así como también es necesario destacar que la legislación penal relativa al cibercrimen en los Países Bajos *"has been, or is being, updated to meet the standards of the international treaties and conventions to which the Netherlands is a party."*[21]

Por otro lado, en España, *"el legislador español partió de la base de regular el problema informático específicamente y optó por la modificación de los tipos tradicionales completándolos con las necesidades requeridas para adaptarlos a las peculiaridades del*

[20] Koops, Bert-Jaap. (25 Julio de 2010). Cybercrime Legislation in the Netherlands. Country report for the 18th International Congress on Comparative Law, Washington, DC, 25-31 July 2010, session 'Internet Crimes, 18th, 40. 9 de Diciembre de 2016, De SSRN Library Base de datos.

[21] Los Países Bajos ratificaron el Convenio de Budapest para la Ciberdelincuencia el año 2006.

*delito informático*[22]. Esto queda plasmado en la Ley Orgánica n° 10/1995 del 23 de noviembre 1995, en la cual el legislador español, se decantó por la técnica legislativa contraria a la cual adoptó el legislador chileno; Tipificando los delitos de corte informático en el Código Penal, mediante la extensión de los tipos tradicionales, así como en la introducción de tipos nuevos. Esta normativa la encontramos en el Código Penal español, título X que trata Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, también en el título XI de los delitos contra el honor, en el título XIII de los delitos contra el patrimonio y el orden socioeconómico, y en el título XVIII, de las falsedades.

Este tratamiento de la legislación informática en España fue sujeto de una reciente reforma del Código Penal tras la Ley Orgánica 5/2010 de 22 de Junio de 2010, y de una más antigua, la Ley Orgánica 1/2015, del 30 de Marzo de ese año. Estas sucesivas modificaciones han respondido a las lagunas punitivas que la legislación originaria trajo aparejadas, así como también a las dificultades que la ley nº 10/1995 tuvo a la hora de ser empleada para perseguir los delitos que buscaba castigar. *"El esfuerzo del legislador de 1995 de integrar y adaptar lo máximo posible los nuevos delitos informáticos a los tipos delictivos tradicionales (estafa, daños, violación de secretos, etc.), pareció responder a la idea de que la llegada de las nuevas tecnologías hubiese comportado un cambio de las modalidades de agresión a los bienes jurídicos clásicos, recurriendo a la creación de artificiosas y poco apropiadas formulaciones legislativas y a una discutible ubicación*

[22] García, J. (Mayo-Agosto 2008). El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, 74, 289 - 308.

*sistemática de los nuevos delitos informáticos dentro del Código Penal"*[23]. La reforma introducida por la Ley Orgánica Constitucional 5/2010 introdujo dos nuevos tipos penales, la reforma 1/2015 elimina algunas, crea otros varios, reformula anteriores y elimina una categoría completa de graduación delictual para este tipo de criminalidad.

El constante cambio que las legislaciones penales extranjeras experimentan en cuanto al tratamiento que dan a los delitos informáticos, es un claro signo de que la legislación relativa a esta materia requiere de una revisión constante y detallada, en cualquier país del mundo en que el acceso a internet se encuentre masificado. En nuestro país, muy especialmente, la legislación penal vigente que busca combatir la ciber delincuencia lleva más de 26 años sin modificarse; Esa es la cantidad de años que nuestra legislación lleva sin cumplir de manera satisfactoria la protección de los bienes jurídicos que ataca la ciber criminalidad.

"*According to the 2019 Official Annual Cybercrime Report, cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind."*[24]

La criminalidad informática, se está volviendo, la principal amenza a la que se enfrentan las compañías y los Estados del mundo. Se hace perentorio contar con

---

[23] Salvadori, I. (2011). Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado. Anuario de Derecho Penal y Ciencias Penales, VOL. LXIV, 222-252. 10 de Diciembre, De Agencia Estatal Boletín Oficial del Estado Base de datos.

[24]Steve Morgan, Editor-in-Chief Cybersecurity Ventures. (2019). 2019 Official Annual Cybercrime Report. 3 de Septiembre de 2019, de HERJAVEC Group Sitio web: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

herramientas legales eficientes que permitan hacerle frente, y como hemos podido comenzar a vislumbrar, la legislación chilena relativa al bien jurídico protegido en cuestión, que se compone en exclusiva de la Ley 19.223, no parece estar a la altura de lo que se requiere dadas las circunstancias globales.

## II. Segunda Parte: Análisis de los cuatro tipos penales de la Ley 19.223.

La legislación relativa al cibercrimen, es decir, relativa a aquellas formas de criminalidad que atentan contra bienes informáticos, en Chile la encontramos únicamente en la forma de la Ley 19.223. Como ya se ha establecido, el legislador de la época se decantó por la formula legislativa de una ley especial, en vez de realizarle una modificación a nuestro Código Penal, para lo cual se argumentó que el bien jurídico protegido en los tipos penales relativos al cibercrimen correspondería a bienes distintos a los tradicionalmente contemplados en los tipos del Código Penal; a saber, este nuevo bien jurídico protegido correspondería a los sistemas informáticos per se (entendidos genéricamente) y no a una nueva forma de comisión de delitos que afectasen a los bienes jurídicos tradicionalmente protegidos, lo cual conllevaría en opinión del legislador, a que la técnica legislativa de la reformulación de los actuales tipos del Código Penal fuese inadecuada, por proteger estos, bienes jurídicos de una naturaleza completamente distinta.

## 1.1. Análisis individual de los cuatro tipos penales de la Ley 19.223

Artículo 1°: *El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.*

### Tipicidad Objetiva

a. Conducta Punible

Como podemos desprender de la lectura del precedente artículo, este tipifica un delito de resultado, que castiga la conducta que traiga como consecuencia la destrucción o la inutilización, tanto de un sistema informático, como de la información en él contenida; y lo hace extensivo a los componentes de un sistema informático individualizados. Por lo tanto, la conducta punible descrita en el Artículo primero de la Ley 19.223 abarca conductas lesivas hacia un bien tangible de orden computacional e informático incluyendo de manera individualizada todas las piezas que pueden potencialmente componerlo. Desde la placa madre hasta un simple puerto USB, tanto como de un bien intangible, el cual corresponde a la información y los datos que en aquél sistema se encuentren almacenados. Esta descripción amplia que realiza del tipo el artículo primero, supone una amplia

discrecionalidad para los jueces que conozcan de una causa, puesto que les faculta para conocer y declarar su admisibilidad ampliamente. Por ejemplo, si alguien rompe la unidad óptica de un computador, la ley, interpretada literalmente, faculta al dueño de ese sistema informático cuya unidad óptica fue dañada para querellarse por este artículo. Por supuesto, esto da cuenta de la deficiente redacción del artículo, puesto que el bien jurídico protegido abarca piezas del sistema informático que no pueden considerarse como circunscritas al bien jurídico protegido que el propio legislador declaro como objeto de esta ley (según la propia historia fidedigna de esta que custodia el ilustre congreso nacional), como lo vendrían siendo cables, pantallas, o cualquier remota pieza de hardware que no sea esencial al ordenador. Es un artículo que da lugar a vaguedades, que hace necesaria la interpretación judicial, y teniendo en cuenta que el principio rector de nuestro Ordenamiento Jurídico Penal corresponde al Principio de Legalidad, es una redacción que acarrea la ineficiencia de la norma para cumplir con la finalidad de protección de estos nuevos bienes jurídicos relevantes que con esta legislación se quisieron resguardar.

La redacción de este artículo tiene su parte más interesante al final, pues es en las últimas líneas donde dispone que la información que resulte destruida o dejada inutilizable debido a una conducta maliciosa debe ser castigada. Aquí es importante hacer un paralelo sobre cómo funcionaba el mundo de la informática hace 20 años. A saber, no existían grandes servidores que funcionaran como bodegas de almacenamiento de datos, cuestión que si ocurre hoy en día en los denominados “Data Centers”. Por lo tanto, toda la información era almacenada en unidades físicas llamas “Disquetes” y luego en unidades ópticas llamadas “CD-Room”, pero principalmente era almacenada en los discos duros de

cada computador o sistema informático, por lo que su destrucción o afectación que la hiciera inutilizable, ya que no existían respaldos de ella en la propia internet. Esto hacía prácticamente imposible volver a acceder a ella. Por supuesto, hoy en día, es prácticamente imposible deshacerse de la información que es subida a internet. Estamos viviendo la paradoja contraria.

Es este segundo inciso del artículo primero, el que contribuiría a su mayor aplicación práctica el día de hoy, puesto que de la simplicidad de su redacción, es posible la obtención de un silogismo judicial en que el supuesto típico, antijurídico y culpable se tratase de un caso de Hacking, o de Ransomware, ambos delitos de enorme cuantificación económica que tienen una amplia frecuencia de comisión la actualidad[25] (y teniendo a la vista que a la época en que la Ley 19.223 entro en vigencia no existía el Ransomware resulta interesante que pudiese darse la aplicación de esta ley para

b. Sujeto Activo.

El sujeto activo para el Artículo 1 es denominado con la expresión *"El que"* lo cual denomina que cualquier persona puede convertirse en autor de la conducta señalada por aquél tipo, denominación que convierte al artículo primero de la Ley 19.223 en un *Delito*

[25] Steve Morgan, Editor-in-Chief Cybersecurity Ventures. (2019). 2019 Official Annual Cybercrime Report. September 3rd, 2019, de HERJAVEC Group Sitio web: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

*Común* [26]. Puede también darse la hipótesis de que participe en la comisión del ilícito más de un autor, o autores en distintos grados y con distintas clases intervenciones en la comisión del ilícito, al final pudiendo configurarse cualquier hipótesis de coautoría. Es un tipo que describe a un sujeto activo amplio, haciendo la subsunción del hecho en el tipo más fácil, aplicable a cualquier persona o grupo de personas.

### 1. Tipicidad Subjetiva

En el artículo primero nos encontramos con que la redacción utiliza el adjetivo "maliciosamente". Este, nos reconduce inmediatamente a la existencia de un requisito de voluntariedad específico. Es menester que para que se configure el tipo, exista una intención de causar el daño descrito no sólo consciente, sino que positiva. Por lo tanto, además del elemente cognitivo, tenemos el componente volitivo del tipo, pero en el caso de este último es menester que la destrucción o inutilización de un sistema informático, o de sus componentes, o de la información en él contenida, hayan sido la finalidad última del ciber delincuente, por lo que nos encontramos ante un tipo subjetivo que exige para el juicio de tipicidad, la concurrencia de dolo directo, con la enorme carga probatoria que eso implica, y

[26] *Según el profesor Raúl Guillermo López Cabello "Sujeto activo es el autor de la conducta típica. Por lo general, se alude a dicho sujeto con las expresiones "el que" o "quien". En estos casos, sujeto activo del delito puede ser cualquiera, dando lugar a lo que denomina "Delitos Comunes".* López Camelo, R. Darío Jaque, G. (2004). Manual de Derecho Penal Parte General. Bahía Blanca, Argentina: Editorial de la Universidad Nacional del Sur.

descartando por ende, cualquier caso en que nos encontrásemos con un delito meramente culposo que cumpliera con la tipicidad objetiva del tipo.

Artículo 2°

*"El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio."*

Tipicidad Objetiva

a. Conducta Punible

El Artículo 2° de la Ley 19.223 tiene una formulación absolutamente distinta a la del Art. 1°. La descripción fenomenológica del tipo, alude a lo que se conoce genéricamente como hacking, que consiste en acceder a un sistema informático utilizando cualquier técnica informática. Es un tipo abierto en lo relativo a la conducta punible, puesto que la conducta

manifestada para la configuración del tipo puede prácticamente ser cualquiera, siempre y cuando el fin que se consiga, sea la manipulación de información digital de propiedad ajena.

La descripción de la conducta en este tipo es muy vaga, puesto que no enumera posibles métodos, ni tampoco entrega directrices en las que basarse para determinar que se está ante una intromisión indebida, sólo se limita a enumerar que para que se configure el tipo, es menester que el sujeto activo "intercepte, interfiera, o acceda" a un sistema informático. Cualquier conducta que pueda entenderse como tal, es suficiente razón de pedir para entablar acciones legales contra el autor del hecho dañoso.

b. Sujeto Activo

Al igual que en el Artículo 1°, el legislador utiliza una redacción bastante genérica que deja abierta la posibilidad a cualquier individuo con capacidad penal para perpetrar y ser responsable de este delito. No existe en la formulación de este tipo penal un sujeto activo determinado o específico, sino que nos encontramos ante "El que", es decir, ante cualquiera que realice la conducta descrita. El legislador nos pone enfrente nuevamente de un *Delito Común*[27] en que el puede darse cualquier hipótesis de autoría.

Tipicidad Subjetiva

[27] Ibíd.

En este respecto, el artículo 2 de la Ley 19.223, utiliza una formulación bastante parecida al primero, el Art. 2°, referido a grandes rasgos a todo tipo de hackeo, utiliza la expresión “El que con el ánimo de apoderarse, usar o conocer indebidamente”[28], la cual detona que para la configuración del tipo es menester la concurrencia del dolo de primer grado, también llamado dolo directo. Este artículo se diferencia del primero justamente en que si bien el primero también exige la concurrencia de un dolo directo, en la formulación del Artículo 2° el elemento volitivo es muchísimo más específico. En el Art. 2° es menester para el sujeto víctima probar que el sujeto activo actuó con un ánimo cierto de apoderarse, de usar o de conocer información a la cual no tiene acceso ni autorización para acceder, es decir, que lo haga “indebidamente” Y esto hace muchísimo más difícil su utilización. En el fondo, la formulación de este artículo dificulta la aplicación real en sede judicial del art. 2° toda vez que exige probar que el ciber criminal haya actuado tendiendo a una finalidad específica además de directa, que por otro lado deja fuera toda conducta reprochable en que el ciber delincuente acceda indebidamente a un sistema informático, y obtenga la información en él contenida, pero sin apoderarse de ella, usarla, o siquiera conocerla. Como por ejemplo lo han hecho muchos hackers históricamente, sólo por deporte.

Por otro lado, también resulta muy vaga la redacción del tipo, en cuanto en un solo delito podrían darse las 3 hipótesis planteadas, es decir, que el ciber delincuente se apodere, conozca, y además utilice la información obtenida, tanto, como podría darse una situación en que algún sujeto acceda a un sistema, pero no se apropie, use

[28] El subrayado es propio.

ni interiorice de la información en él contenida, sino que la venda, o la filtre a la web, pero sin jamás saber su contenido.

Tenemos por lo tanto que la descripción fenomenológica del tipo, estrictamente hablando, deja fuera conductas lesivas de comisión extremadamente frecuente en la actualidad, como lo son el data leaking, y el data mining.

Artículo 3°

*"El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio."*

## Tipicidad Objetiva

a. Conducta Punible

El elemento fenomenológico que tiene que ocurrir para que se configure el tipo del artículo tercero, corresponde a la alteración, daño o destrucción de los datos contenidos en un sistema de información. Vemos que el bien jurídico protegido es nuevamente acotado a la información que almacena un sistema informático, pero en este caso, lo que el tipo busca proteger es la integridad y por así decirlo "la vida" de los datos almacenados en un sistema,

a diferencia del artículo 2° que castiga la intromisión y la obtención de conocimiento sobre esos datos cuando no se tiene la autorización para acceder a ellos, sin importar su devenir. En el caso del artículo que analizamos en el presente párrafo, es irrelevante si es que los archivos y la información que resulte dañada, alterada o destruida producto de la intromisión, fueron leídos o llegados a conocer por cualquier medio posible.

Lo que el artículo 3° castiga es simplemente cualquier conducta que desemboque en un resultado que altere, dañe o modifique, sin tomar en consideración si al hacerlo, el sujeto activo entró en conocimiento sobre el contenido de la información afectada.

Tenemos entonces que este artículo sólo se refiere a las lesiones que el sujeto activo pudiese eventualmente provocarle a la información contenida en un sistema informático; es este artículo, si se le compara, exactamente igual al primero, con la diferencia de que cambia el bien jurídico protegido. En el primero, es el sistema informático en cuanto tal, en cambio en este, corresponde a la información en el almacenada. Al igual que con los dos anteriores, es menester hacer presente que este artículo impide combatir las nuevas formas de ciber delincuencia que comercian con la información, sin causarle ningún tipo de daño per se, sino que simplemente se valen de ella para revelarla, siendo incapaz también el artículo tercero, de hacer frente a las formas más frecuentes que toma la ciber criminalidad.

b. Sujeto Activo

El sujeto activo es, al igual que en los dos primeros artículos “El que”. Lo cual como ya hemos dicho, convierte al tipo en un *delito común* y para el cual puede darse cualquier

hipótesis de autoría. Basta con que quien cometa una acción que pueda subsumirse dentro de las hipótesis tenga capacidad penal para que se constituya como autor del delito tipificado.

## Tipicidad Subjetiva

Este artículo utiliza la misma formulación que el artículo primero: *"El que maliciosamente";* por lo que nos encontramos ante un requisito de voluntariedad directa. Es menester que para que se dé el supuesto del tipo, el autor del daño haya tenido justamente ese resultado como meta final de sus acciones. Por lo tanto, el elemento volitivo requiere además de conciencia, una voluntad positiva de parte del autor del daño hacia la obtención del resultado descrito en el tipo, o sea, el sujeto activo debe tener la intención cierta de alterar, dañar o destruir los datos contenidos en un sistema informático para poder subsumir su accionar en el tipo. Por lo tanto, a la hora de realizar el juicio de tipicidad nos encontramos ante la existencia de un requisito de dolo directo.

Artículo 4°

*"El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."*

## Tipicidad Objetiva

a. Conducta Punible

En este, el último artículo de la Ley 19.223, el elemento fenomenológico del tipo que tiene que darse, corresponde a la revelación o difusión de los datos contenidos en un sistema de información.

Se da entonces que la conducta castigada es lisa y llanamente la revelación o difusión de la información almacenada en un sistema informático. Sin importar el tipo de información del que se trate o los medios por los que se llevó a cabo su obtención, así como tampoco la finalidad que el ciber delincuente tuvo en mente al momento de la comisión del delito. Es una formulación abierta que abarca cualquier manera en la que pueda conseguirse el hecho descrito en el tipo.

b. Sujeto Activo

La primera parte de la formulación del artículo 4° es abierta, pues utiliza la expresión “El que” al igual que todos los otros artículos de la Ley 19.223, todos ya precedentemente analizados. Esto nos da cuenta de que cualquier persona con capacidad penal puede convertirse en el autor de la conducta definida en el tipo penal en cuestión. No importa si es que el sujeto que realiza la revelación o difusión de la información contenida en el sistema informático tiene acceso o no a ellos. Nos encontramos, entonces, al igual que en los artículos anteriores, ante un delito común.

Ahora, si el sujeto activo no sólo tiene acceso, sino que es quien tiene a cargo el sistema, es decir, es “el responsable” de este, la pena se aumenta en un grado, lo cual denota una doble modalidad en el mismo tipo, la cual depende de la eventual posición de garante que el sujeto activo podría tener para con el sistema que almacenaba los datos difundidos.

Por lo tanto, el artículo 3° cubre la hipótesis de delito común, toda vez que cualquier sujeto con capacidad penal puede configurarse como el culpable de la ejecución de la conducta descrita, mas también se hace cargo de aquella situación en la que es la persona directamente responsable, quien tiene a cargo aquel sistema, pasando en este caso el sujeto activo a sufrir una pena mucho mayor.

Entonces tenemos que el Artículo 4° de hecho se refiere a dos hipótesis de autoría distintas, una abierta, en la que se trata de un delito común, y otra específica, en la que nos encontramos ante un delito especial, debido a que la formulación del tipo prevé que este sea un *sujeto cualificado,* es decir, que reúna ciertas condiciones específicas (en este caso de

corte jurídico), pues es menester que para que se adecúe al juicio de tipicidad, el autor de la revelación o difusión de la información tenga que estar vinculado con el sistema al punto de ser “el responsable” de este, es decir la persona que lo tiene a cargo. Nos encontramos frente a una ampliación del deber de cuidado que debe tener en su calidad de garante, quien sea directamente responsable de aquella información.[29]

## Tipicidad Subjetiva

Al igual que en los artículos 1° y 3°, el artículo 4° utiliza la expresión “maliciosamente” para referirse al elemento volitivo del tipo, lo cual denota que el autor del hecho dañoso debe tener la voluntariedad directa de conseguir dicho resultado. Como ya ha sido manifestado, esto constituye un requisito que transforma al tipo penal contenido en el artículo 4° en un delito común que requiere de dolo directo para su adecuación al juicio de tipicidad. Es decir, además de plena conciencia de las consecuencias que dicho accionar podría acarrear, el resultado tiene que ser la meta del autor del daño cuando este realiza la conducta determinada en el tipo, en este caso: la revelación o difusión indebida de la información almacenada.

[29] Márques Cárdenas, A. González Payarés, O. (enero-junio 2008). La Coautoría: Delitos Comunes y Especiales. Revista de Diálogos y Saberes, ISSN0124-0021, 29 - 50.

## 1.2. Análisis común de los cuatro tipos penales.

Bien Jurídico protegido de los cuatro tipos penales de la Ley 19.223

El bien jurídico protegido de los 4 tipos penales de la Ley 19.223 corresponde a grandes rasgos a los sistemas informáticos y a la información en ellos contenidos. Esto es tremendamente importante, puesto que significa que nuestra legislación sectorial es específica al respecto, y por lo tanto no incluye delitos que sean atentatorios contra otros bienes jurídicos aun cuando impliquen necesariamente la utilización de un medio informático para su comisión, (los cuales son conocidos como *"Delitos Computacionales")*[30] como por ejemplo lo serían el delito de pornografía infantil, o el delito de estafa informática*, lo cual deja fuera del alcance de protección a un número importante de conductas delictuales que no pueden subsumirse en estos tipos. Según la historia fidedigna de la Ley, el diputado Viera-Gallo Viera Gallo señaló expresamente que esta nueva normativa debía proteger el nuevo bien que surge con el uso de las nuevas tecnologías computacionales, así como la información en ellos contenida en cuanto tal y en ningún caso enfocarse en penar el fenómeno delictivo cometido a través de medios informáticos; la comisión de la cámara baja que aprobó el proyecto de Ley estableció que se entiende que "*el delito informático es, en sí mismo, una acción ilícita reprochable, y que no se trata de un mero instrumento para*

[30] Moscoso Escobar, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. Revista chilena de Derecho y Tecnología, Vol. 3 N.1, 11-78.

*cometer otros delitos, sino de la protección que el sistema jurídico penal chileno hace de los sistemas automatizados de tratamiento de información."*[31]

Es menester tomar en consideración también, que *"Durante la tramitación, se tomó en consideración el concepto amplio de delito informático como un símil al concepto de «cibercrimen» norteamericano (el cual corresponde a una acción típica, antijurídica y culpable, para cuya consumación se utiliza o afecta una computadora o sus accesorios)"*[32]. Pero del análisis de la historia de la Ley, tanto como de la norma misma, nos encontramos con que el legislador tomó este concepto, pero lo restringió y utilizó inadecuadamente, de manera que el bien jurídico que el legislador quiso proteger mediante esta ley, corresponde a los sistemas informático computacionales per se, no a su utilización en cuanto plataforma de comisión de un delito, sino a cualquier conducta que revista cualquier tipo de lesividad a ellos y a la información en ellos contenida, en cuanto entidades complejas indispensables para el desarrollo de la sociedad.

Tenemos por lo tanto, que la Ley 19.223 sólo cubre un tipo de delito muy específico en la legislación contra el cibercrimen, que como ya sabemos, corresponde a un área de la criminalidad muy amplia, y en constante masificación, el cual corresponde a los sistemas informáticos en cuanto tales y a la información en ellos contenida; y que en ningún caso otorga protección a otros bienes jurídicos que revistan importancia para nuestro

---

[31] Bliblioteca del Congreso Nacional. (1992). Historia de la Ley 19.223. Jueves 5 de Septiembre de 2019, de BCN Sitio web: https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/7025/

[32] Lara, JC. Martínez, M. Violler, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. Revista chilena de Derecho y Tecnología, Vol. 3, NRO. 1, 101-137.

ordenamiento jurídico, como por ejemplo lo son, a muy grandes rasgos, la vida humana o la propiedad (estos delitos, que atentan contra otros bienes jurídicos, pero cuya comisión se lleva a cabo en el ciber mundo, se conocen como *Delitos Informáticos*[33] y se penan según normativas distintas a la Ley 19.223).

## Sujeto Activo

Del análisis precedentemente hecho, tenemos que los cuatro artículos que componen la Ley 19.223 corresponden a delitos comunes, es decir, a aquellos delitos cuya comisión puede ser llevada a cabo por cualquier persona que cuente con los medios necesarios para su comisión. A saber, que tenga acceso a internet y que sea poseedor de los conocimientos necesarios para involucrarse en este tipo de refinada criminalidad.

## Tipicidad

En cuanto a la tipicidad objetiva, cada artículo busca resguardar distintas formas de atacar los bienes jurídicos protegidos por la ley, que como ya se ha explicado, corresponden a los sistemas informáticos, y a la información en ellos contenida; La tipicidad subjetiva conseguida con la manera en que los tipos penales fueron formulados, apunta sin embargo, en una dirección contraria.

Los artículos primero, segundo y cuarto, utilizan la palabra “maliciosamente”; y el tercero utiliza la formulación “indebidamente”, por lo cual es posible vislumbrar que el

[33] Ibíd.

legislador de la época prefirió no hacer de los delitos informáticos, delitos culposos, sino, que prefirió transformarlos en delitos que requieren de un dolo directo y especial en su comisión para ser considerados como tales por un tribunal penal. Esto, fue materia de debate en sala durante la discusión previa a la aprobación del proyecto; ya decía el diputado Bosselin, en una de aquellas oportunidades, que *"todos sabemos que al exigirse un dolo específico o una especial malicia, no regirá la presunción del artículo primero del Código Penal, sino que será necesario acreditar en el propio juicio la concurrencia de esa especial perversidad."*[34] Muy probablemente, este legislador tenía razón en su punto, tomando en consideración la muy escaza aplicación procesal que la Ley 19.223 ha tenido en sus ya más de veinticinco años de vigencia. Al respecto, el Convenio de Budapest sobre la ciber delincuencia (2001), que corresponde a un esfuerzo internacional por combatir el ciber crimen, propone un catálogo de tipos penales culposos. Sabido es que probar un elemento volitivo así de específico, como lo son los contenidos en la Ley 19.223, es en extremo difícil.

[34] Ibíd.

# III. Tercera Parte: Análisis y descripción fenomenológica de las formas actuales de la criminalidad informática más frecuentes.

Acabamos de analizar en detalle la ley 19.223, distinguiendo los elementos del tipo para cada uno de sus 4 artículos. Es menester recordar que la Ley 19.223 es la única ley vigente en Chile en lo relativo al cibercrimen, así como es menester recordar que data de 1993, hace ya más de 26 años.

Según el aclamado profesor de física Leonard Susskind, un año tecnológico equivale a siete años "normales"[35]. Es necesario tener un ratio como ese en cuenta al analizar fenomenológicamente las actuales formas de comisión de criminalidad informática.

En este capítulo, nos avocaremos a analizar las formas de comisión de la criminalidad informática que han ido aumentando su frecuencia en la actualidad, como lo son el atemporal pero no menos considerable Hacking, el Phising y el muy en boga Ransomware.

## 3.1. Hacking

El hacking comenzó casi tan pronto como comenzó la masificación de la interconexión de redes en el Estado de Massachussets, específicamente en las dependencias del

[35] Sebastian Edwards. (2016). Ya pronto tu empleo desaparecerá. 17 de Abril de 2016, de La Tercera Sitio web: http://voces.latercera.com/2016/04/17/sebastian-edwards/ya-pronto-tu-empleo-desaparecera/

Massachussets Institute of Technology. Inicialmente sólo denotaba aquellas conductas ejecutadas por estudiantes que arreglasen o simplificasen alguna función de los ordenadores. En las primeras décadas desde el nacimiento de la internet, el hacking ni siquiera era visto como una conducta potencialmente peligrosa ni mucho menos negativa; Fue durante la década de los 80 en que algunos hackers comenzaron a incurrir en prácticas de dudosa legalidad, lo que llevó a los Estados Unidos a emitir su primera ley de protección a los sistemas informáticos, que como ya sabemos, data de 1985.

Según el diccionario *Merriam Webster*, una de las definiciones para el término hacker corresponde a "*a person who illegally gains access to, and sometimes tampers with information in a computer system*"[36]

Entonces, el hacking consiste en la intromisión en un sistema informático ajeno, de manera remota e ilegal desde otro sistema informático, con la finalidad de alterar, conocer o hacerse de la información en él contenida.

Puede ser ejecutado por cualquier persona que tenga los conocimientos técnicos necesarios y acceso un ordenador.

Hoy en día el hacking está absolutamente masificado y se utiliza para todo tipo de delitos que involucren el acceso no autorizado a sistemas computacionales y a datos almacenados en un sistema de almacenamiento ajeno, como lo serían los centros de Big Data.

---

[36] Merriam Webster. (2016). Definition of: Hacker. 16 de enero, 2016, de Merriam Webster Sitio web: https://www.merriam-webster.com/dictionary/hacker

Los propósitos de los hackers son increíblemente disímiles y variados. Pueden ir desde el robo de contraseñas bancarias hasta el hacktivismo (practica en que muchos hackers se ponen de acuerdo para atacar páginas con contenidos con los que desacuerdan, en una especie de ciber-autotutela).

El hacking fue la actividad que levantó la alerta roja gubernamental en el mundo, primeramente en Estados Unidos. Fue la primera actividad tratada como ilegal y en base a ella fue que surgió la legislación relativa al cibercrimen. Desde el comienzo del cibercrimen, hasta el día de hoy, el hacking ha sido el principal medio de comisión de delitos informáticos.

Según estadísticas de la PDI, un 89.99% de las denuncias recibidas por delitos informáticos en los últimos cinco años, corresponden a conductas que se pueden entender como hacking, a saber, el espionaje y el sabotaje informático[37]. Tomando en consideración que el total de denuncias corresponde a un total de 4.685, tenemos que alrededor de 4.216 de las denuncias hechas se podrían considerar como conductas de hacking, y que si se realiza una búsqueda de jurisprudencia que contega “Ley 19.223” entre sus caracteres en el buscador Vlex tan sólo aparecen 144 fallos…por lo tanto, se puede inferir que la Ley 19.223, en sus artículos primero y segundo, ha sido escasamente utilizada por la judicatura para penalizar las conductas relativas al hacking en nuestro país.

[37] Jefatura Nacional de Asuntos Públicos de la PDI. (2019). Radiografía a denuncias por Delitos Informáticos. 5 de Septiembre de 2019, de PDI Sitio web: http://www.pdichile.cl/centro-de-prensa/detalle-prensa/2019/07/10/panorama-de-las-denuncias-en-cibercrimen

## 3.2. Phishing

*"A form of social engineering in which an attacker, also known as phisher, attempts to fraudulently retrieve legitimate user's confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion. Such communications are most frequently done through emails that direct users to fraudulent websites that in turn collect the credentials in question. Examples of credentials frequently of interest to phishers are passwords credit card numbers, and national identification numbers.*

*The word "Phishing" is an evolution of the word "fishing" by hackers who frequently replace the letter "f" with the letters "ph" in a typed hacker dialect. The word arises from the fact that users, or phish, are lured by mimicked communication to a trap or hook that retrieves their confidential information."*[38]

Sus inicios se remontan al año 2003[39], año en que los ciber delincuentes, en específico, los hackers, idearon esta forma de criminalidad. Todo comenzó con la creación de cientos de cuentas de correo electrónico que contenían en la dirección el nombre de alguna compañía reconocida y con amplio respaldo. *"E-mail fraudsters register dozens of lookalike domain names, such as yahoo-billing.com and ebay-fulfillment.com. They also create Web sites that contain the names of well-known companies and brands like microsoft.checkinfo.com."*[40] De

[38] Jacobsson, M. Myers, S. (2007). Phishing and Countermeasures. Indiana: John Wiley & Sons, Inc.

[39] Unidentified. (2004). A Brief History of Phishing. 16 de Enero de 2017, de The Washington Post Sitio web: http://www.washingtonpost.com/wp-dyn/articles/A59350-2004Nov18.html.

[40] Ibíd.

esta manera, los ciber delincuentes comenzaron enviar olas masivas de spam[41] con links a páginas web fraudulentas que requerían de identificación, permitiéndoles robar los datos que las víctimas utilizaban para poder acceder. Otra manera más simple, que de hecho fue la utilizada en el hack informático más grande de la historia[42] corresponde a aquél método en que el ciber delincuente envía un email que contiene datos o un enlace que re direcciona a otros datos, los cuales no son sino un virus que se apropia de información vital, tal como cuentas bancarias, datos de identidad en la red, registros de transacciones, y en general, toda aquella información que sirva para suplantar la identidad de la víctima. Es justamente, de esto de lo que se trata, de apoderarse de manera encubierta, anónima y fraudulenta, de información relacionada a la identidad de la víctima, específicamente de lo que conocemos como *Datos Personales*, para a través de ellos poder suplantarla en su vida virtual, en todos los ámbitos en que sea posible, pero especialmente en aquellos en los que es posible usufructuar, como lo son las cuentas bancarias, y así perpetrar una criminalidad *tradicional.*

En nuestro país, según el último reporte entregado por la brigada de Ciber Crimen de la PDI, las denuncias por Phishing corresponden a un 3.61% del total realizado en los últimos cinco años[43], a pesar de que nuestro país es el tercer país más vulnerable al Phishing de

[41] Correo basura o no deseado, potencialmente peligroso, y que no pasa los filtros predeterminados de la compañía proveedora de emailing.

[42] Pagliery, J. (2015). The inside story of the biggest hack in history. 16 de Enero de 2016, de CNN Tech Sitio web: http://money.cnn.com/2015/08/05/technology/aramco-hack/.

[43] Jefatura Nacional de Asuntos Públicos de la PDI. (2019). Radiografía a denuncias por Delitos Informáticos. 5 de Septiembre de 2019, de PDI Sitio web: http://www.pdichile.cl/centro-de-prensa/detalle-prensa/2019/07/10/panorama-de-las-denuncias-en-cibercrimen

todo Latinoamérica[44], pero ya se ha vuelto algo tan cotidiano que los usuarios de correo electrónico se han ido educando para evitar caer en este tipo de estafa informática, tanto es así que probablemente, los únicos en realizar las denuncias, son un porcentaje de aquellos que lamentablemente sí terminan por convertirse en víctimas de estas estafas cibernéticas.

Como es posible ver, del análisis realizado en la segunda parte de este trabajo de investigación, se vislumbra que los artículos segundo y cuarto de la Ley 19.223 podrían dar lugar a un silogismo judicial que permitiese castigar esta conducta, ya que como sabemos, el Phishing, a través de maniobras fraudulentas, consigue la obtención de información personal de los usuarios de un sistema informático, conducta castigada en el inciso según de la citada norma legal, a la vez que el artículo cuarto permitiría penalizar al ciber delincuente que difunda maliciosamente la información que a través del Phishing obtenga.

### 3.3. Ransomware

El Ransomware nació en la década de los 90, pero no fue sino alrededor del 2005 que volvió a posicionarse como un delito informático frecuentemente utilizado, y *"As of 2016, it is considered one of the most prevalent forms of attack against computer systems requiring limited exposures to vulnerabilities and minimal reconnaissance on targeting"*[45]

---

[44] Lorena Wastavino, comunicaciones DSTI. (2019). Chile es el tercer país más vulnerable al phishing en Latinoamérica. 5 de Septiembre de 2019, de Universidad de Chile Sitio web: http://www.uchile.cl/noticias/155187/chile-es-el-tercer-pais-mas-vulnerable-al-phishing-en-latinoamerica

[45] Liskan, A y Timothy, G. (2017). Ransomware, -defending Against Digital Extortion. California, United States: O'Rilley.

La palabra Ransomware proviene del inglés *ransom*, que a grandes rasgos significa "pago de un rescate"[46] y de la terminación de la palabra *Software*. El Ransomware consiste en la utilización de programas de encriptación de archivos que son introducidos maliciosamente por virus y que le impiden al dueño del ordenador infectado acceder a ellos. Existen dos variantes de ellos, aquellos malware que encriptan archivos o carpetas unitarias y aquellos que simplemente bloquean el acceso total al computador si es que no se paga un rescate previo. Para esto, los ciberdelicuentes actúan de manera parecida al Phishing, comúnmente, enviando un link que de ser abierto, pone en operación el malware que "secuestra la información".

Para realizar su cometido, utilizan distintos portales de pago muy parecidos a paypal, e incluso emplean contadores regresivos de tiempo, que indican un aumento en el valor de rescate por cada intervalo de tiempo que pasa sin que se pague el rescate pedido. Una vez que la víctima del delito realiza el pago, el acceso a su información u ordenador le es devuelto.

Tan efectivo en su cometido es este delito, que una de sus variantes más conocidas, el programa (malware) CryptoWall (ya dado de baja) logró reunir 18 millones de dólares durante el 2015 (y sólo tomando en consideración el periodo comprendido hasta junio de ese año).[47]

Durante las últimas décadas, la escalada en los ataques de Ransomware se tomó las portadas de los medios del mundo, una gigantesca ola de ciber ataques de esta naturaleza

[46] Traducción libre.

[47] Ibíd.

se llevaron a cabo de manera masiva durante el año 2016, 2017 y el pasado 2018, volviéndolo una pesadilla tanto para sujetos particulares, como para grandes compañías, y hasta para los distintos servicios gubernamentales de los Estados del mundo, que vieron como su funcionamiento dependió del pago de un rescate al hacker u organización de estos, que estuviesen lanzando el ciber ataque, y por lo tanto, que intentaban hacerse con el dinero del rescate. Cabe destacar, que durante el año 2018, si bien la cantidad de ataques de Ransomware aumentó, el monto solicitado para el rescate de los sistema disminuyó a la mitad de lo que venía siendo en años anteriores, quedando en promedio en la suma de $522 USD[48]. Esto tiene que ver con las medidas de seguridad que los particulares han comenzado a tomar, y que han logrado una disminución en la efectividad de estos ataques, lo cual hace vislumbrar que no sólo en Chile, sino que en el mundo, la legislación penal no es lo suficientemente efectiva para combatirlos, por lo que los particulares tienen que desembolsar grandes partes de sus partidas presupuestarias en contratar servicios de ciber seguridad privada.

El sector de la ciber seguridad se ha convertido en una especie de autodefensa privada imprescindible ante la incapacidad de los ordenamientos jurídico penales del mundo de proteger efectivamente los bienes jurídicos protegidos que ha creado la sociedad de la información.

---

[48] Symantec. (2019). R Internet Security Threat Report. 6 de Septiembre de 2019, de Symantec Corporation Sitio web: https://resource.elq.symantec.com/LP=6819?inid=symc_threat-report_istr_to_leadgen_form_LP-6819_ISTR-2019-report-main&cid=70138000001Qv0PAAS.

# IV. Cuarta Parte: Lagunas de Punibilidad de la legislación actual.

4.1. Lagunas de punibilidad detectadas en el análisis realizado en el presente trabajo de investigación jurídica, a la luz de los fenómenos descritos en la parte III.

¿Aplica algún tipo de la legislación penal chilena para el Hacking?

En efecto, el artículo 2° de la Ley 19.223 se hizo pensando específicamente en el delito del hacking[49] que era la manera de cibercrimen más emblemática y, por cierto, la mayor frecuencia de comisión a esa fecha.

Según lo que analizamos en el capítulo anterior, y a la luz de la historia de la Ley, el artículo primero de la Ley 19.223, tanto como el segundo, fueron formulados teniendo en mente la creación de un tipo que penara tanto la interferencia como el sabotaje informático, ambas conductas que genéricamente hablando, se entienden como hacking; Ya lo decía el legislador en la discusión del proyecto *"En el artículo 1° se sanciona la inutilización del sistema en sí mismo; en el 2°, la interferencia, lo que de alguna manera representa el espionaje en los sistema de computación;*

Pero ya conociendo el concepto de hacking, se puede vislumbrar que las acciones que este comprende, así como también sus resultados, son también subsumibles en el artículo 1° y el artículo 3°. *«El delito de hacking, por constituir fundamentalmente un acceso*

[49] Según la historia fidedigna de la Ley, citada anteriormente en este trabajo.

*indebido o no autorizado, induce a la creencia, no errada por cierto, de que este ilícito se presentará como medio o herramienta de comisión de otros delitos informáticos ya tratados, y que, por lo tanto, su característica podría ser la de configurarse como un hecho delictivo necesario para la comisión de otros»*[50].

El artículo 2**°** castiga el hacking propiamente tal, al tratar sobre un *acceso indebido* en un sistema informático, cuando este además se realiza con el ánimo de apoderarse, usar o conocer la información contenida en él, pero un hacking puede perfectamente conllevar como resultado otras manifestaciones negativas, como lo sería el tipo objetivo descrito en el artículo 1**°** cuyo sujeto activo es aquel que *"destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento"* o también el artículo 3**°**, cuyo sujeto activo viene siendo aquel que *"altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información".*

Lamentablemente, el artículo 2° excluye al hacking originario, al predecesor del que conocemos hoy: aquél que simplemente se hace por diversión, por la curiosidad que tiene el hacker de probar sus habilidades o de explorar las posibilidades que el ciberespacio le entrega. Bajo los requisitos de tipicidad subjetiva del tipo establecidos en el artículo 2°, no es posible penalizar un hacking *blanco* (aquél que sólo irrumpe, pero no lesiona el sistema informático, ni revela la información en él contenida) .

Tenemos por lo tanto, que la amplitud del concepto de hacking, permiten que sea subsumido nada más, ni nada menos, que en los tres primeros artículos de la Ley 19.223,

---

[50] Moscoso Escobar, R. (2014). La Ley 19.223 en general y el delito de *hacking* en particular. Revista chilena de Derecho y Tecnología, Vol. 3 NRO. 1, 11-78.

pero respecto del análisis del artículo segundo es posible ver que por su la tipicidad subjetiva que el legislador incluyó en el tipo, lamentablemente, ni el mencionado artículo segundo, ni ninguno de los otros tres de la citada Ley, permiten castigar el hacking en su práctica originaria.

Por lo tanto, la Ley 19.223 aplica para el delito de hacking, más lo hace de manera imprecisa, y no permite subsumir en ninguno de sus tipos, el hacking per sé, es decir, aquél que no lo utiliza como medio para llegar a otro fin, sino que corresponde al fin en sí mismo del ciber delincuente.

¿Aplica algún tipo de la legislación penal chilena para el Phising?

Lamentablemente, la Ley 19.223 no contiene ningún tipo penal que sea aplicable a cases de Phishing. El tipo penal más cercano bajo el cual podría conocerse judicialmente un caso de esta índole, vendría siendo el tradicional delito de estafa. Pero debido al anacronismo al que nuestro código penal se ve enfrentado, sobre todo en lo que respecta a las tecnologías contemporáneas, *"Lamentablemente la figura de la estafa clásica tiene algunos problemas, vinculados principalmente al error, ya que se ha sostenido que solo las personas naturales pueden ser objeto de un error en los términos que este delito exige, y no una máquina o dispositivo"*[51]

[51] Christiansen Z, Axel. (2014). La arcaica ley informática chilena que mantiene en "tierra de nadie" diversos delitos. 14 de Enero de 2017, de La Tercera Sitio web: http://www.latercera.com/noticia/la-arcaica-ley-informatica-chilena-que-mantiene-en-tierra-de-nadie-diversos-delitos/

El tribunal supremo de España, en un fallo que dio por zanjado el asunto, estimó que a *"las máquinas no se les puede engañar y a los ordenadores tampoco, por lo que en los casos en los que el perjuicio se produce directamente por medio del sistema informático, con el que se realizan las operaciones de desplazamiento patrimonial, no se producen ni el engaño ni el error necesarios para el delito de estafa"*[52]

La legislación chilena tampoco se hace cargo de es interrogante. Por un lado, la legislación chilena referida al ciber crimen, se limita a la Ley 19.223, que como hemos ya viste latamente, protege el bien jurídico correspondiente al sistema informático y la información en él contenida. Indirectamente claro, protege al usuario de los sistemas informáticos víctimas de ciber ataques, ya que lo que resguarda corresponde a sistemas e información que son de su propiedad, y aquí es donde se vuelve interesante analizar las características del Phishing en cuanto a potencial tipo penal.

Es evidente que el Phishing ataca al usuario de un sistema informático, al buscar obtener maliciosamente información que le podría ser de provecho al ciber delincuente para la comisión de otro tipo de conducta reprochable, ya correspondiente al catálogo de los delitos tradicionales, ya correspondiente a un delito informático. Pero no importando la finalidad que el ciber delincuente haya tenido a la hora de cometer Phishing contra una víctima, este actúa en el ciber mundo. No sólo utiliza un sistema informático como medio de comisión, sino que la mayor parte del Íter Criminis se da en el ciber mundo. El ataque, el error del usuario, y los potenciales daños que podría sufrir la víctima también, por lo que no corresponde su categorización dentro del catálogo de los delitos tradicionales.

---

[52] Jaén Vallejo, M. Perrino Pérez, A. (2015). La Reforma Penal del 2015. Madrid: Editorial Dyckinson.

La víctima de Phishing es una persona natural, pero sufre el error sobre aquellos bienes de su propiedad que operan o se encuentran en el ciber mundo, que es también el mismo plano en que sufre los daños que le provoca dicha conducta lesiva.

Es así entonces, como es que hoy en día nos encontramos ante una gran laguna de punibilidad para poder combatir el Phishing, ya que ni la Ley 19.223 lo contempla, ni tampoco el catálogo de los delitos tradicionales. Y siendo que corresponde a la tercera forma más denunciada de ciber criminalidad a la Policía de Investigaciones de Chile en los últimos cinco años[53], se concluye que corresponde a una laguna de punibilidad que el legislador debe solucionar.

## ¿Aplica algún tipo de la legislación penal chilena para el Ransomware?

Si nuestra legislación penal relativa al cibercrimen no presupone ningún tipo penal que pudiese aplicarse al Phishing, que viene siendo una conducta masivamente cometida desde comienzos de la pasada década, no es para nada descabellado que la misma situación se repita con el Ransomware, que es mucho más sofisticado tecnológicamente

---

[53] Jefatura Nacional de Asuntos Públicos de la PDI. (2019). Radiografía a denuncias por Delitos Informáticos. 5 de Septiembre de 2019, de PDI Sitio web: http://www.pdichile.cl/centro-de-prensa/detalle-prensa/2019/07/10/panorama-de-las-denuncias-en-cibercrimen.

[53] Lorena Wastavino, comunicaciones DSTI. (2019). Chile es el tercer país más vulnerable al phishing en Latinoamérica. 7 de Septiembre de 2019, de Universidad de Chile Sitio web: http://www.uchile.cl/noticias/155187/chile-es-el-tercer-pais-mas-vulnerable-al-phishing-en-latinoamerica

hablando. El artículo 1 es lo más cercano que nuestra legislación provee al respecto, puesto que una de las hipótesis del Ransomware es justamente la intromisión ajena en un sistema informático a través de un virus (llamado *Malware*) que deja inutilizable, obstruido o impide[54] el funcionamiento del software hasta el pago del rescate.

El inciso segundo del citado artículo, dictamina que *"Si como consecuencia de estas conductas se afectaren los datos[55] contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo";* En el Ransomware, de no pagarse la suma monetaria (cuestión que se hace en criptomonedas y a través de servidores y centros de almacenamiento ubicados en jurisdicciones muy controversiales en cuanto a su adherencia al combate contra el ciber crimen, como lo es Rusia)[56] típicamente conlleva a la eliminación de la información almacenada en dicho sistema de información, a la pérdida total que el usuario víctima sufre de ella, por lo que el juez penal podría intentar realizar un silogismo que enmarcara el Ransomware en el artículo primero de la Ley 19.223.

Cómo el Ransomware es una suerte de "secuestro" digital de información, el juez podría realizar también un juicio de tipicidad en lo que respecta a esta parte del ilícito, mas dejando fuera toda la parte concerniente a secuestro, extorsión e incluso amenaza que el Ransomware implica, lisa y llanamente utilizando otro tipo penal en la búsqueda de dar sanción al delito, a saber utilizando un tipo que contemple la inducción a error que sufre la víctima, de parte del ciber delincuente, así como la sustracción de bienes de su propiedad,

---

[54] El subrayado es propio. Todos aquellos verbos son los rectores en la redacción del citado artículo primero; el subrayado es propio.

[55] El subrayado es propio.

[56] Rusia no forma parte de los Estados que adhieren al Convenio de Budapest sobre la Ciber Delincuencia.

que vendrían a ser la información secuestrada por el ciber delincuente a través del programa de malware.

Por su parte, el artículo 3 de la Ley 19.223 en su inciso primero, podría considerarse como un tipo penal que aplique para aquellos casos en que el ciber delincuente destruya o elimine los datos personales o información contenida en el sistema informático victima de Ransomware, pero de todas maneras tampoco es posible adecuarlo en un juicio de tipicidad pues el artículo carece de gran parte de los elementos del Ransomware, ya que sólo aplica para la etapa final de la comisión del delito, dejando fuera el error que sufre la víctima, el secuestro de la información, y la extorsión para que realice el pago; aplicando únicamente al resultado final de un caso de Ransomware en que la víctima no realice el pago solicitado por el ciber delincuente, y que finalmente conllevaría a la destrucción de la información y a la eventual aplicación del artículo tercero de la Ley 19.223 para conocer de un caso de esta naturaleza.

Por lo tanto, hoy en día es imposible sancionar penalmente el Ransomware como tal, toda vez que no existe ningún tipo penal en que pueda adecuarse en nuestra legislación. Nos encontramos, al igual que con el Phishing, pero de manera muchísimo más grave y evidente, ante una gran laguna de punibilidad.

4.2. Soluciones que el Derecho comparado ha encontrado para situaciones de lagunas de punibilidad como las recientemente descritas.

- Análisis de Derecho comparado con la legislación española relativa a la materia (especialmente al nuevo catálogo de delitos informáticos tipificados en la última reforma de su código penal).

Durante el año 2015, España aprobó una ley que modificó gran parte de su código penal; una de las grandes innovaciones que esta reforma trajo consigo, corresponde justamente al tratamiento dado a los delitos informáticos, y lo hace con especial énfasis en la criminalidad informática relativa a los delitos económicos, pues *"los delitos más frecuentes en el ámbito de la delincuencia informática tienen que ver con la criminalidad económica a través de la manipulación de datos con el objeto de influir en el resultado de su procesamiento"*[57].

La reforma española no sólo se hace cargo de la criminalidad informática en lo relativo a las formas de comisión símiles al delito de estafa, sino que al ser España un Estado que ha ratificado el Convenio de Budapest de la Unión Europea para la Ciberdelincuencia, en su última reforma al código penal, adopta íntegramente los postulados de esta, siendo los más nuevos del 12 de agosto de 2013. En esa directiva, el parlamente europeo se refiere directamente a los ataques organizados del cibercrimen, aludiendo que "*Los ataques contra los sistemas de información y, en particular, los ataques vinculados a la delincuencia organizada, son una amenaza creciente en la Unión y en el resto del mundo, y cada vez preocupa más la posibilidad de ataques terroristas o de naturaleza política contra*

[57] Ibíd.

*los sistemas de información que forman parte de las infraestructuras críticas de los Estados miembros y de la Unión. Esta situación pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia y exige, por tanto, una respuesta por parte de la Unión, así como una cooperación y coordinación reforzadas a escala internacional."*[58] A partir de este extracto, puede vislumbrarse la extensión de peligrosidad que el parlamento europeo estima que el ciber crimen posee.

España acogió este llamado ratificando el instrumento y reformando los tipos penales vigentes desde 1993. Lo hizo sin una ley sectorial, introduciendo nuevos tipos, y por lo tanto agregando nuevos bienes jurídicos protegidos al catálogo del Código Penal español. Esta ley suprimió algunos tipos anteriormente vigentes, e incluyó otros en los que el enfoque está en la intromisión malintencionada y con fines dañosos a *sistemas informáticos*, enfoque que los antiguos tipos penales españoles no poseían, y que por lo tanto le dejaba a los ciber delincuentes una peligrosa laguna punitiva sobre la cual poder operar. Es esta la principal directriz de la directiva de 12 de agosto de 2013 del parlamento europeo.

Así, la reforma al Código Penal español introdujo los artículos 197 bis, 197 ter, 197 quáter y 197 quinquies. Siendo el 197 un artículo original no sujeto a modificación que pena el espionaje. El artículo 197 bis está expresamente referido al espionaje informático a sistemas, es decir a "computadores interconectados" como los que existen en organizaciones sociales complejas, como empresas, reparticiones gubernamentales, etc.

---

[58] Diario Oficial de la Unión Europea. (12 de agosto de 2013). DIRECTIVA 2013/40/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO. 18 de enero de 2016, de Parlamento Europeo Sitio web: https://www.boe.es/doue/2013/218/L00008-00014.pdf.

Pero ya dando un vistazo rápido al artículo 197, deviene obvio que es un tipo mucho más completo y acabado de los de nuestra Ley 19.223, pues presupone variadas formas de comisión dentro de las cuales se incluye aquella que es llevada a cabo por medios informáticos sobre la manipulación indebida de datos personales. En Chile la legislación vigente sobre protección de datos personales es extremadamente ineficiente y nuestra legislación sobre delitos informáticos ni siquiera los menciona. A pesar de la importancia y trascendencia de la que esa materia goza.

Otra novedad de la reforma 1/2015 en esta materia viene a ser que tanto la producción como la adquisición de software hechos u optimizados para la comisión de delitos informáticos son a partir de ahora considerados como delitos que tienen su propio tipo penal (art. 197 ter). El artículo 197 quáter amplía las penas cuando la comisión se atribuye a un grupo organizado de carácter criminal, y finalmente, el artículo 197 quinquies trata sobre responsabilidad proveniente de esta forma de criminalidad cuando el autor es una persona jurídica.

Los tipos penales ya existentes que se mantuvieron fueron a su vez reforzados con la reforma del 2015 con una considerable elevación en sus penas. Esto ocurre con conductas conscientes de dañar, deteriorar, alterar, suprimir, o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos (Art. 264 Código penal español).

El legislador español intentó que la reforma *"permitiera ofrecer diferentes niveles de respuesta a la diferente gravedad de los hechos, los supuestos de daños informáticos y las interferencias en los sistemas de información."*[59]

[59] Ibíd.

En conclusión, no resulta curioso ni descabellado que el legislador español haya legislado tipos penales sobre el cibercrimen con tanto detalle, ni que los haya dotado de la misma relevancia que los delitos tradicionales, haciéndolos parte armónica del catálogo tradicional de tipos del Código Penal, toda vez que la vida en la actualidad es simplemente inconcebible sin los medios informáticos. No podemos desentendernos del hecho de estar viviendo en la sociedad de la información.

- Soluciones que han encontrado otras legislaciones de la tradición continental.

Italia por su parte también ratificó el Convenio de Budapest de Cibercrimen, por lo que realizó una reforma durante el año 2008 que adecúa su legislación interna a dicho convenio. Desde dicha modificación, ubica su legislación penal relativa al cibercrimen dentro del catálogo de delitos del código penal. Italia llevó a cabo una reforma como la española el año 2008, y reformó los tipos penales relativos al cibercrimen que habían entrado en rigor en virtud de una ley promulgada en 1993, además de agregar tipos nuevos relativos a la firma electrónica y de introducir (muy novedosamente, por cierto) en el Código Penal italiano nuevos tipos penales relativos a materias de *daño informático. "el legislador italiano ha distinguido, siguiendo las recomendaciones internacionales, entre daños a datos y daños a sistemas informáticos, y ha tipificado ambas conductas como delitos distintos. Sin embargo, en contra de lo que ha ocurrido en muchos países europeos (como, por ejemplo, en Alemania, Austria, España y Rumanía), nuestro legislador no se ha limitado a introducir en el*

*Código penal dos tipos delictivos autónomos en subjecta materia, sino que ha creado un complejo sistema normativo formado por cuatro normas distintas."*[60]

- Soluciones que han encontrado países del Common Law.

Estados Unidos ha sido el país que ha llevado la vanguardia en el combate contra la criminalidad informática. Fue el primero en legislar al respecto y es el que más mayores esfuerzos intenta en miras a renovar constantemente su legislación contra el cibercrimen, siendo la última el *Cybersecurity Act* de 2015 que busca promover la cooperación entre distintas entidades para combatir la criminalidad informática, específicamente lo que se refiere a compartir información sobre posibles amenazas. Estados unidos ha promulgado variadas leyes federales (conocidas como "Acts") que abarcan de manera bastante minuciosa las conductas relativas al ciber crimen, así como también las instituciones llamadas a combatirlo.

Esta manera de enfrentar el fenómeno de la criminalidad informática en Estados Unidos tiene muchísimo sentido y aplicación, ya que la normativa penal relativa al cibercrimen no sólo tiene calidad de ley federal, sino que, a mayor abundamiento, cada Estado tiene sus propias normas, que vienen a complementar el tratamiento al ciber crimen dado por la leyes federales.

---

[60] Salvadori, I. (enero-junio 2013). La regulación de los daños informáticos en el código penal italiano. IDP. Revista de Internet, Derecho y Política, NRO. 16, 44 - 60.

Cabe hacer un paralelo en este punto con nuestro país, y recordar la discusión parlamentaria dada en nuestro país en el año 1993, cuando la Ley 19.223 estaba en discusión; ocasión en la cual se estimó que lo mejor era seguir el modelo adoptado por Estados Unidos en 1985, que el modelo de países de la tradición continental, desconocemos si el legislador de la época tomó en consideración que en los Estados Unidos la normativa federal es complementada con la estatal.

El Reino Unido por su parte ha adoptado una estrategia global contra el cibercrimen ante la latente amenaza que representa para el comercio internacional y los mercados, pero lo ha hecho utilizando una formula bastante particular. Ha emitido una serie de *Acts* y regulaciones bastante específicas que dictaminan conductas y resguardos que las instituciones deben adoptar para protegerse a sí mismas, y también a la población, y en lo que respecta a la legislación en específico, acaba de aprobar la adopción de normativas de la unión europea que van a entrar en rigor el próximo año. Dentro de estas se encuentran *The Network and Information Security Directive (NIS Directive),* que es considerada como "*The cornerstone of the European Union cybersecurity legislative policy*"[61] y que consiste en un conjunto de obligaciones para los operadores de servicios básicos y para proveedores de servicios digitales. Otra regulación de corte europeo que debería entrar el rigor el próximo año es la *General Data Protection Regulation,* la cual establece obligaciones emanadas por

[61] Ward, C. (2016). The UK's Cybersecurity Regulatory Landscape: An Overview. 18 de Enero de 2016, de Hogan Lovells Law firm Sitio web: http://www.hldataprotection.com/2016/12/articles/international-eu-privacy/the-uks-cybersecurity-regulatory-landscape-an-overview/

normas de seguridad sobre los controladores y proveedores de servicios informáticos y los faculta a acceder incluso al campo de los datos personales.

Vemos entonces, que el Reino Unido, se enfoca en una protección de los bienes jurídicos informáticos ex ante, haciendo obligatorias determinadas medidas de protección tanto para particulares, como para las divisiones y organizaciones gubernamentales pertenecientes al mismo Estado.

# V. Parte: Proyecto de Ley que derogaría tácitamente la Ley 19.223

## 5.1. Generalidades del proyecto de Ley contenido en el mensaje Nº 164-366

El día Jueves 25 de Octubre del 2018, el ejecutivo envió un mensaje al congreso nacional, que contiene un proyecto de Ley que busca la derogación tácita de la Ley 19.233, y su reemplazo por nueva normativa penal que se adecúe a los estándares contenidos en el Convenio de Budapest del Cibercrimen. Dicho convenio proviene del Consejo Europeo y data del año 2004, pero nuestro congreso recién aprobó la incorporación de nuestro país a dicho instrumento el 17 de Noviembre del 2016, y lo ratificó el 20 de abril del 2017.

Este instrumento internacional es un esfuerzo colaborativo que ha permeado las fronteras europeas y que hoy ya sido ratificado por alrededor de 53 países del mundo[62],

62

incluidos los Estados Unidos. El principal objetivo del Convenio de Budapest, es la coordinación y cooperación internacional en el combate al cibercrimen; esto, en el marco en que este tipo de criminalidad carece de fronteras de comisión, y puede desarrollar su Íter Criminis en las más diversas partes del mundo.

Este proyecto de Ley presentado por el ejecutivo, es el tercer intento de modificación de la Ley 19.223 (luego de dos intentos infructuosos, uno del ejecutivo en el año 2002, y otro que corresponde a una moción parlamentaria del mismo año, también fallida), de adecuar nuestra legislación penal relativa al cibercrimen a los tiempos modernos, y así, de deshacerse del anacronismo legislativo que nuestro país mantiene en esta área.

Este proyecto de Ley, adopta las definiciones dadas por el Convenio de Budapest, y establece 17 artículos, 7 de los cuales corresponden a tipos penales, 10 que corresponden a alcances procesales y circunstancias modificatorias de la responsabilidad penal, más 3 artículos transitorios que re refieren a la entrada en vigencia de la Ley. El legislador, ejecutivo en este caso, se decanta una vez más por la técnica de la legislación penal especial, y prefiere no agregar nuevos tipos al catálogo de delitos tradicionales del derecho penal.

Se vislumbra que de aprobarse este proyecto de Ley, sería una herramienta bastante más efectiva para combatir el fenómeno de la criminalidad informática, el cual aumenta en proporciones descomunales, habiendo aumentando en la considerable cifra de un 74% entre el año 2016 y el año 2017[63].

[63] Presidencia de la República, Ministerio del Interior y Seguridad Pública, Ministerio de Justicia y Derechos Humanos. (2018). Mensaje Presidencial 164-366. 4 de Septiembre de 2016, de BCN Sitio web: https://www.camara.cl/pley/pley_detalle.aspx?prmID=12715&prmBoletin=12192-25.

Este proyecto de Ley introduce modificaciones que extienden al ámbito de aplicación de la ley penal relativa al cibercrimen latamente, haciendo posible la penalización de conductas modernas de cibercrimen que no se creían posibles cuando se discutió la Ley 19.223; Permite también una unificación de la legislación penal internacional que combate el cibercrimen, puesto que todos los Estados que lo ratifican tienen que adecuar su legislación penal interna para cumplir con las directrices del Convenio.

5.2. Particularidades del proyecto de Ley contenido en el mensaje Nº 164-366

El proyecto de Ley contenido en el mensaje 164-366 del año 2018, como ya se ha dicho, amplía latamente el catálogo de tipos penales de nuestro ordenamiento jurídico penal, relativos al cibercrimen; Lo cual es un avance sustancial en la materia.

De ser aprobado y promulgado, permitiría llenar las lagunas de punibilidad relativas al Phishing y al Ransomware, que como ya hemos podido observar, no son punibles con la legislación actual.

En su artículo primero, tipifica la *Perturbación Informática*, dentro de la cual podría subsumirse el Ransomware; En su artículo segundo, penaliza el *Acceso Ilícito* a un sistema informático, para lo cual aplicaría el Hacking en sus múltiples variantes de comisión. El artículo tercero pena la *Interceptación Ilícita*, lo cual atiende a los worms, antiguamente conocidos como virus troyanos; El artículo cuarto pena directamente la *Destrucción de un*

*sistema informático o los datos en él almacenados*, por lo que aplica para todas las conductas lesivas que terminen por tener ese resultado, siendo también factible utilizarlo para penar el Ransomware. En el artículo quinto nos encontramos con la *Falsificación Informática*, que tiene que ver con la alteración y modificación de datos que luego se hagan pasar por auténticos. El artículo sexto tipifica el *Fraude Informático*, que consiste en la utilización de los datos almacenados en un sistema informático, cuando esta busque obtener beneficios económicos ilícitos provenientes de dicha actividad. Finalmente, el artículo séptimo pena el Abuso Informático, que consiste en la utilización de Malware para la comisión de los ilícitos penados en los artículos cuatro y cinco del proyecto de Ley.

Como se ha podido vislumbrar el proyecto es bastante completo, y cumple además con la necesariedad de adecuar nuestra legislación penal al Convenio de Budapest, pero es necesario hacer notar, que al igual que la Ley 19.223, este proyecto de Ley exige un requisitos de voluntariedad específico de dolo directo en cada uno de sus tipos, utilizando reiteradamente las expresiones “maliciosamente”, “indebidamente” e “ilícitamente” lo cual, como ya analizamos con anterioridad en este trabajo de investigación, es de cuestionable utilidad práctica, e implica un trabajo probatorio mucho más difícil y específico que si tan sólo se tratase de un catálogo de delitos culposos.

No se advierte con claridad cuál es el motivo que el legislador ha tenido, una vez más, para transformar los tipos penales del cibercrimen en delitos dolosos en vez de culposos; si nos encontramos ante una conducta de Ransomware, o Phishing, evidentemente estas fueron cometidas dolosamente, pero procesalmente hablando, esto implica una dificultad más elevada en sede judicial.

Por otra parte, y al igual que la Ley 19.223, este proyecto, con su catálogo de delitos dolosos, hace imposible penalizar el Hacking originario (o Hacking Blanco), aquél que dio nacimiento a la criminalidad informática, pero que comenzó como una molesta intromisión en un sistema informático, que no tenía por objetivo causar ningún daño intencionalmente, y que sigue siendo el punto de partida de cualquier ciber delincuente en entrenamiento.

# VI. Parte: Conclusiones

La conclusión de este trabajo de investigación, es que la Ley 19.223 se aprecia superada por el fenómeno de la criminalidad informática en la actualidad, y que viene estándolo desde hace muchísimo tiempo. No es idónea para enfrentarlo debido al natural paso del tiempo y el avance exponencial que aquello conlleva para las técnicas de criminalidad informática; también, debido a lo escueta que es; pero muy especialmente, debido a las dificultades probatorias que conlleva el que sea un catálogo de delitos dolosos en vez de delitos culposos, mismo error en el cae el proyecto de Ley que busca su derogación tácita, presentado por el ejecutivo en el año 2018.

Se concluye que el legislador nacional debería decantarse por modificar el proyecto de ley que se encuentra actualmente en su primer trámite legislativo en el congreso, y eliminar los vocablos del tipo que exigen dolo para penar la criminalidad informática; tal y como lo han hecho las legislaciones de vanguardia en la materia, como lo son los Países Bajos y los Estados Unidos; de esto modo, nuestro país podría contar con una legislación penal realmente eficaz para combatir el cibercrimen

Chile, corriendo ya el año 2019, se enfrenta ante una enorme laguna punitiva en una materia que para todos los gobiernos del mundo desarrollado, es del más alto orden, y el nuevo proyecto de Ley lleva casi un año descansando en el congreso, esperando a que le den la atención de máxima urgencia que requiere.

El Ordenamiento Jurídico Penal chileno, en lo que respecta al cibercrimen, es del todo insuficiente para combatir el extenso y dañoso delito de la criminalidad informática.

# Bibliografía


- Claudio Paul Magliona Markovich, Macarena López Medel. (1999). Delincuencia y Fraude Informático. Santiago de Chile: Editorial Jurídica de Chile .

- Nicolás Oxman. (2º Semestre 2013). Estafas informáticas a través de Internet: Acerca de la imputación penal del “phishing” y el “pharming”. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, XLI, 211-262

- Susan W. Brenner. (2012). La Convención sobre Cibercrimen del Consejo de Europa. Revista chilena de Derecho y Tecnología, 1. NRO. 1, 221 - 238.
- Carlos María Romero Casabona en Fernando Pérez Álvarez. (2007). De los delitos informáticos al cibercrimen. Universidad de Salamanca: Aquilafuente.

- Dra. Josefina García García-Cervigón. (mayo-agosto 2008). El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales , Nº 74, 289-308.

- Ivan Salvadori. (enero-junio 2013). La regulación de los daños informáticos en el código penal italiano. IDP. Revista de Internet, Derecho y Política, Nº 16, 44 - 60.

- Faustino Gudín Rodríguez-Magariños. (2008). NUEVOS DELITOS INFORMÁTICOS: PHISING, PHARMING, HACKING Y CRACKING. 23 de agosto, 2016 , de Ilustre Colegio de Abogados de Madrid Sitio web: http://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf

- Christian Fuchs. (2008). Internet and Society: Social Theory in the Information Age. Austria: Routledge.

- Koops, Bert-Jaap. (25 Julio de 2010). Cybercrime Legislation in the Netherlands. Country report for the 18th International Congress on Comparative Law, Washington, DC, 25-31 July 2010, session 'Internet Crimes, 18th, 40. 9 de Diciembre de 2016, De SSRN Library Base de datos.

- Moscoso Escobar, R. (2014). La Ley 19.223 en general y el delito de hacking en particular. Revista chilena de Derecho y Tecnología, Vol. 3 N.1, 11-78.

- Lara, JC. Martínez, M. Violler, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. Revista chilena de Derecho y Tecnología, Vol. 3, NRO. 1, 101-137.
- Márques Cardenas, A. Gonzalez Payarés, O. (enero-junio 2008). La Coautoría: Delitos Comunes y Especiales. Revista de Dialogos y Saberes, ISSN0124-0021, 29 - 50.
- Jacobsson, M. Myers, S. (2007). Phishing and Countermeasures. Indiana: John Wiley & Sons, Inc.
- Liskan, A y Timothy, G. (2017). Ransomware, defending Against Digital Extortion. California, United States: O'Rilley.
- Moscoso Escobar, R. (2014). La Ley 19.223 en general y el delito de *hacking* en particular. Revista chilena de Derecho y Tecnología, Vol. 3 NRO. 1, 11-78.