Universidad Andrés Bello

Facultad de Derecho

Álvaro Francisco Bustos Bobadilla y Carlos Alberto Zúñiga Sánchez

Análisis de los delitos informáticos en el derecho chileno y comparado

Tesina para optar al grado de Licenciado en Ciencias Jurídicas dirigida por el Profesor don Sergio Peña Neira.

Santiago de Chile

2013

Álvaro Bustos Bobadilla

Agradezco a mis padres, especialmente a mi madre por tenerme paciencia y servirme con mucho cariño todas las tazas de café que necesité para escribir la presente obra, también a mi abuela Ximena, a quien adoro y a mi hermano "Chinchillo" por jugar en su PC mientras escribíamos.

Carlos Zúñiga Sánchez

Agradezco de todo corazón a todas aquellos quienes me han apoyado para poder llegar hasta estas instancias, ya que sin ellos no podría haberlo logrado, y en especial a aquella persona que me sabido entender y comprender en todo.

Gracias a todos.

Introducción

La presente tesina tiene como finalidad realizar un análisis acerca de los delitos informáticos en nuestra legislación y en derecho comparado, informando al lector acerca de la realidad actual de las regulaciones relativas a estos delitos y ver las falencias de nuestra legislación.

Esta tesina es de carácter explicativo, puesto que la metodología sistemática que se empleará en el desarrollo de esta obra será imparcial, por lo tanto, se abstendrá de emitir comentarios, criticas, argumentos u opiniones de carácter valórico, simplemente se hará un análisis descriptivo y científico de la temática a desarrollar.

Se puede observar que nuestro ordenamiento jurídico carece de regulación suficiente para solucionar de manera eficaz y eficiente los conflictos jurídicos que se suscitan en relación con la informática, dejando de manifiesto las imprecisiones que el legislador ha cometido en el desarrollo de la presente ley. Por ello, la búsqueda de respuestas a este tipo de problemáticas se hace de carácter imperativo, y el presente trabajo tratará de solucionar de la mejor manera posible dichas problemáticas.

En segundo lugar, teniendo presente lo dicho con anterioridad, el objetivo y justificación de la presente obra es desarrollar de manera comparativa y sistemática un análisis a la legislación nacional y extranjera, evidenciando con ello el mayor o menor desarrollo en los respectivos ordenamientos jurídicos analizados, poniendo énfasis en el régimen jurídico nacional, entregando las herramientas suficientes y necesarias para identificar las falencias y deficiencias que ha desarrollado el régimen jurídico desde la dictación de la ley hasta la actualidad, además, entregando al lector los medios necesarios para lograr familiarizarse de modo más preciso y completo con la temática relativa a los delitos informáticos.

En cuanto al contenido de la presente obra, es menester señalar que en el primer capítulo se abordarán temáticas de carácter general en lo relativo a los delitos

informáticos, estableciendo con ello una base para mejor comprensión de la obra en los capítulos posteriores.

En el segundo capítulo, se abordará directamente el análisis, tanto de la legislación nacional como de la legislación comparada, exponiendo detalladamente sus normativas y criterios relativos a los delitos informáticos. Lo anterior servirá como fundamento para la posterior proposición de soluciones a las problemáticas relativas a la aplicación de la ley que trata sobre los delitos informáticos en Chile.

Por último, en el tercer capítulo se abordará de forma directa el problema en cuanto a la aplicación de la ley 19.223, los criterios que tiene en consideración el legislador nacional en lo relativo a los requisitos de aplicación de ésta en comparación con los criterios de las legislaciones extranjeras y nuestras propuestas encaminadas a mejorar la efectividad de dicha normativa.

Capítulo I

I. Aspectos generales relativos a la informática

Antes de comenzar el análisis expuesto de esta obra será necesario dar a conocer los aspectos generales relativos a la informática con la finalidad de que el lector tenga una mejor y más amplia posibilidad de entendimiento respecto a la temática a abordar, ya que debido a lo extenso de su contenido y a lo complejo que resultan muchas definiciones en cuanto a su redacción, se hace menester mencionar conceptos que tienen como finalidad arrojar luz sobre aquellos pasajes obscuros o de difícil interpretación en la presente obra.

Dentro de estos conceptos podemos encontrar el delito, que para estos efectos se entenderá, según Enrique Cury como una acción u omisión típicamente antijurídica y culpable[1], en el fondo este concepto será de gran utilidad para esclarecer con posterioridad el concepto de delito informático y sus respectivas clasificaciones.

Es también de suma importancia para los efectos de esclarecer con mayor facilidad el concepto de delito informático exponer la noción del concepto de informática, que se entiende que es aquella ciencia que estudia y tiene como objeto el tratamiento automatizado o electrónico de la información[2]. Cabe hacer presente que este concepto nos obliga a tener en cuenta todo aquello que conforma un aparato de tratamiento automatizado o electrónico de la información, es decir, los componentes de una computadora o cualquier dispositivo que sea capaz de procesar información (como lo es un I-phone, i-pads, tablets, laptops, smartphones, etc.)

Un aparato que sea capaz de realizar tratamientos automatizados o electrónicos de información está compuesto por dos grandes tipos de soportes, los cuales son el

[1]CURY URZÚA, ENRIQUE, "Derecho Penal, parte general", Santiago, Chile, Ediciones Universidad Católica de Chile, 2009, 9a. ed., p. 243.
[2]MAGLIONAMARKOVICTH, CLAUDIO PAUL, "Delincuencia y fraude informático", derecho comparado y ley No. 19.223, Santiago, Chile Editorial Jurídica de Chile, 1999, p. 19.

hardware (soporte físico) y el software (soporte lógico)[3]. En cuanto al primero, se alude a la maquinaria, la CPU y todos los periféricos. Cualquier dispositivo microelectrónico que contrasta con el software, constituido por las instrucciones que indican a la computadora qué hacer[4], y en cuanto al segundo elemento se alude al equipo lógico, logicial, o soporte lógico. Esta parte inmaterial está formada por un conjunto de programas que determinan el funcionamiento de los circuitos físicos que se contienen en el sistema informático.[5]

Ahora bien, teniendo en cuenta lo expuesto anteriormente, es el derecho informático el que debiese encargarse de regular esta materia, ya que se trata de un conjunto de principios, instituciones y normas jurídicas de naturaleza fundamentalmente específica que tiene por fin último la regulación de toda actividad derivada de las ciencias informáticas.[6] En el caso de nuestro país, de ello se encarga la ley 19.223, que trataremos con mayor profundidad en los capítulos segundo y tercero.

A. Delito informático

Es un hecho que a lo largo de la historia de la evolución de la sociedad, ésta ha avanzado a pasos agigantados, tanto en su forma de desarrollo cultural como también en lo relativo a las tecnologías creadas por el hombre, es aquí donde surgen los llamados "Delitos informáticos" donde la mal utilización de las nuevas tecnologías de la información, en especial de los sistemas automatizados de tratamiento de la información o "Softwares" ha acarreado consecuencias muy perniciosas en la actual Sociedad, las cuales se evidencian en los diversos delitos relacionados con medios informáticos, sin embargo es aquí donde se debe comenzar a realizar un serie de distinciones las cuales ayudarán a diferenciar de forma clara y precisa los diferentes delitos en los cuales se utilizan medios informáticos, ya que es de vital trascendencia entender que no todo delito en el cual se utiliza tecnología de la información es un delito informático.

---

[3]HERRERA BRAVO, RODOLFO, "Reflexiones sobre la delincuencia vinculada con la tecnología digital (basadas en la experiencia chilena)", http://rodolfoherrera.galeon.com/refxdel.pdf, p.5.
[4]VERA QUILODRÁN, ALEJANDRO A, "Delito e informática, La informática como fuente de delito", Santiago, Chile Ediciones Jurídicas La Ley, 1996, p. 237.
[5]HUERTA M., MARCELO, "Delitos informáticos", Santiago, Chile, Editorial Jurídica ConoSurLtda, 1998, 2a. ed, p.340.
[6]Ibíd., p. 237.

Así surge la pregunta: ¿Que es un delito informático? diversos autores establecen las variadas definiciones entre las cuales podemos encontrar las más importantes.

Así un delito informático es "Toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable, y atente contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del empleo de las tecnologías de la información, y el cual se distingue de los delitos computacionales o tradicionales informatizados".[7], ésta es una idea similar a la sostenida por el profesor alemán Ulrich Sieber, quien los define como "todas las lesiones dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente"[8], sin embargo se encuentra inmersa en esta última definición el elemento del dolo, (que más adelante trataremos con más detalle). Cabe tener presente que como se señala en las presentes definiciones, no todo delito cometido por un medio informático es un delito informático propiamente tal, puesto que hay que efectuar una gran distinción entre un delito informático y un delito computacional, el primero consiste como ya se mencionó en aquellos casos donde la conducta atenta contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes[9] y en el caso del segundo, "el bien jurídico que requiere de protección resulta amparado por otras normas penales (propiedad, fe pública, orden público, etc.). Estando la autonomía del tipo referida a los medios de comisión y requiriéndose el uso del computador o de sus equipos periféricos"[10] esto implica que aquellos delitos en los cuales se utilice un medio computacional con el cual se vulnere, a modo de ejemplo, las partes de un ordenador provocando graves daños a su estructura física, sería un delito de daños a la propiedad, por ende, la sanción punitiva se enmarcaría en la legislación de aplicación general y no propiamente en el tratamiento que se debiese aplicar a los delitos informáticos, como es el típico caso donde un virus computacional, el cual fuerza el voltaje de la fuente de

[7]BELTRAMONE GUILLERMO,HERRERA BRAVO RODOLFO, ZABALE EZEQUIEL, "Nociones básicas sobre los Delitos Informáticos**",** Ponencia preparada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile, agosto de 1998, p. 6.
[8] HERRERA BRAVO RODOLFO, "Reflexiones sobre la delincuencia vinculada con la tecnología digital (basadas en la experiencia chilena)", http://rodolfoherrera.galeon.com/refxdel.pdf, p.7.
[9] HERRERA BRAVO RODOLFO, Ibid., p.3.
[10]JIJENA LEIVA, RENATO, "La protección penal de la intimidad y el delito informático"., Santiago, Chile, Ed. Jurídica de Chile, 1992, p. 85.

poder del ordenador provocando un corto circuito y con ello daños irreversibles a éste en su soporte lógico.

En síntesis, para poder entender en su cabalidad qué es un delito informático se debe comprender aquello que atente contra el soporte lógico o "software" y no contra el soporte físico o "hardware", por ello además se debe tener presente que a raíz de lo anterior se suscita la necesidad de distinguir claramente entre un delito computacional y uno informático, ya que constituye un importantísimo aporte para delimitar el tipo penal apropiado en la aplicación al delito informático.

B. Clasificación

Como se ha podido apreciar, en la actualidad las tecnologías informáticas han ido evolucionando de una forma abrumadora y veloz, donde la obsolescencia de las tecnologías cada vez es de menor tiempo, es por ello que es necesario para poder dar mayor certeza al presente estudio establecer las diferentes formas de delitos informáticos que se pueden suscitar en la actualidad.

Así podemos encontrar muchas modalidades de ilícitos informáticos, para ello utilizaremos la clasificación más aceptada por la mayoría de la doctrina la cual es propuesta por el profesor Ulrich Sieber entre los delitos de:

1.- fraude mediante la manipulación de los datos;

2.- delitos de espionaje informático, piratería de software y sustracción de alta tecnología;

3.- el sabotaje informático;

4.- la sustracción de servicios;

5.- el delito de acceso indebido;

6.- y el fraude fiscal relacionado con el ordenador.[11]

[11]HERRERA BRAVO RODOLFO, Ibíd., p. 11.

En cuanto a esta clasificación, posteriormente se procederá a hacer un análisis respecto a la relación existente entre estas y el derecho chileno.

De antemano, es menester dejar en claro que las figuras típicas que se expondrán a continuación, como es el caso del sabotaje informático o los delitos de espionaje informático, entre otras, han sido abordadas por las legislaciones que se analizarán más adelante, además de ello resulta de vital trascendencia esclarecer que dichas figuras típicas constituyen el género y los conceptos que deriven de dichas figuras constituirán la especie.

i. Delitos de Sabotaje Informático

Rodolfo Herrera Bravo define el sabotaje informático como la acción típica, antijurídica y dolosa destinada a destruir o inutilizar el soporte lógico de un sistema computacional mediante el empleo natural de las tecnologías de la información.[12] Teniendo en cuenta la presente definición, consideramos que ésta incorpora un elemento que no merece ser incorporado a dicho concepto, el cual es el dolo, (tema que trataremos con mayor precisión más adelante).

Hay que tener presente que lo esencial en éstos delitos es que, ya sea en primera instancia es destruir parte de los datos e información esencial para el aparato tecnológico, o por lo menos alterar su normal funcionamiento en cuanto a las operaciones que debiese realizar éste de forma habitual.

Por ello con la actual evolución de la ciencia de la informática se han elaborado las más diversas formas y medios de cometer este tipo de ilícito, y entre las más importantes se pueden apreciar las siguientes:

Programas Virus: es un "programa computacional"[13]que puede producir alteraciones más o menos graves en los sistemas de tratamiento de información a los que ataca. Entendiéndolo de esa manera, podríamos decir que todas las modalidades antes

[12]Ibíd., p. 12.
[13]Véase en JOYANES, AGUILAR LUIS, "Fundamentos de programación, algoritmos, estructura de datos y objetos", 3a. ed., editorial Mc Graw Hill, p. 84.

señaladas y las que se emplean para manipular el sistema son virus, es decir, programas o software. Son programas externos al del ordenador que causan daño.

Esta aseveración la postula el profesor Rodolfo Herrera Bravo, quien postula que el gran criterio para poder diferenciar entre los demás delitos de sabotaje informático y un virus informático radica en que el primero posee independencia, es decir, el programa o archivo que se crea para poder provocar un daño al sistema operativo no se adhiere necesariamente a otro, pudiendo actuar de forma directa o a través de otros medios, mientras que los virus propiamente tales, su principal característica es que éstos se propagan por el sistema , creando copias simultaneas de un archivo determinado, provocando en la mayoría de los casos la destrucción o mal funcionamiento del aparato al cual infectan.

Sin embargo advertimos que el presente postulado, en cierta forma carece de la profundidad necesaria para poder efectuar la distinción que se desea llevar a cabo entre el virus y los demás delitos de sabotaje informático, ya que, como se expondrá más adelante, hay ciertas modalidades de sabotaje informático, que si bien podrían utilizarse medios independientes para efectuar el ilícito, dentro del mismo ilícito hay casos en los cuales éstos se incorporan dentro de un programa o archivo, produciendo así la desnaturalización de la distinción antes señalada, como es, por ejemplo, la modalidad de la Bomba Lógica o "Logic Bomb" en las que se efectúa la situación descrita con anterioridad.

De antemano, es menester dejar en claro que las figuras típicas que se expondrán a continuación, como es el caso del sabotaje informático o los delitos de espionaje informático, entre otras, han sido abordadas por las legislaciones que se analizarán más adelante, además de ello resulta de vital trascendencia esclarecer que dichas figuras típicas constituyen el género y los conceptos que deriven de dichas figuras constituirán la especie.

Diversos autores han tratado de postular la distinción entre un virus y los demás delitos de sabotaje, sin lograr su cometido, por ello tratar de efectuar dicha distinción en el presente trabajo sería abordar de forma incorrecta la finalidad de éste, ya que el

presente capitulo solo busca aclarar de forma general los distintos delitos informáticos, para así posteriormente efectuar el análisis a la legislación chilena y su real aplicación.

Bombas Lógicas o "Logic Bombs" de Actuación Retardada: Corresponden al código oculto dentro de una aplicación que se activa cuando se cumplen determinadas condiciones. Por ejemplo una fecha u hora, tras un determinado número de operaciones, secuencia de teclas o comandos, etc. Estos programas persiguen la destrucción o modificación de datos en un momento futuro determinado.

Ahora bien, dentro de las bombas lógicas hay una modalidad en que la principal distinción es la temporalidad en que se reproduce el programa o archivo ilícito, este es el denominado,

Cancer Routine o "Rutina Cáncer": Que consiste en instrucciones que consumen en poco tiempo un software debido a que se expanden al auto reproducir el programa "cáncer" en distintas partes del programa de aplicación, escogidas aleatoriamente durante cada uso.[14]Como se puede apreciar, el daño que se produce es idéntico al de una bomba lógica común, la distinción radica como se dijo anteriormente, en primer lugar, en la temporalidad en que se produce la propagación de la bomba, pero, en segundo lugar, además en la forma en el cual ésta se distribuye, de forma aleatoria en determinados archivos, variando cada vez que se ingresa o inicia el "Software".

System Crash: Son programas que logran un bloqueo total del sistema informático afectando el sistema operativo y los programas almacenados, colapsando el disco duro.[15]

Gusanos: son programas que se infiltran en otros programas legítimos de procesamiento de datos para modificar o destruir la información, pero que a diferencia de los virus, no pueden regenerarse.[16]Sin embargo hay que tener especial atención en este tipo de programa ilícito, ya que, los gusanos utilizan las redes de comunicaciones para expandirse de sistema en sistema, es decir, una vez que un gusano entra a un sistema examina las tablas de ruta, correo u otra información sobre otros sistemas, a fin de copiarse en todos aquellos sistemas sobre los cuales encontró información. Este

[14]HERRERA BRAVO RODOLFO, p. 13.
[15]Ibíd., p. 13.
[16]Ibíd., p. 13.

método de propagación presenta un crecimiento exponencial con lo que puede infectar en muy corto tiempo a una red completa.

Existen básicamente 3 métodos de propagación en los gusanos:

Correo electrónico: el gusano envía una copia de sí mismo a todos los usuarios que aparecen en las libretas de direcciones que encuentran en el computador dónde se ha instalado.

Mecanismos basados en RPC (Remote Procedure Call): el gusano ejecuta una copia de sí mismo en todos los sistemas que aparecen en la tabla de rutas (rcopy y rexecute).

Mecanismos basados en RLOGIN: el gusano se conecta como usuario en otros sistemas y una vez en ellos, se copia y ejecuta de un sistema a otro.

ii. Delitos de Fraude Informático o Manipulaciones no autorizadas de datos

El profesor Romeo Casabona los define como la "incorrecta utilización del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o están ya contenidos en el computador en cualquiera de las fases de su procesamiento o tratamiento informático, siempre que sea con ánimo de lucro y en perjuicio de tercero"[17]

Ahora bien, al igual que la anterior clasificación es necesario establecer las diferentes modalidades de comisión que posee este delito, las formas en las cuales se puede manifestar entre las más importantes se encuentran:

Trojan Horse o Caballo de Troya: son programas aparentemente útiles, que contienen un código oculto programado para ejecutar acciones no esperadas y generalmente indeseables sobre el computador. Del mismo modo que el caballo de Troya mitológico parecía ser un regalo pero contenía soldados griegos que dominaron la

[17]VERA QUILODRÁN, ALEJANDRO A, "Delito e informática, La informática como fuente de delito", Santiago, Chile Ediciones Jurídicas La Ley, 1996, p. 109.

ciudad de Troya, los troyanos de hoy en día son programas informáticos que parecen ser software útil pero que ponen en peligro la seguridad y provocan muchos daños.

Manipulaciones en el input o entrada de datos (Data Diddling): los datos son capturados en documentos originales, tales como registros o facturas, y mediante un método se pueden introducir a la máquina para su proceso.

Técnica Salami o Rounding Down: consiste en introducir al programa instrucciones para que remita a una determinada cuenta cantidades pequeñas de dinero de muchas cuentas corrientes. Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada, consistente en que las cantidades de dinero muy pequeñas, se van sacando repetidamente de una cuenta y se transfiere a otra.

Manipulación indebida de datos a través de la utilización de un sistema de tratamiento de la información: ésta manipulación puede realizarse a través de la utilización de un sistema (input) en los programas, en la salida de datos del sistema (output) y las manipulaciones a distancia, mediante conexión telemática vía módem a un computador.

iii. Delitos de Espionaje Informático

Consiste en la obtención no autorizada de datos almacenados en un fichero automatizado, en virtud del cual se produce la violación de la reserva o secreto de información de un sistema de tratamiento de la misma. [18]

La comisión de estos posee una variada clasificación pero las más importantes se señalan a continuación.

Data leakage o divulgación no autorizada de datos reservados: son delitos de espionaje industrial, que consisten en la sustracción de información confidencial, mediante técnicas tan simples como el copiar un archivo para luego venderlo.

Wiretapping o Pinchado de líneas: consiste en una intercepción programada de las comunicaciones que circulan a través de las líneas telefónicas, con el objeto de

[18]HERRERA BRAVO RODOLFO, Ibíd., p. 20.

procurarse ilegalmente la información, pero permitiendo luego, la recepción normal de la comunicación por parte del destinatario de la misma. Por este último motivo, es prácticamente imposible descubrirlo antes de advertir que la información secreta ha sido conocida y utilizada por otros.

La forma más simple de cometerlo es ubicando el cable por el que circula la información en forma análoga y pincharlo directamente. Así, las señales telefónicas se pueden grabar, para luego ser demoduladas por el módem, el que las transforma a señal digital que puede ser ingresada al ordenador. Otras formas más complejas permiten realizar pinchados a distancia, especialmente a través de la captación de las señales microondas emitidas por teléfonos móviles, las cuales igualmente pueden ser demoduladas en el módem del delincuente, para que la información tenga un lenguaje comprensible.

Electronic Scavenging o Recogida de información residual: se producirá cuando una persona obtiene sin autorización la información que ha sido abandonada sin ninguna protección como residuos de trabajo.

iv. Delito de "Piratería" Informática o copia ilegal o no autorizada de programas del Ordenador.

Consiste en la copia o uso ilegal de los programas. La piratería es un problema enorme debido a que es muy fácil de llevar a cabo. En la mayor parte de los casos, robar un programa no es más difícil de lo que significa copiar un disco compacto de música ajeno. Los piratas de softwares renuncian al derecho de recibir actualizaciones y soporte técnico, pero obtienen el uso del programa sin pagar por él.

Según el legislador chileno, persigue no solo la reproducción, sino también la distribución, comunicación, plagio, transformación, exportación o importación de softwares, sin autorización, con o sin ánimo de lucro. Debe ser utilizado para ello un sistema de tratamiento de información y su comisión atenta contra el legítimo derecho del fabricante del programa.

v. Delito de acceso no autorizado o hacking directo

Hacking: consiste en acceder a la información de una persona contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información sin su consentimiento.

Cabe señalar que la característica esencial del hacking es la de acceder o vulnerar la base de datos o sistema de procesamiento de datos, sin cometer daño a ésta, sin embargo debe además considerarse que la doctrina discute respecto a la real tipificación del hacking directo, hay argumentos a favor y en contra, pero debido a lo extenso de la materia a tratar no será objeto del presente estudio.

Sin perjuicio de lo dicho anteriormente, es necesario aclarar que diversas modalidades de hacking las cuales son de la más variada forma y modo, así encontramos los más importantes, y de los cuales concordamos en su totalidad con los propuestos por mayoría de la doctrina, los cuales son:

Spoofing: hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. Este se puede realizar de diversas formas.

IP Spoofing o suplantación de IP: Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.

ARP Spoofing: suplantación de identidad por falsificación de tabla ARP. (ARP son las siglas en inglés de Address Resolution Protocol, Protocolo de resolución de direcciones en español).

DNS Spoofing: suplantación de identidad por nombre de dominio.

Web Spoofing o suplantación de una página web real, Mail Spoofing: Suplantación en correo electrónico de la dirección e-mail de otras personas o entidades.[19]

Shoulder surfing: Consiste en espiar directamente a los operadores y anotar la contraseña a través de la observación visual del momento en que el usuario digita la contraseña en el teclado del ordenador.[20]

Para concluir, ha quedado de manifiesto que la presente clasificación los delitos informáticos busca dos objetivos de suma importancia, el primero establecer un marco general relativo a éstos hechos ilícitos proporcionado nociones y elementos que ayuden a comprender conceptos y definiciones que de cierta forma son ajenas al común de las personas, con lo cual, cobra una vital importancia para efectuar el desarrollo posterior de la presente obra, y el segundo objetivo, busca otorgar las bases para el posterior análisis relativo a la legislación chilena, ya que en su mayoría de los delitos informáticos señalados anteriormente no se encuentran tratados en ésta, por ello se requiere profundizar el tema comenzando de esta forma.

C. Bien jurídico protegido

En cuanto al bien jurídico protegido por la materia que tratamos, en Chile la doctrina no se ha puesto de acuerdo respecto a uno en particular, de hecho se ha mencionado una serie de bienes jurídicos que podrían estar amparados por el tema que nos ocupa, tales como, Patrimonio, intimidad, confidencialidad, seguridad y fiabilidad del tráfico jurídico y probatorio, propiedad sobre la información, y la pureza de la técnica que supone la informática, son algunos de los bienes que suelen mencionarse[21], sin embargo el bien jurídico protegido que el legislador consideró para la redacción de la ley 19.223 es "el proteger un nuevo bien jurídico surgido con el uso de las modernas tecnologías

[19]Glosario de términos relacionados con los delitos informáticos, www.delitosinformaticos.com, entrada del 2 de marzo del año 2009, consultada el 11 de noviembre del 2012, URL:http://www.delitosinformaticos.com/03/2009/delitos/glosario-de-terminos-relacionados-con-los-delitos-informaticos#.UKAepOTglDs

[20]HERRERA BRAVO RODOLFO, Ibíd., p. 27.

[21] BRAVO HERRERA, RODOLFO, ibíd., p. 8.

computacionales: la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan. Aquella, por el actual desarrollo tecnológico de la sociedad merece ser protegida mediante la creación de figuras delictuales nuevas, que pongan de relieve su importancia"[22]. En el fondo, lo que el legislador busca proteger bajo esta lógica no es una serie de bienes jurídicos, sino que uno en particular que tiene carácter universal y no particular como sucede con el caso del dominio o la privacidad y que surge producto del avance de la tecnología dentro de la sociedad, lo que hace necesario que se protejan nuevos intereses relevantes de las personas en tanto sujetos sociales, considerados especialmente valiosos y consecuentemente, dignos de protección penal frente a conductas que los dañan o ponen en peligro.

López Pinto Agrega que las premisas fundamentales en las que se basa este bien jurídico son:

La primera premisa que plantea es la libertad de opción. El alterar, obstaculizar, inutilizar o destruir un sistema de tratamiento de información, impedirá utilizarlo, y con ello, no se podrán adoptar decisiones satisfactorias, afectándose la expresión máxima de libertad en el actuar del hombre, cual es la capacidad de decidir. Además, si consideramos que el ilícito informático es de carácter masivo, no sólo afecta a una o algunas personas, sino a la sociedad toda, en los más diversos ámbitos de la existencia humana, sería inoficioso fundar la protección de la informática en consideraciones individualistas, como la protección de la propiedad o de la intimidad personal, dejando de lado otros aspectos que pueden verse afectados como la utilización ilícita de la ciencia informática en la política, la economía, la seguridad nacional, la salud pública, la educación y muchos otros.

En el fondo, lo que sostiene este autor es que al ser el delito informático un acto u omisión que puede dañar bienes jurídicos de carácter particular como social, si este logra vulnerar derechos o garantías de una o más personas (tales como la intimidad, seguridad o su patrimonio), se hace necesario crear una protección por parte del legislador sobre el bien jurídico más amplia, en el sentido de que todos, y cada uno de los miembros de la

[22]Véase LÓPEZ PINTO, R. "Delito informático: bien jurídico protegido en la ley N°19.223", Revista Ad Libitum N°3. Universidad Central de Chile. 1994, pp. 22-26.

sociedad puedan estar asegurados en cuanto a su libertad de tratamiento de la información que puedan estimar como personal o privada, pública o con acceso restringido.

La segunda premisa que sostiene es que la ciencia informática se debe fundar en consideraciones éticas. Esto quiere decir que la finalidad de la ciencia informática debiese tener como finalidad el perfeccionamiento y progreso de la humanidad, en el sentido de que debiese ser un medio para tomar decisiones o un medio para llevarlas a cabo mediante el uso de un aparato automatizado que realice un tratamiento de información, todo ello encaminado a lograr alcanzar la mayor realización espiritual como material posible de la persona humana, lo que a fin de cuentas se aproxima a alcanzar el bien común a través de la libertad para tomar decisiones.

Respecto a este punto, a nuestro parecer, teniendo en cuenta nuestra realidad tecnológica actual y nuestro sistema democrático en un Estado de derecho, en donde se entiende que el Estado está al servicio de la persona humana, con mayor razón debiese darse protección a estos nuevos bienes jurídicos que han surgido producto del avance de la ciencia por parte de nuestro legislador, ya que en la actualidad muchos de los actos jurídicos cotidianos que realizan las personas en la sociedad (como por ejemplo, celebrar contratos, efectuar operaciones bancarias, etc.) se llevan a cabo mediante el empleo de dispositivos de tratamiento de información, en consecuencia, si se ampliara la protección a estos bienes jurídicos, se lograría una mejor protección a los derechos y garantías que consagra nuestro ordenamiento jurídico.

Es importante también destacar que este autor considera que lo importante es que la decisión que se tomó esté fundada en un valor y no que esté fundada en la ejecución de decisiones predeterminadas, a modo de ejemplo, sostiene que el valor o desvalor entre dos programas computacionales destinados a destruir, modificar o inutilizar un sistema de tratamiento de información (hecho constitutivo de delito), tales como un virus y un antivirus, estará determinado por la finalidad que existe en cuanto a su empleo, en el caso del antivirus, los efectos de su ejecución estarán justificados puesto que su finalidad es proteger el bien jurídico, que en este caso es la pureza, calidad e idoneidad de la ciencia informática, por lo tanto, siguiendo esta lógica, el virus sería para estos efectos

constitutivo de delito puesto que la finalidad para la cual este se emplea sería el desvalor[23].

Sobre la misma temática analizada anteriormente, Rodolfo Herrera sostiene que existe la posibilidad de que en los delitos informáticos pueda existir una multiplicidad de bienes jurídicos que se protegen, debido a la naturaleza de los datos, información y derechos que se vulneran, tales como la propiedad intelectual si el delito recayese sobre datos informáticos que contengan material creado por su dueño, como sucede con la piratería o copia ilegal de programas computacionales[24].

Respecto a este punto, teniendo en cuenta que los delitos informáticos tienen un campo de acción demasiado amplio (en donde se pueden afectar tanto derechos individuales como sociales), y según avanza el tiempo y la tecnología informática, ésta prácticamente se encuentra en cada hogar, entonces, teniendo en cuenta lo anterior, surge la necesidad de que el legislador considere este tema con mayor énfasis con la finalidad de que se logre proteger al mayor número de posibles sujetos pasivos del delito.

Finalmente Roberto Herrera sostiene que, "respecto al bien jurídico de la idoneidad, calidad y pureza de la técnica que supone la informática, de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan, propuesto por el legislador, lo consideramos impreciso. Primero, porque comprende a toda información contenida en un sistema informático, en circunstancias que somos de la idea de distinguir previamente la naturaleza de los datos procesados y sólo proteger penalmente a aquellos relevantes o de importancia. Segundo, es erróneo sancionar como "delito informático" a los atentados contra todo el sistema informático, incluido el soporte físico o hardware. Y además, incurre el legislador en enfoques equivocados a causa de su desconocimiento en la materia, de manifiesto en las contradicciones en que incurre, ya que en su oportunidad explicó este punto diciendo que el sistema informático era el nuevo bien jurídico que se quiere proteger, el cual difícilmente puede asimilarse a otros penalmente protegidos.

[23]Ibíd. pp.22-26.
[24]BRAVO HERRERA, RODOLFO, ibíd., pp. 9-10.

Entonces, ¿cuál es supuestamente ese nuevo bien jurídico, la información en cuanto tal o la totalidad del sistema informático, incluido el hardware?"[25].

En síntesis de todo lo analizado hasta el momento, intentaremos dejar en claro cuál es el bien jurídico en concreto que se busca proteger, si bien es cierto, teniendo en cuenta lo expuesto anteriormente a que el delito informático propiamente tal no puede recaer sobre el soporte físico del dispositivo o hardware, sino que sobre el lógico o software, concluimos según esta lógica que todos aquellos programas, instrucciones o comandos electrónicos que el dispositivo de procesamiento de información pueda llevar a cabo son objeto del delito informático, por lo tanto quedan excluidos como delitos informáticos aquellos daños, inutilizaciones, o destrucción del material físico del cual se compone el dispositivo de tratamiento de información, puesto que los actos que atenten contra éste mediante un dispositivo de procesamiento de información serán considerados como delito de daños propiamente tal, y no como un delito informático.

Entonces, a modo de conclusión, podríamos decir que el bien jurídico que se busca proteger con el presente tipo penal seria una serie de derechos y garantías que el ordenamiento jurídico consagra a favor de las personas que podrían encontrarse inmersos dentro de un software dependiendo del elemento electrónico de que se trate, como por ejemplo, en el caso de fotografías subidas desde una cámara fotográfica digital a un computador, podríamos hablar de elementos personales de quien que las sube, en ese caso el bien jurídico protegido podría ser la privacidad y el dominio sobre dichos archivos o datos electrónicos.

D. Sujetos del delito informático

En cuanto a los sujetos del delito informático, será necesario entender qué es un sujeto activo y un sujeto pasivo del delito informático. Para estos efectos, quienes pueden ser sujeto activo o pasivo del delito en materia de delitos informáticos, serán las personas o grupos de personas que pueden cometer (sujeto activo) o ser afectados

[25]BRAVO HERRERA, RODOLFO, ibíd., p. 10.

(sujeto pasivo) por la comisión de un hecho ilícito, en este caso particular de un delito informático.[26]

Aclarado el concepto es necesario también tener presente que en la misma obra, se señala que pueden ser sujeto activo del delito informático "cualquier persona física o natural", pero luego agrega que "no creemos en cambio que puedan serlo las personas jurídicas teniendo en cuenta la naturaleza de las acciones involucradas"[27].

A nuestro juicio esa postura es razonable, puesto que en la actualidad existe discusión doctrinaria acerca de la responsabilidad penal de las personas jurídicas, que es una temática que no nos atañe abordar en la presente obra. Sin embargo, si nos ponemos en la hipótesis de que una persona perteneciente a una personalidad jurídica comete delitos de esta naturaleza, creemos que será responsable personalmente la persona natural que cometió el acto y no la persona jurídica de la que es parte.

En cuanto al sujeto pasivo del delito si seguimos esta misma lógica, puede serlo tanto una persona natural como una jurídica, aunque es necesario recordar que para ser sujeto pasivo de un delito informático se debe ser titular de derechos sobre un software o soporte lógico de un dispositivo de tratamiento de información que sea de tal importancia que se encuentre protegido por el tipo penal, ya que de lo contrario el sujeto pasivo podría ser víctima de otro tipo de delito, como el de daños por ejemplo.

[26]BELTRAMONE, GUILLERMO, HERRERA BRAVO, RODOLFO, ZABALE, EZEQUIEL, "Nociones básicas sobre los delitos informáticos", ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de derecho penal y criminología, celebrado en la universidad de Chile en Agosto de 1998.,p. 7.
[27]Ibíd. p.7.

Capítulo II

En el presente capitulo nos avocaremos a realizar un extenso análisis acerca de la legislación chilena, teniendo en consideración los distintos elementos que configuran el tipo penal relativos los delitos informáticos, asimismo se analizarán diferentes legislaciones internacionales, en específico Francia, Alemania y España, las cuales constituyen las más relevantes e influyentes a nivel global, por ello se comenzará con la legislación nacional:

I. Análisis general de la legislación chilena

En Chile existe solo una ley vigente hasta la fecha que regula materias relativas a los delitos informáticos, esta es la ley 19.223, la cual solo está compuesta de cuatro artículos, la cual expondremos a continuación.

> *"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.*
>
> *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.*
>
> *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.*
>
> *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."*[28]

[28]República de Chile, Ley 19.223, Tipifica figuras penales relativas a la informática, Valparaíso, 7 de Junio de 1993.

Así para comenzar el análisis de la presente ley es necesario clasificar los delitos los cuales consagra ésta, estos son sabotaje informático y espionaje informático.

A. Sabotaje informático

Entenderemos por sabotaje informático a la definición anteriormente proporcionada en el capítulo primero de esta obra, así se concebirá como la acción típica, antijurídica y dolosa destinada a destruir o inutilizar el soporte lógico de un sistema computacional mediante el empleo natural de las tecnologías de la información, aunque nuevamente volvemos a destacar que a nuestro juicio el elemento doloso no debiese incluirse en la normativa (por razones que se explicarán con posterioridad)

Estos se encuentran consagrados en los artículos N° 1 y 3 de la presente ley, los cuales consagran la afectación del los sistemas de tratamientos de la información incluyendo su funcionamiento, como los datos contenidos en éste.

En primer lugar se deben identificar los sujetos objeto del tipo penal, por ello es menester comenzar con al sujeto activo, en cuanto a éste, cabe señalar que la presente ley en su generalidad utiliza en todos sus artículos la expresión "el que" por ello y en razón de lo anterior, no se requiere de la realización de la acción por parte de un sujeto calificado, es decir, puede ser efectuada de forma indistinta por cualquier persona.

En relación con el sujeto pasivo cabe tener presente lo anteriormente señalado, es decir puede ser cualquiera de forma indistinta, eso incluye tanto personas naturales o jurídicas tanto de derecho público como privado.

En segundo lugar, las faz objetiva del tipo se configura por determinadas conductas realizadas por los sujetos, en específico en el artículo primero se señala en el comienzo de éste "destruir", "inutilizar" el sistema de tratamientos de la información o sus componentes, y la segunda señala "impedir" "modificar" u "obstaculizar" su funcionamiento, y para finalizar, el artículo primero en su inciso segundo se aplica una agravante cuando se afecten datos contenidos en el sistema. Todo ello relacionado con

el artículo numero 3 y las expresiones "dañar" y "destruir", las cuales son de vital importancia el presente delito de sabotaje informático.

En cuanto al primero entenderemos por "destruir" a reducir a pedazos o destrozar[29] y por "inutilizar" hacer inútil, vano o nulo algo[30], con lo cual entendemos que el legislador al utilizar dichas expresiones enmarcó al sujeto activo con la ejecución de dichas acciones sobre el sistema de tratamiento de la información o aparato lógico y además sobre el elemento físico, lo cual a nuestro parecer no sería el tratamiento adecuado para ello por los motivos que posteriormente señalaremos en el capítulo tercero de la presente obra, ya que ahora solo efectuaremos un análisis de carácter expositivo identificando solo los elementos de la presente legislación.

En relación con el correcto funcionamiento, los verbos "impedir" lo entenderemos como estorbar, imposibilitar la ejecución de algo[31], "modificar" como transformar o cambiar algo mudando alguno de sus accidentes[32], y por ultimo "obstaculizar" como impedir o dificultar la consecución de un propósito[33] , con lo cual, según lo expuesto anteriormente cualquier conducta o acción que afecte el correcto funcionamiento tanto el sistema de tratamiento de la información como el soporte físico de éste, ya sea que estorbe, imposibilite, trasforme o dificulte el funcionamiento de éstos constituirá un ilícito de carácter punible bajo la esfera de los delito informáticos, situación la cual no compartimos, y que con posterioridad se abarcará con mayor profundidad.

En el artículo N° 3 de la presente ley se utilizan los verbos "dañar" y "destruir", entenderemos por el primero como causar detrimento, perjuicio, menoscabo, dolor o molestia.[34] Y por el segundo como lo anteriormente señalado, con lo cual el legislador al

[29]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/dpd/?key=destruir
[30]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=inutilizar
[31]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=impedir
[32]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=modificar
[33]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=obstaculizar
[34]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=da%C3%B1ar

efectuar dicha distinción previo las dos hipótesis posibles en cuanto a la ejecución del sabotaje informático, cual es en primer lugar la producción de un perjuicio o menoscabo en un sistema de tratamiento de la información continuando su funcionamiento de forma impropia para la cual fue diseñado, y en segundo lugar, la hipótesis más amplia en la cual se establece la destrucción del sistema lógico por la acción típica, no pudiendo continuar con su funcionamiento, con lo cual se produce así una relación de género y especie, donde la destrucción es el género y el daño la especie

En tercer lugar analizaremos la faz subjetiva del tipo, en la presente ley cabe señalar que las figuras contenidas en ésta se satisfacen solo con dolo, por lo cual se debe dejar fuera cualquier análisis tendiente a incorporar la culpa en las presentes figuras, ya que al señalar " el que maliciosamente" queda de manifiesto dicha situación, sin embargo surge una discusión relativa a el tipo de dolo el cual se debe entender para el presente tipo, parte de la doctrina señala que debe ser solamente dolo directo, y la otra parte señala que se debe incorporar dolo eventual, esta situación será analizada con posterioridad en el capítulo tercero de esta obra

B. Espionaje informático

Como señalamos anteriormente, el espionaje informático según la definición expuesta con anterioridad consiste en la obtención no autorizada de datos almacenados en un fichero automatizado, en virtud del cual se produce la violación de la reserva o secreto de información de un sistema de tratamiento de la misma. Esta figura típica se encuentra manifiesta en los artículos 2 y 4 de la presente ley.

En el artículo 2 se consagra el delito de espionaje informático al establecer en el tipo penal la frase "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". Analizando el presente artículo podemos concluir en primer lugar que en cuanto al sujeto activo, éste resulta ser indeterminado al igual como sucede en lo relativo al sabotaje informático, y en cuanto a la víctima, en esta clase de delitos siempre será

indeterminada, ya que no se establece en ninguna norma relativa al tema un sujeto pasivo en particular.

En segundo lugar, en cuanto a la faz subjetiva del tipo, ésta se puede manifestar a través de tres ánimos que puede tener el sujeto activo, los cuales son: apoderarse, usar o conocer.

En primer término se alude a "apoderarse", que significa poner algo en poder de alguien o darle la posesión de ello[35] entonces, teniendo en cuenta el presente concepto, para que se pueda aplicar la norma al sujeto activo será necesario que éste tenga la intención de hacerse con los datos contenidos en un sistema de tratamiento de información de forma indebida, vale decir, sin la autorización de la víctima.

En cuanto al término "usar", la Real Academia Española lo define como hacer servir una cosa para algo[36]. En el fondo, para que sea aplicable la norma al caso concreto, será menester que el sujeto activo tenga la intención de ejecutar o iniciar las funciones de un programa computacional o software contenido en un sistema de tratamiento de información ajeno sin la autorización de quien corresponda.

En lo relativo al término "conocer", se define como averiguar por el ejercicio de las facultades intelectuales la naturaleza, cualidades y relaciones de las cosas[37]. En el fondo, el legislador considera necesario para la aplicabilidad de la norma que el sujeto activo tenga el ánimo de descubrir la funcionalidad de un programa computacional o software contenido en un sistema de tratamiento de información ajeno, y en caso que el sujeto no tenga dicha intencionalidad, la norma no podrá ser aplicada al caso concreto.

En tercer lugar, en lo relativo a la faz objetiva del tipo, nos encontramos con tres conductas que el sujeto activo puede llevar a cabo para la comisión del delito, estas son: interceptar, interferir o acceder.

---

[35]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=apoderarse

[36]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=usar

[37]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=conocer

En cuanto al concepto "interceptar", éste se define como apoderarse de algo antes de que llegue a su destino[38], es decir, para que opere el delito bajo esta modalidad será menester que el sujeto activo acceda a una vía de comunicación del sujeto pasivo (como por ejemplo su correo electrónico), una vez que tenga acceso a dicha vía, deberá hacerse con el control de la información o datos que la víctima intenta enviar a un destinatario determinado (por ejemplo usando Wiretapping).

En cuanto al acto de "interferir", se entiende que es cruzar, interponer algo en el camino de otra cosa, o en una acción[39]. Para que se logre llevar a cabo el delito mediante esta modalidad, será necesario que el sujeto activo logre evitar la transferencia de información por parte de la víctima a su destinatario mediante el empleo del algún software maligno.

En lo relativo al término "acceder", éste significa entrar en un lugar o pasar a él[40]. Entonces, teniendo en cuenta el concepto, para que se cometa el delito con esta modalidad será necesario que el sujeto activo logre vulnerar las defensas del soporte lógico que contiene la información para poder llegar hasta ella, este es el caso donde pudiese aplicarse la técnica del hacking o acceso no autorizado por parte de la víctima a un sistema de tratamiento de información.

Por último, en lo relativo a la faz subjetiva del delito, resulta necesario destacar que para efectos de poder consumarlo, se requiere que el sujeto activo actúe exclusivamente de forma dolosa, en otras palabras, si el sujeto activo no tiene la intención de usar, conocer o apoderarse que lo motive a llevar a cabo alguno de los tres actos antes descritos, entonces éste no podrá ser sancionado por la presente norma.

Continuando con el análisis del espionaje informático el artículo 4, en cuanto al sujeto activo, éste es indeterminado al igual que en el caso anterior, puesto que el tipo penal dispone "el que", situación que hace que el legislador no haga distinciones entre quienes pueden cometer este tipo de actos ilícitos, mientras que en lo relativo al sujeto

[38]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=interceptar
[39]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=interferir
[40]Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=acceder

pasivo, como se dijo anteriormente, este siempre será el mismo en esta materia, es decir, será indeterminado.

Analizando lo relativo a la faz objetiva del tipo penal, en este caso será de suma importancia destacar que se expresa a través de dos actos, los cuales son: revelar o difundir.

En lo relativo al concepto de "revelar", este significa Descubrir o manifestar lo ignorado o secreto[41]. En virtud de lo expuesto, podemos decir que es necesario que el sujeto activo descubra información secreta o en reserva de la víctima para luego, darla a conocer a terceros, es importante recalcar que dichos datos deben encontrarse contenidos en el soporte lógico de un sistema de tratamiento de información a la cual el sujeto activo haya podido tener acceso para luego proceder a actuar por esta vía.

En cuanto al término de "difundir", la Real Academia Española lo define como Propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc.[42]En este sentido, entenderemos con este concepto que el acto por el cual el sujeto activo cometerá el delito será mediante el traspaso o la publicación de los datos que obtenga de un sistema de tratamiento de información, todo esto por supuesto, que no hay consentimiento por parte de la víctima del delito.

Como bien señala el artículo en análisis "Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado", esto implica una situación agravante de la pena si quien actúe de las dos formas señaladas con anterioridad está a cargo del cuidado del sistema de tratamiento de información, un claro ejemplo de ello sería un funcionario de una empresa a cargo de computadoras que contienen información reservada o secreta de ésta, si dicha persona actúa bajo los dos supuestos antes señalados en lo relativo a los datos de la empresa contenidos en los computadores, a él se le aplicará dicha agravante.

---

[41] Real academia española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=revelar

[42] Real Academia Española, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013, URL: http://lema.rae.es/drae/?val=revelar

En cuanto a la faz subjetiva del tipo penal, al igual que en los anteriores, se requiere necesariamente del dolo por parte del sujeto activo para que éste pueda ser sancionado por la norma, ya que en su defecto, no podrá ser sancionado por ésta, en otras palabras, si el sujeto comete el acto ilícito con culpa, no se le podrá aplicar la sanción establecida en el tipo penal.

II. Análisis general de la legislación extranjera

A. Francia

En el Código Penal Francés en su Libro III, Título II, Capítulo III: De los atentados contra los sistemas de tratamiento automatizado de datos, se puede encontrar le tratamiento relativo a nuestro análisis, principalmente entre los artículos 323-1 a 323-7 y en el Artículo 441-1 sobre:

Falsificación y uso de documentos electrónicos falsificados.

i. Acceso fraudulento a un sistema de elaboración de datos.

> *Article 323-1: "Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.*
>
> *Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.*
>
> *Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende"*[43]

.

Como se puede apreciar la presente norma del cuerpo Francés señala que al acceder o permanecer de manera fraudulenta, en todo o en parte de un sistema de tratamiento automatizado de los datos se castiga con dos años de prisión y una multa de 30.000 €., y se de ello

[43]Code Pénal Français, www.legifrance.gouv.fr, entrada del 12 de marzo del año 2013, consultada el 12 de marzo del 2013,
URL:http://www.legifrance.gouv.fr/affichCode.do;jsessionid=22D4A6DF9BAA3E2DFAF08A26560E15CF.tpdjo02v_1?idSectionTA=LEGISCTA000006149839&cidTexte=LEGITEXT000006070719&dateTexte=20130312

Cuando resultó ya sea la eliminación o modificación de los datos contenidos en el sistema, o problemas de funcionamiento de este sistema, la pena es de tres años de prisión y una multa de € 45.000.

Cuando los delitos en los dos primeros párrafos se han cometido en contra de un sistema de tratamiento automatizado de datos personales aplicado por el Estado, la pena se elevará a cinco años de prisión y 75.000 €

Cabe señalar que en la presente norma para que el delito se encuentre consumado no requiere la destrucción, alteración o daño de los datos contenidos en el sistema de tratamiento de la información, ni el apoderamiento, uso o conocimiento de la información que éste contiene, más aun tampoco la revelación o difusión de los datos contenidos en él, así, la norma sanciona al sujeto con la mera introducción al sistema de tratamiento de la información aunque esta haya sido culposa u accidental.

ii. Sabotaje informático

> *Article 323-2. "Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.*
>
> *Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende"*[44].

Lo anterior señala que el hecho de obstaculizar o perturbar el funcionamiento de un sistema de tratamiento automatizado de datos se castiga con cinco años de prisión y una multa de € 75.000, y además, cuando el delito se haya cometido en contra de un sistema de tratamiento automatizado de datos personales aplicado por el Estado, la pena se elevará a siete años de prisión y una multa de 100.000 €.

El presente artículo consagra dos elementos de suma importancia, el primero y más evidente es la distinción entre el sabotaje informático y alteración de datos contenido en el sistema de tratamiento de la información, y por otro lado la consagración de una agravante cuando el sistema automatizado de datos personales es aplicado por el Estado, constituyendo esto una fuerte herramienta implementada por el legislador para la protección de los datos resguardados por entidades del Estado, ya que estas en su vital

[44] Ibid.

función cualquier tipo de alteración que sufran causaría consecuentemente daños gravísimos a las personas afectadas.

iii. Destrucción de datos.

> *Article 323-3. "Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.*
>
> *Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende"*[45].

.

Como se puede apreciar lo anterior señala que la introducción fraudulenta de datos en un sistema de tratamiento automatizado, o eliminar o modificar fraudulentamente los datos que contiene, será castigado con cinco años de prisión y una multa de € 75.000. Además, Cuando el delito se haya cometido en contra de un sistema de tratamiento automatizado de datos personales aplicado por el Estado, la pena se elevará a siete años de prisión y una multa de 100.000 €.

Al igual que el artículo 323-2 el legislador francés incorporó dos elementos, por un lado, el objeto del delito son los datos que contiene el sistema de tratamiento automatizado, ya sea su modificación o supresión contenidos en el mismo, y por el otro la agravante cuando estos datos son de carácter personal y aplicados por el Estado.

Así mismo en este sentido se incorpora el artículo 323-3-1, señalando que, el hecho, sin causa justificada, importar, poseer, ofrecer, vender o poner el equipo disponible, un instrumento, un programa de computadora o los datos proyectados o adaptados especialmente para cometer uno o más delitos bajo Artículos 323-1 a 323-3 será castigada con las penas respectivamente para la propia infracción o el delito más severamente castigados, como lo consagra expresamente la norma:

> *Article 323-3-1: "Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni*

[45] Ibid.

des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée"[46].

El legislador francés al incorporar este numeral al artículo 323-3, su objetivo fue tipificar aquellas conductas en las que el sujeto por el solo hecho y sin causa justificada, promueve o proporciona los instrumentos o elementos para la comisión de los delitos señalados anteriormente por éste, como son el acceso fraudulento a un sistema de elaboración de datos, sabotaje informático y destrucción de datos, artículos 323-1 a 323-3 respectivamente, las cuales serán castigadas con las penas respectivas para la propia infracción o el delito más severamente castigados, por ejemplo, si un individuo de nacionalidad francesa desarrolla un software o sistema con el cual puede alterar el correcto funcionamiento o acceder a datos de carácter privado en una base de datos de alguna entidad pública, y ofrece o proporciona los medios para la cometer un sabotaje informático masivo a dicho país por otro sujeto, aunque este no hubiese participado en el ataque sería sancionado por la presente norma.

iv. Asociaciones para cometer delitos informáticos.

Article 323-4. "La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée".[47]

De lo anterior se extrae que la participación en cualquier grupo o asociación formada establecido para la preparación, caracterizada por uno o varios hechos materiales, de uno o más de los delitos previstos en los artículos 323-1 a 323-3-1 será castigado con las penas prescrita para el mismo delito o la infracción más gravemente castigado, es decir, esta especial figura sanciona a la asociación de un grupo de sujetos los cuales efectúan alguno de los delitos contemplados anteriormente por el legislador, más conocidos en el medio informático y cibernético como "Bandas de Hackers o Piratas Cibernéticos"

[46] Ibid.
[47] Ibid.

v. Sobre las Personas

> *Article 323-5:"Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35"*[48]

Principalmente el presente artículo señala que las personas físicas culpables de las infracciones previstas en el presente capítulo incurrirán igualmente en las penas accesorias que van desde la prohibición por un periodo de cinco años de los derechos civiles y civiles de familia (323-5 N°1), de ocupar cargos públicos o para realizar la actividad profesional o social en cuyo ejercicio o con ocasión de la cual se cometió la infracción (323-5 N°2), de emitir cheques que no sean los que permitan la retirada de fondos por el librador o del librado aquellos que son certificados (323-5 N°6), hasta el comiso de la cosa que sirvió o fue destinado a cometer el delito o de la cosa que es producto (323-5 N°3), la clausura de las instituciones o más establecimientos que hayan sido utilizados para cometer el delito, por un periodo de 5 años; (323-5 N°4), la exclusión durante un período de cinco años, de la contratación pública; (323-5 N°5), la publicación o difusión de la decisión en las condiciones previstas en el artículo 131-35, del presente código.

Con ello queda de manifiesto que el legislador francés otorga herramientas fuertes y contundentes para sancionar las conductas ilícitas que atentan contra el sistema de tratamiento automatizado de la información, estableciendo además penas accesorias para el sujeto que vulnera el tipo penal.

[48] Ibid.

En cuanto a las personas jurídicas el legislador francés propuso lo siguiente:

> *Article 323-6: "Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.*
>
> *L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise"*[49]

Las personas jurídicas penalmente responsables, de conformidad con el artículo 121-2 de los delitos previstos en este capítulo se hacen responsables además de la multa, de acuerdo con los procedimientos establecidos en el artículo 131-38 , de las penas previstas en el artículo 131-39, además de la prohibición a que se refiere el apartado 2 º del artículo 131-39, se aplicará a la actividad en el curso de o en conexión con el ejercicio de que se cometió el delito.

Estableciendo así la responsabilidad de las personas jurídicas o morales por la vulneración a la presente norma.

Y para finalizar el presente capítulo, se establece el castigo en grado de tentativa el acceso fraudulento a un sistema de elaboración de datos, sabotaje informático y destrucción de datos, artículos 323-1 a 323-3 respectivamente, como así lo consagra la norma:

> *Article 323-7: "La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines"*[50]*.*

vi. Falsificación y uso de documentos electrónicos falsificados.

Por último el legislador francés decidió regular este tipo de delitos de una manera separada a la del Libro III, Título II, Capítulo III: De los atentados contra los sistemas de tratamiento automatizado de datos, y darles un tratamiento en el Libro IV, Título IV, Capítulo IV de la falsificación de las marcas de la autoridad, para abarcar con mayor amplitud dicho ilícito subsumiéndolo en el artículo 441-1 como así lo consagra la norma:

[49] Ibid.
[50] Ibid.

> *Article 441-1: "Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.*
>
> *Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende"*[51].

Se desprende de lo anterior que Constituye una falsedad toda alteración fraudulenta de la verdad, susceptible de causar un perjuicio y realizada por cualquier medio, en un escrito o en cualquier otro medio de expresión de pensamiento que tenga por objeto o que pueda tener como efecto constituir la prueba de un hecho con consecuencias jurídicas o de un derecho, la falsificación y uso de falsificación se castiga con tres años de prisión y una multa de € 45.000.

Cabe recalcar que la intención del legislador francés al dar tratamiento en esta locación del cuerpo normativo es abarcar tanto los documentos de carácter común como los documentos electrónicos propiamente tales, ya que su tratamiento de forma separada se suprimió por el presente artículo para una mayor simplicidad y efectividad al momento de aplicar la norma.

En síntesis, el legislador francés se ha preocupado de proteger la información en su conjunto y no sólo aquella que se encuentra en el soporte informático, es decir, que su preocupación se ha centrado en las conductas fraudulentas de acceso y uso ilícito de los sistemas de tratamiento automatizado de datos, absteniéndose de regular las manipulaciones informáticas en perjuicio patrimonial de terceros, núcleo principal del fraude informático, así centrándose en la falsedad informática, sólo cuando el dato alterado se encuentre sobre un soporte informático.

Por lo tanto, las defraudaciones patrimoniales por medios informáticos quedan sin

Regulación especial, ya que el legislador francés las subsume en la figura clásica de estafa del Art. 313-1 a 313-3 del Código Penal.

[51]Ibid.

B. España

Como se ha mencionado anteriormente con el análisis de la legislación francesa, el estudio de la normativa española relativa a los delitos informáticos se hará de forma explicativa e imparcial, evitando exponer opiniones o juicios de valor respecto de ésta en el presente capítulo, por lo que procederemos analizando de forma imparcial y objetiva la legislación vigente, para luego, en el capítulo siguiente, efectuar un análisis crítico y detallado respecto a las legislaciones mencionadas.

Para comenzar es importante tener presente que el legislador de España decidió tipificar los delitos informáticos en su Código Penal, medida adoptada también por Francia y otros países tales como Italia, Alemania, Austria y Canadá. Es importante dejar de manifiesto que la legislación relativa al tema en cuestión la podemos encontrar en una serie de normas a partir del artículo 263 en adelante del mismo cuerpo legal, de las cuales solo haremos un análisis profundizado sobre aquellas que tengan mayor relevancia en cuanto al tema en desarrollo.

i. Sabotaje informático

Podemos encontrar legislación relacionada con los delitos informáticos a partir del capítulo IX: de los daños, en donde se considera que el sabotaje informático, es decir todo acto delictivo que implique alteración, modificación, eliminación, utilización de archivos electrónicos o cualquier especie de software que se encuentre dentro de un sistema de tratamiento de información sea sancionado por algunas de las normas que se expondrán a continuación.

El artículo 263.1 del Código Penal español dispone:

> *"El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de 400 euros."*[52]

[52]Código Penal español, www.ub.edu, entrada del 17 de Enero de 2013, Consultada el 12 de Marzo de 2013, http://www.ub.edu/dpenal/CP_vigente_2013_01_17.pdf, p.134.

Dentro del concepto de propiedad ajena en este artículo se tiene en consideración el elemento material y lógico de un sistema de tratamiento de información, teniendo esto presente y para efectos de esta investigación, a partir de esta norma se comienzan a proteger ciertos bienes jurídicos relacionados con el tema en análisis.

Ya en el artículo 264.1 se tipifica una conducta que a nuestro juicio es un delito informático propiamente tal y dispone lo siguiente:

> *"El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, o programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años."*[53]

Por lo tanto, como el acto delictivo recae sobre un bien inmaterial o software, que se traduce en todos aquellos datos, programas o documentos electrónicos ajenos contenidos dentro de un sistema automatizado de tratamiento de información, es un delito informático propiamente tal y no un delito computacional (distinción que se hizo en el primer capítulo de la presente obra).

Sucede una situación similar con el artículo 264.2 que establece:

> *"El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años."*[54]

A diferencia del numeral anterior, aquí estamos en presencia de una figura la cual tipifica aquella conducta que obstaculiza o interrumpe de forma grave el funcionamiento de un sistema de tratamiento de información ajeno, el punto central de este numeral es tener en cuenta que dicho sistema está compuesto por un elemento físico o hardware y el elemento inmaterial o software, por lo tanto, los daños pueden recaer sobre cualquiera de esos dos elementos que componen el sistema, a diferencia del numeral anterior que solo contempla actos delictivos que atentan contra el software de un sistema de tratamiento de información. Por lo tanto, a modo de ejemplo, si un sujeto con el empleo de un virus o cualquier software maligno mencionado en el capítulo anterior logra

[53]Ibid, p.135.
[54] Ibid, p.135.

interrumpir u obstaculizar el adecuado funcionamiento del sistema de tratamiento de la información y hace que éste se apague, se suspenda, o su hardware comience a presentar fallas y que producto de ello se dañen, deterioren, alteren, supriman o se hagan inaccesibles los datos contenidos en dicho sistema será sancionado con la presente norma y es importante tener en cuenta que este numeral establece una agravante en relación al numeral previo.

Lo mismo sucedería si por otro medio que no implique el uso de algún software malicioso se logre causar los daños antes descritos, tanto al hardware como al software del sistema de tratamiento de información.

Ahora bien, si analizamos la norma desde una perspectiva más profunda, al señalar que "de manera grave" se causen los daños antes descritos podríamos deducir que hay una serie de conceptos que el legislador español ha empleado que permiten determinar la gravedad de los perjuicios causados, entre ellos:

Suprimir, eliminar o borrar: con estos conceptos se alude a la destrucción total o parcial de uno o más softwares determinados, de tal forma que sea imposible la recuperación de la información perdida y por lo tanto, que sea imposible devolver al estado anterior la calidad del elemento lógico sobre el cual recayó todo el daño causado.

Deteriorar, alterar o dañar: el legislador español al emplear estos términos nos permite deducir que se está refiriendo al acto de suprimir, variar o modificar, parte de uno o más archivos electrónicos o softwares al interior de un sistema de tratamiento de información ajeno, en donde las consecuencias para dicho elemento son irreversibles y por lo tanto, es imposible que se pueda recuperar dicho software al estado anterior al momento de su afectación, quedando como consecuencia un funcionamiento anormal.

Por lo tanto, a modo de conclusión respecto de lo anterior, el legislador español considera que quien actúe cumpliendo lo que señala el tipo penal, actuando según los parámetros antes mencionados, lo hará de manera grave dependiendo de la condición económica de la víctima, la cuantía del daño, el valor del bien jurídico y el valor del objeto material del delito propiamente tal, los dos primeros factores se pueden desprender del artículo 263.1 del Código.

ii. El "hacking" o acceso sin autorización a un sistema lógico

En cuanto al hacking, desde una perspectiva amplia, es un concepto con el cual se hace referencia a la entrada indebida o no autorizada a sistemas de tratamiento de información ajenos, sin embargo, el legislador español ha considerado sancionar este tipo de conductas si se comete actuando sobre datos de una empresa que tengan la calidad de "secreto de empresa", o sobre aquella información que sea calificada como secretos y que sea parte de la intimidad de una persona. Comenzando nuestro análisis sobre el delito que recae sobre el secreto de empresa hay que tener en cuenta el artículo 278 del mismo cuerpo legal que establece:

> *"El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses."*[55]

Analizando el artículo antes citado, en primer lugar, es de suma importancia entender el concepto de "apoderarse" que significará para estos efectos como el acto de "tomar una cosa ajena como si fuera propia"[56]. Ahora bien, como la norma establece, quien por cualquier medio logre obtener un dato, documento o software que se encuentre dentro de un sistema de tratamiento de información que sea propiedad de una empresa, con el fin de descubrir un secreto, es decir, de revelar información que la empresa ha decidido mantener en reserva, debería ser sancionado con la pena que establece la norma.

Sumado a lo anterior, es necesario aclarar que la norma al ser extremadamente amplia en relación a los medios de comisión del delito se podría dar el caso de que con sus propios ojos un sujeto que solo observe la información contenida en el sistema lógico de una empresa a través de un monitor y con ello busque descubrir uno o más secretos de la empresa, estaría cumpliendo con el tipo penal señalado en el artículo anterior, sin necesidad de usar algún aparato electrónico u otro medio material para cometer el acto ilícito.

---

[55]Ibid., p. 142.
[56]Diccionario educativo juvenil Larousse, México, 2001, 2.a ed., p.32.

En el caso de que la información que tiene calidad de secreta sea difundida o cedida a terceros por la persona que la haya descubierto, se le aplicará la agravante del apartado 2 del mismo artículo, el cual dispone:

> *"Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos."*[57]

En el caso del apartado 3 del presente artículo, existe la posibilidad de que además de las penas que imponen los tipos penales mencionados, existe la posibilidad de aplicar penas por el apoderamiento o destrucción de los datos a los cuales se tuvo acceso de forma ilícita.

De los siguientes artículos se desprende una serie de variantes del tipo penal establecido en el artículo 278 del presente Código, entre ellas tenemos el artículo 279 que dispone:

> *"La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva, se castigará con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.*
>
> *Si el secreto se utilizara en provecho propio, las penas se impondrán en su mitad inferior."*[58]

En el fondo, la responsabilidad penal del sujeto activo del delito aumentará en los casos en que éste divulgase información secreta de la empresa teniendo la obligación legal o contractual de guardar reserva sobre aquella información que deba mantenerse en secreto.

Relacionado con lo expuesto en los párrafos anteriores, dentro del título X: delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, capítulo I: del descubrimiento y revelación de secretos, el artículo 197 dispone lo siguiente:

> *"El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de*

[57]Ibid, p. 142.
[58]Ibid, p.142.

comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses."[59]

Haciendo un análisis profundo sobre este artículo, básicamente cambia el sujeto pasivo del delito, ahora es la persona física (o persona natural como lo considera el legislador chileno) y no una empresa, además de ello la norma alude a otros elementos, tales como cartas y efectos personales que serían objetos materiales distintos a los señalados por el artículo 278 en adelante, por ende, si a modo de ejemplo una persona empleando un software maligno logra acceder sin autorización al correo electrónico de otra persona, con ese solo acto ya estaría cometiendo un delito informático, porque accede a un sistema lógico en donde pueden existir archivos electrónicos y una enorme variedad de softwares que contengan información personalísima de la víctima del delito, por lo tanto, se puede concluir que el bien jurídico protegido en esta norma es el derecho a la intimidad de la persona.

Luego, el apartado 2 del mismo artículo agrega:

"Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero."[60]

Por lo tanto, como vimos anteriormente, el acto de apoderarse, utilizar, suprimir, eliminar o borrar, Deteriorar, alterar o dañar cualquier tipo de dato o información que en este caso sea de carácter personal de la víctima del delito y que se encuentre dentro de un sistema de tratamiento de información se sancionará de la misma forma que el apartado anterior.

El apartado 3 del presente artículo señala lo siguiente:

"El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo. Atendidas las

[59]Ibid, p.113.
[60]Ibid, p.113.

reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33."[61]

En este apartado se sanciona el hacking propiamente tal, puesto que se centra en el acceso sin autorización a un sistema de tratamiento de información en donde se traspasa todo el sistema de seguridad contenido en el sistema para así lograr tener acceso a todos los archivos o software que se encuentren dentro de dicho sistema.

Lo interesante de este apartado es que también se le atribuye responsabilidad penal a una personalidad jurídica que cometa el delito y sanciones para ésta.

Como agravante de lo anterior, el apartado 4 dispone:

"Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior."[62]

Por lo tanto, en síntesis, el hecho de difundir la información por parte de la persona que obtuvo los datos, imágenes, grabaciones o alguna otra especie de efectos personales por medios ilícitos agrava la pena, como también se sanciona de una forma atenuada a aquellos que sin haber intervenido en la comisión del delito, divulguen a terceros toda aquella información perteneciente a la víctima que tenga la calidad de ser personal y que forme parte de su intimidad.

Al igual que en el hacking aplicado en el secreto de empresa, el apartado 5 señala:

"Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior."[63]

Consideramos necesario señalar que el apartado 5 del artículo antes citado señala que existe un agravamiento de la pena contra quienes siendo responsables o encargados del cuidado de la información que tiene la calidad de ser privada y personal de la víctima del

[61]Ibid, p.113.
[62]Ibid, p.113.
[63]Ibid, p. 113.

delito, como también establece otro agravamiento si se difunden, ceden o revelen a terceros los datos a terceros, situación contemplada también en el artículo 279.

El apartado 7 del mismo artículo señala:

> *"Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años."*[64]

En el fondo, la normativa analizada demuestra que el legislador español manifiesta un especial interés en dar protección al derecho a la intimidad y a la propiedad privada, incluyendo expresamente en las normas a los aparatos informáticos y elementos lógicos contenidos en ellos como elementos que deben ser protegidos por el ordenamiento jurídico.

iii. Protección a los softwares

El Código Penal español en su capítulo XI, titulado "De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores", en su sección primera, de los delitos relativos a la propiedad intelectual, señala en el artículo 270 en su apartado 1 lo siguiente:

> *"Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.*
>
> *No obstante, en los casos de distribución al por menor, atendidas las características del culpable y la reducida cuantía del beneficio económico, siempre que no concurra ninguna de las circunstancias del artículo siguiente, el Juez podrá imponer la pena de multa de tres a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días. En los mismos supuestos, cuando el beneficio no exceda de 400 euros, se castigará el hecho como falta del artículo 623.5."*[65]

Como se puede apreciar, hay que tener en cuenta en primer lugar que existen dos requisitos para poder cumplir con el presente tipo penal, los cuales son el ánimo de lucro

[64] Ibid, p.114.
[65] Ibid, p.138.

y el perjuicio ocasionado a un tercero, comenzando con el primer requisito, éste es un elemento subjetivo del tipo penal, puesto que si el sujeto en el transcurso de la comisión del acto o serie de actos ilícitos tiene la intencionalidad de obtener ganancias económicas, se presume que actúa de forma dolosa y es importante también tener en cuenta, que el segundo requisito es de suma importancia, puesto que en el evento de que un sujeto de forma dolosa reproduzca, plagie, distribuya o comunique de forma pública total o parcialmente una obra de cualquier naturaleza contenida en un sistema de tratamiento de información sin la autorización de los titulares correspondientes, pero si ese actuar no causa perjuicios a terceros, entonces, el sujeto activo de dicho acto o serie de actos no estaría cumpliendo con el tipo penal expuesto en el presente apartado, y por ende, no podría ser sancionado por la presente norma.

En cuanto al segundo inciso del apartado en análisis, también se considera delictivo el acto de distribuir los bienes señalados en el inciso anterior al por menor, pero con una penalidad atenuada teniendo en consideración la cuantía reducida del beneficio económico que se obtiene por cometer el acto ilícito.

Relacionado con lo anterior, el apartado 2 del mismo artículo dispone lo siguiente:

> *"Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien intencionadamente exporte o almacene ejemplares de las obras, producciones o ejecuciones a que se refiere el apartado anterior sin la referida autorización. Igualmente incurrirán en la misma pena los que importen intencionadamente estos productos sin dicha autorización, tanto si éstos tienen un origen lícito como ilícito en su país de procedencia; no obstante, la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando aquéllos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento."*[66]

El hecho de que el sujeto activo exporte, importe o almacene sin autorización de los autores o dueños de dichos ejemplares también se considera un actuar doloso y en el caso de las importaciones, independiente de si dichos ejemplares tienen un origen lícito o ilícito en el país de procedencia, si éstas no cuentan con la autorización de quien corresponda se considerará para estos efectos como un acto ilícito penado por el presente tipo penal, sin embargo, esta norma no operará en los casos de que el ejemplar

[66]Ibid, p.138.

haya sido adquirido del propio titular de derechos sobre dicho ejemplar en algún estado perteneciente a la unión Europea.

El apartado 3 establece:

> *"Será castigado también con la misma pena quien fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo."*[67]

Para efectos del desarrollo de la presente obra, enfocando este apartado dentro de los delitos informáticos, el sujeto activo en este apartado es quien crea, importa o pone en circulación todo tipo de medio que tenga como finalidad aportar en la inutilización de cualquier mecanismo o software de defensa de todos los ejemplares mencionados en el apartado 1 del presente artículo (podría ser un software maligno o algún aparato electrónico que logre vulnerar la defensa del sistema lógico que contiene los ejemplares mencionados con anterioridad).

iv. Pornografía infantil

El Código Penal español, en el Capítulo V titulado "De los delitos relativos a la prostitución y la corrupción de menores" En materia de pornografía infantil, el apartado 1 del artículo 189 establece lo siguiente:

> *"1. Será castigado con la pena de prisión de uno a cinco años:*
>
> *a) El que captare o utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.*
>
> *b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido".*[68]

[67]Ibid, p.138.
[68]Ibid. p.109.

En primer lugar, analizando lo establecido en la letra a), es importante señalar lo siguiente: para que el acto ilícito se configure como un delito informático es necesario que el sujeto activo capte a los menores o incapaces como lo señala el numeral con un dispositivo electrónico que tenga la capacidad de captar y almacenar imágenes o videos, (como por ejemplo, un celular con cámara integrada, una cámara digital, o cualquier otro dispositivo con la característica particular de captar imágenes, videos o ambos), para luego almacenar esa información en un soporte lógico, el cual puede ser una página de internet en donde ésta podrá ser almacenada.

En cuanto a lo que dispone la letra b) del presente artículo, se sancionará también a quien produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición del material pornográfico obtenido por el sujeto activo, entonces, para que se configure el hecho ilícito como un delito informático es necesario que el sujeto que realice las conductas que concuerden con el tipo penal dispuesto en el presente párrafo lleve a cabo dichos actos a través de soportes lógicos, como por ejemplo, exhibiendo el material pornográfico en una página web.

Cabe destacar también lo que señala el apartado 2 del artículo 189, el cual dispone:

> *"2. El que para su propio uso posea material pornográfico en cuya elaboración se hubieran utilizado menores de edad o incapaces, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años."*[69]

En este caso, para que se logre configurar el tipo penal como un delito informático, solo basta que el sujeto activo del delito conserve o tenga bajo su poder un respaldo del material antes señalado en un sistema de tratamiento de información, o al interior de algún dispositivo electrónico que tenga la capacidad de almacenar softwares o elementos lógicos (como podría serlo una memoria USB, un celular que tenga capacidad de almacenar archivos, un disco duro, etc.).

v. Delitos de Calumnia e injuria

Los artículos 205 y 206 del Código penal español aluden al tipo penal de la calumnia, el primero de ellos dispone:

[69]Ibid. p.109.

> *"Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad."*[70]

Para que el presente tipo penal se logre consumar como un delito informático, será necesario que el sujeto activo impute el delito a otra persona conociendo su falsedad por medio de algún soporte lógico, como pudiese serlo un correo electrónico, una página web, por medio de una publicación en una red social (como Facebook o Twitter, entre otras) o por medio de cualquier otro soporte lógico que cumpla con el objeto del tipo penal.

Asimismo, el artículo 206 del mismo cuerpo legal establece:

> *"Las calumnias serán castigadas con las penas de prisión de seis meses a dos años o multa de doce a 24 meses, si se propagaran con publicidad, y, en otro caso, con multa de seis a 12 meses."*[71]

Teniendo en cuenta lo expuesto en el párrafo anterior, si se llegase a consumar el delito de calumnia en la calidad de delito informático, será necesario distinguir si se llevó a cabo con o sin publicidad, puesto que la comisión con alguno de estos elementos determinará la pena aplicable al sujeto activo. En primer lugar, si el delito se cometió con publicidad (por medio de una red social o a través de una página web pública) se le aplicará una pena mayor al sujeto activo, esto se basa en el daño que se le causa a la víctima producto de la afectación a su honra o a su integridad psíquica y emocional. Ahora bien, si el delito se comete sin publicidad, por ejemplo, si el sujeto activo del delito crea un archivo de escritura en donde imputa a otra persona un delito conociendo su falsedad, pero no lo publica y en su defecto lo almacena dentro de algún dispositivo electrónico, se le aplicará una pena de menor grado, puesto que en este caso no se estaría afectando a la víctima, como sucedería en el caso de que la calumnia se hiciese pública.

En el capítulo III del Código Penal español titulado "Disposiciones generales", el artículo 211 establece:

> *"La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante."*[72]

[70] Ibid. p.115.
[71] Ibid, p.116.

En el fondo, al igual que la calumnia, para que la injuria se cometa en calidad de delito informático, será necesario que el sujeto activo publique sus dichos que atentan contra la dignidad u honra de la victima a través de algún soporte lógico que permita su publicidad, como pudiese serlo una publicación en alguna red social o alguna pagina web que tenga la característica de disponer de libre acceso al público a través de internet.

vi. Daños

El artículo 263 del Código Penal español dispone:

> *"El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de 400 euros."*[73]

La principal característica del tipo penal establecido en este artículo es su amplitud en lo relativo a daños, ya que al disponer que "El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código" se pueden ver aludidos por la norma una serie de conductas que puedan ajustarse al tipo penal, entre ellas se podría considerar la comisión de daños a un software o programa computacional perteneciente a la víctima, y en tal evento, como el hecho ilícito se materializaría sobre un elemento lógico e inmaterial, podríamos estar en presencia de un delito informático.

A modo de conclusión, es importante señalar que el legislador español, en primer lugar, considera que los delitos informáticos pueden atentar contra una multiplicidad de bienes jurídicos, tales como la propiedad, la privacidad, la pureza e idoneidad de los datos contenidos en un sistema de tratamiento de información, etc., y por esta razón, el legislador de España decidió subsumir los delitos informáticos dentro de la protección jurídica que se le da a otros bienes jurídicos, a través de otras ramas del derecho, posición que nosotros no compartimos por razones que se expondrán en el capítulo tercero. Además de ello es importante destacar que la legislación española, al igual que la

[72] Ibid, p.116.
[73] Ibid, p.134.

chilena le proporciona mucha importancia al ánimo del sujeto activo, situación que nosotros no compartimos por razones que expondremos más adelante.

C. Alemania

Para comenzar con el análisis a la legislación alemana cabe señalar cuáles son los principales delitos que regula su Código Penal y la importancia que estos poseen en el tratamiento punitivo de los delitos informáticos de dicho país, entre los más importantes se encuentra: el espionaje de datos (Sección 202.a), phishing (Sección 202b) Actos preparatorios de espionaje de datos y phishing (Sección 202c), estafa mediante ordenador o fraude informático (Sección 263.a), falsificación de datos probatorios (Sección 269), modificaciones complementarias del resto de las falsedades documentales (Sección 270, 271, 273, 274 y 348), engaño en el tráfico jurídico mediante sistemas de procesamiento de datos (Sección 270), modificación de datos (Sección 303.a) y sabotaje informático (Sección 303.b).

i. Espionaje de datos.

> *Abschnitt 202.a: "(1) Wer rechtswidrig Daten erhält für sich selbst oder anderen, die nicht für ihn bestimmt waren und wurden besonders gegen unbefugten Zugriff geschützt, wenn er umgangen hat den Schutz, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.*
>
> *(2) Im Sinne des Absatzes (1) oben genannten Daten werden nur diejenigen gespeichert oder übertragen werden elektronisch oder magnetisch oder sonst in einer W{{eise, die nicht sofort spürbar sein"*[74].

Principalmente el presente artículo señala "quien consiga sin autorización, para sí o para otro, datos que no estaban destinadas a él y que estén especialmente protegidos contra el acceso ilegítimo será castigado con pena privativa de la libertad de hasta tres años o con multa.

[74]StGB, en la versión promulgada el 13 de noviembre de 1998, Gaceta de Leyes Federales [Boletín Oficial Federal] I, p. 3322, modificado por el artículo 3 de la Ley de 2 de octubre de 2009, Boletín Oficial Federal I, p. 3214,www.gesetze-im-internet.de, entrada 2 de octubre del 2009, consultada el 13 de marzo del 2013, URL: http://translate.google.cl/translate?hl=es&sl=en&tl=de&u=http%3A%2F%2Fwww.gesetze-im-internet.de%2Fenglisch_stgb%2Fenglisch_stgb.html

Los Datos, a efectos del apartado I, serán sólo aquellos que sean almacenados, transmitido electrónica, magnéticamente, o de forma no inmediatamente accesible".

Del presente artículo se pueden inferir tres elementos fundamentales, el primero de ellos relativo al tipo de información que se maneja por el titular legítimo de ésta, ya que, los datos contenidos en el sistema de tratamiento de la información deben ser considerados por el usuario de carácter privado, el segundo elemento es la accesibilidad de los datos, ya que estos según el artículo en cuestión al señalar "especialmente protegidos contra el acceso ilegítimo" deben estar protegidos del acceso que pudiese tener un sujeto de forma común, quedando la punibilidad supeditada a lo anterior, y por último el sujeto activo de la acción debe poseer la condición de restricción a los datos que está accediendo, ya que si éste pudiese acceder a ellos de forma legítima y regular no se enmarcaría en el tipo penal.

ii. Phishing

> *Abschnitt 202.b: "Wer widerrechtlich fängt Daten (§ 202a (2)) nicht für ihn bestimmt sind, für sich selbst oder andere mit technischen Mitteln aus einem nicht-öffentlichen Datenverarbeitungsanlage oder aus der elektromagnetischen Ausstrahlung einer Datenverarbeitungsanlage, so ist die Strafe Freiheitsstrafe von nicht mehr als zwei Jahren oder Geldstrafe, wenn die Tat verursacht eine schwere Strafe unter den sonstigen Rückstellungen"*[75].

Del tenor del artículo se postula "Todo aquel que intercepta ilegalmente datos (sección 202a (2)) no previstos por él, por sí mismo o mediante otra técnica de una instalación de procesamiento de datos que no sea pública o de la emisión electromagnética de un centro de procesamiento de datos, será castigado con pena de prisión no superior a dos años o una multa, a menos que el delito incurra en una pena más grave en virtud de otras disposiciones.

El legislador alemán, al incorporar este tipo de delitos a su legislación criminal, lo que busca es reafirmar que el bien jurídico protegido "privacidad de la información" sea resguardado con mayor efectividad, ya que, como se señaló anteriormente, para que se configure el tipo penal es necesario que el tipo de información al que el sujeto activo accede sea de aquellas que se encuentren protegidas del acceso público, pero la diferencia

[75]Ibid.

con la sección 202.a apunta a aquellos datos que si bien son privados no se encuentran protegidos de forma especial por el sujeto quien lo posee legítimamente , como por ejemplo encriptados, contraseñas, códigos, etc. De esta manera el artículo en análisis tutela y resguarda las situaciones que se encuentran fuera de la Sección 202.a.

iii. Actos preparatorios de espionaje de datos y Phishing

> *Abschnitt 202.c: "(1) Wer bereitet die Begehung einer Straftat nach § 202a oder § 202b durch die Herstellung, den Erwerb für sich selbst oder anderen, Verkauf, die Lieferung in ein anderes, Verbreitung oder machen sonst zugänglich*
>
> *Ein. Passwörter oder andere Sicherheitscodes den Zugang zu Daten (202a (2)), oder*
>
> *2. Software zum Zwecke der Begehung einer solchen Straftat,*
>
> *wird mit Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe.*
>
> *(2) § 149 (2) und (3) gelten sinngemäß"*[76].

El presente enunciado señala "(1) El que prepara la comisión de un delito bajo la sección 202 o la sección 202.b por producir, adquirir para sí o para otro, la venta, el suministro a otro, difusión o cualquier otra forma accesible.

Primero contraseñas u otros códigos de seguridad que permiten el acceso a los datos (sección 202a (2)), o Segundo software para el propósito de la comisión de dicho delito, será castigado con pena de prisión no superior a un año o multa. (2) Sección 149 (2) y (3) se aplicarán mutatis mutandis".

Al realizar un primer examen del artículo en cuestión se pueden señalar dos cosas de suma importancia y que diferencian esta sección con la sección anterior, la primera y la más evidente es la sanción por el acto en grado de tentativa, ya que el acto de sustracción de información o difusión de esta no requiere que se encuentre consumado, basta para que el tipo penal este perfecto con la sola preparación de éste. En segundo lugar el objeto sobre el cual recae el delito, como lo señala la norma es "contraseñas u otros códigos de seguridad que permiten el acceso a los datos", por ello el objeto no es propiamente el dato o contenido de la información, que se encuentra en el sistema de tratamiento de la información, sino que el acceso a ella, es decir las contraseñas o

[76]Ibid.

códigos de acceso a la información, ya sea para beneficio propio o de terceros por cualquier medio, y como también lo señala la norma con la creación de un software para la comisión del presente tipo penal, marcando con esto la gran diferencia entre la sección 202.b.

iv. Estafa mediante ordenador o Fraude informático.

> *Abschnitt 263.a: "(1) Wer in der Absicht, den Erhalt für sich selbst oder eine dritte Person eine rechtswidrige materiellen Vorteil schädigt das Eigentum eines anderen durch Beeinflussung des Ergebnisses einer Datenverarbeitung Betrieb durch falsche Konfiguration eines Programms, fehlerhafte oder unvollständige Daten zu verwenden, unbefugte Nutzung Daten oder anderen unerlaubten Einfluss auf den Verlauf der Verarbeitung haftet Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.*
>
> *(2) § 263 (2) bis (7) gelten sinngemäß.*
>
> *(3) Wer bereitet eine Straftat nach Absatz (1) oben, indem er Computerprogramme, dessen Zweck darin, eine solche Tat zu begehen, oder beschafft sie für sich selbst oder anderen bietet sie zum Verkauf oder hält oder führt sie zu einem anderen gelten mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.*
>
> *(4) In den Fällen des Absatzes (3) über § 149 (2) und (3) gelten sinngemäß"*[77]

De la sección anterior se señala "(1) Quien, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro influyendo en el resultado de un proceso de elaboración de datos por medio de una errónea configuración del programa, por medio del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos o a través de intervención desautorizada en el proceso, será castigado con pena de privación de libertad de hasta cinco años o con multa.

(2) Sección 263 (2) a (7) se aplicarán mutatis mutandis.

(3) El que prepara un delito en virtud del inciso (1) anterior escribiendo programas informáticos con la finalidad de que está tratando de comprometerse a actuar, o adquiera para sí o para otro, ofrece a la venta, o la posesión o los entrega a otro será sancionado con prisión de hasta tres años o una multa.

[77]Ibid.

(4) En los casos previstos en el inciso (3) anterior sección 149 (2) y (3) se aplicarán mutatis mutandis.

En primer lugar para comenzar con el análisis de los elementos que dilucidarán la estructura del presente apartado, resulta necesario tener presente los elementos que componen la figura típica de la estafa, por ello se analizará conforme a dicho tipo penal.

El legislador alemán consagra la sanción a los actos preparatorios al señalar "El que prepara un delito en virtud del inciso (1)".

Se efectúa una reestructuración del artículo 263 del cuerpo legislativo que incorpora los elementos básicos de la estafa, el engaño a una persona, el error, el acto de disposición patrimonial lesivo, y los elementos subjetivos especialmente el de la intención de conseguir una ventaja patrimonial, incorporando a la sección 263.a solo los elementos subjetivos del tipo, ya que, tanto el engaño como el error y el acto de disposición patrimonial lesivo no son necesarios para que la conducta sea típica. En este sentido el legislador alemán evitó restringir la sección en estudio para poder sancionar de forma efectiva las defraudaciones que hubiese en un proceso de elaboración de datos cometidos mediante ordenador.

Establece además una agravante del tipo (privación de libertad de uno a 10 años) por la expresa remisión que efectúa al párrafo 263 (2) a (7).

v. Alteración de datos

> *Abschnitt 303.a: " (1) Wer rechtswidrig löscht, unterdrückt, unbrauchbar macht oder verändert Daten (§ 202ª (2)) haftet Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.*
>
> *(2) Der Versuch ist strafbar"*[78].

De lo anterior se puede apreciar "(1)Quien borre, elimine, inutilice o altere ilícitamente datos (202.a, apartado 2) será castigado con pena de privación de libertad de hasta dos años o con multa.

(2). La tentativa será punible".

[78]Ibid.

La disposición protege tanto al que almacena los datos, como a la persona afectada por el contenido de éstos, por ello y con relación a lo anterior, los datos que son protegidos son de aquellos que no son de inmediata percepción, además se tipifican cuatro acciones las cuales se señalan expresamente por el legislador que a continuación se expondrán:

En primer lugar, el borrado de datos, ya sea de forma completa o parcial, con lo cual el destruir el soporte lógico de un dispositivo de tratamiento de la información, borrado de los elementos necesarios para establecer una conexión o acceso a determinados sistemas, se enmarcaría en dicho tipo.

En segundo lugar, la inutilización de los datos, la cual se materializa por el solo hecho que el dato no cumpla su fin propio para el cual fue diseñado.

Tercero, la alteración, son perturbaciones de carácter funcional, relativas a la transformación de su valor informático, por ello los datos poseen un nuevo contenido producto de la alteración efectuada.

Por último y como consecuencia de lo señalado anteriormente se debe tener en consideración que todas las conductas identificadas producen el efecto del ocultamiento de los datos para la persona que posee el acceso legítimo a ellas, lo cual si bien no se aprecia de forma expresa en el tipo penal se sub entiende por todas la consecuencias que produce dichas acciones, con lo cual se hace imperioso señalar lo anterior para una mayor profundidad en el análisis.

vi. Sabotaje informático

> *Abschnitt 303.b: " (1) Wer stört Datenverarbeitungen, die von wesentlicher Bedeutung sind, um anderen durch 1. Begehung einer Straftat unter section303a (1) oder 2. Eingabe oder Übertragung von Daten (§ 202a (2)) mit der Absicht, einen Schaden zu verursachen, um eine andere, oder 3. zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert eine Datenverarbeitungsanlage oder einen Datenträger, wird mit Freiheitsstrafe bis zu drei Jahren oder eine Geldstrafe. (2) Wenn die Datenverarbeitungs-Operation ist von wesentlicher Bedeutung für ein anderes Geschäft, Unternehmen oder einer Behörde, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. (3) Der Versuch ist strafbar. (4) In besonders schweren Fällen des Absatzes (2) über die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren.Ein besonders schwerer Fall tritt in der Regel, wenn der Täter 1. verursacht große finanzielle Verluste, 2. wirkt auf kommerzieller Basis oder als Mitglied einer Bande, deren Zweck die fortgesetzten Begehung von Computersabotage oder 3. durch die Straftat gefährdet Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die nationale Sicherheit der Bundesrepublik Deutschland.*

(5) § 202c gelten sinngemäß für Handlungen zur Vorbereitung einer Straftat nach Absatz (1) erwähnten"[79].

De lo anterior se señala (1) El que interfiere con las operaciones de procesamiento de datos que son de importancia sustancial a otro por: 1. Comisión de un delito tipificado en sección303a (1), o 2. Entrar a la transmisión de datos (sección 202a (2)) con la intención de causar daños a otro; o 3. destruir, dañar, inutilizar, supresión o alteración de un sistema de procesamiento de datos o en un soporte de datos, será sancionado con prisión de hasta tres años o con multa.(2) Si la operación de procesamiento de datos es de importancia sustancial para el negocio de la empresa o de otra autoridad pública, la pena será de prisión de hasta cinco años o con multa.(3) La tentativa será castigada.(4) En los casos especialmente graves en virtud del inciso (2) por encima de la pena será de prisión de seis meses a diez años. Un caso especialmente grave ocurre normalmente si el delincuente1. Provoca importantes pérdidas financieras, 2. Actúa sobre una base comercial o como miembro de una banda cuyo objetivo es la comisión permanente de sabotaje informático, o 3. por la transgresión pone en riesgo el suministro de la población con bienes o servicios esenciales o la seguridad nacional de la República Federal de Alemania.(5) Sección 202c se aplicará mutatis mutandis a los actos preparatorios de un delito previsto en el apartado (1) anterior.

En primer lugar, así y en relación con lo anterior, el legislador alemán tipifica la vulneración de importancia sustancial por lo cual se excluyen del presente artículo cualquier vulneración de carácter irrelevante o de poca importancia para el sujeto que sufre la transgresión del bien jurídico protegido. Por ello se considera abarcar una serie de circunstancias, las cuales van desde la alteración de datos (sección 303a.), espionaje informático (sección 202a (2)) hasta la alteración y destrucción de la información contenida en un sistema de tratamiento de la información, eso abarca tanto los datos propios de esta como los datos los cuales se encuentran almacenados en ella.

En segundo lugar, cabe señalar que en su numeral (2) del presente artículo se aprecia una agravante a la conducta anteriormente descrita , en atención al sujeto pasivo sobre el cual recae la conducta típica, estas son tanto empresas de carácter privado como público,

[79] Ibid.

así el legislador alemán tomó en consideración la gravedad y las circunstancias perniciosas que se podrían derivar al vulnerar y alterar datos de entidades de carácter público en atención a su vital trascendencia en el buen desarrollo de las políticas de una nación, los mismo sucede con las entidades de carácter privado las cuales se pueden ver afectadas de manera gravísima por la alteración y vulneración de los datos sustanciales para ésta, por lo cual las políticas de planificación se pueden ver afectadas tanto a nivel financiero como administrativo. Por ello, la alteración recae en el negocio propio que ejerce la entidad y ésta además se debe ver alterado de forma sustancial, con lo cual se descarta de plano en el presente tipo cualquier alteración de carácter irrelevante, sin perjuicio de las demás tipos penales en los cuales se puede enmarcar dicha conducta.

En cuanto a la tentativa, queda de manifiesto que esta se sanciona, por lo cual el análisis no abarcara más allá de lo señalado.

En tercer lugar, se efectúa por parte del legislador alemán una sistematización del alcance que se debe tener presente cuando se señala aquellas conductas especialmente graves, aumentado la pena base contenida en el tipo , con lo cual se establece una agravante en la circunstancias que señalan las cuales van desde provocar importantes pérdidas financieras, actuar sobre una base comercial o como miembro de una banda cuyo objetivo es la comisión permanente de sabotaje informático, hasta la transgresión que pone en riesgo el suministro de la población con bienes o servicios esenciales o la seguridad nacional. Así todas las circunstancias que se manifiestan con anterioridad tienen una especial protección en atención al gravísimo daño que produciría la realización de estas conductas, cabe solo mencionar que en una situación en la cual un grupo de sujetos se dispone a vulnerar la base de datos de una compañía hidroeléctrica, provocando por ello una alteración grave en al suministro de electricidad a nivel nacional, se constituye en merecedora de una sanción de mayor fuerza, puesto que, en atención al bien jurídico que se menoscaba es de vital conservación. Por ende el legislador alemán tomo en consideración, la importancia en primer lugar en la vulneración patrimonial que se suscitaría en perjuicio del sujeto pasivo de la conducta, en segundo lugar la habitualidad del o los sujetos que se dispongan a realizar la acción típica, ya que se considera por el tipo penal tanto su realización individual o en comunión con otros sujetos, por último, constituyendo el elemento de mayor gravedad

se tiene presente la alteración grave en contra de la población por la vulneración a la seguridad nacional, elemento de vital protección por parte del Estado para los habitantes de la nación.

Para finalizar la mención a la sección 202c, hace presente que se sancionará las conductas tipificadas relativas a la alteración de datos (sección 303a.), espionaje informático (sección 202a (2)), alteración y destrucción de la información contenida en un sistema de tratamiento de la información, por los actos preparatorios de estas, aplicándose mutatis mutandis al tipo penal señalado.

A modo de breve conclusión se puede apreciar el gran desarrollo y protección que el legislador alemán efectuó en materia de delitos informáticos, proporcionando una amplia gama de herramientas para la punibilidad de las conductas antes señaladas, lo cual constituye un avance importante en la regulación de esta materia a nivel mundial.

Así y luego de haber analizado las legislaciones más relevantes en cuanto a la regulación de los delitos informáticos a nivel global pasando por Francia, España y Alemania, corresponderá comenzar el análisis de la legislación chilena, identificando tanto sus aspectos positivos como negativos, proporcionando además herramientas de solución para las problemáticas se presentaran a lo largo del análisis.

Capítulo III

I. Análisis comparativo y crítico de la legislación chilena con legislaciones extranjeras

En el presente capítulo se procederá a hacer un análisis profundo y detallado respecto a nuestra legislación en lo relativo a los delitos informáticos, para luego realizar una comparación de ésta con las legislaciones vistas y analizadas en el capítulo anterior, con la finalidad de determinar si nuestra legislación en esta materia es eficiente al momento de brindar protección a los bienes jurídicos que se busca proteger con la tipificación de conductas que atenten contra éstos.

La ley 19.223 relativa a los delitos informáticos regula de manera poco sistemática los delitos que se desean consagran en ésta, por ello y para una mayor comprensión, el presente análisis se efectuará a la luz de las dos figuras típicas que se encuentran de forma implícita en la presente ley, las cuales son por una parte sabotaje informático y por otra espionaje informático.

A. Sabotaje informático

Como se puede apreciar, luego del análisis efectuado anteriormente en el capítulo segundo de la presente obra, para poder efectuar el análisis comparativo del presente tipo penal es menester tener en consideración los parámetros utilizados para el análisis de la legislación chilena, por ello se comenzará por lo más elemental.

i. Sujeto activo

Se puede apreciar que en la legislación chilena no se determina que la ejecución del acto requiera de un sujeto calificado para la configuración del delito al utilizar la voz "el que" en la totalidad de sus apartados, y de una forma similar a lo que establece Francia en sus artículos 323-1 a 323-7 y en el Artículo 441-1 sobre falsificación y uso de documentos electrónicos falsificados, con la salvedad de que en dicha legislación no se hace mención de forma manifiesta a la expresión "el que". En cuanto a Alemania al utilizar expresiones tales como "quien", "todo aquel", "el que", en la redacción de sus secciones queda de manifiesto al igual que en Chile la falta de requerimiento de un sujeto calificado para la ejecución de la acción como lo señalan así sus apartados 202.a, 202.b, 202.c, 303.a, y 303.b, respectivamente. Por último en cuanto a España se configura el mismo tratamiento que la legislación chilena al utilizar la expresión "el que" en la gran mayoría de sus artículos relativos al delito informático dentro de los cuales, lo más relevantes son los establecidos en los artículos 264.1 a 264.4 y 278 respectivamente, sin embargo, y sin perjuicio de lo dicho anteriormente se puede apreciar que concurre un tratamiento especial por parte del legislador español , cuando la conducta es efectuada por una persona jurídica, a la cual le establecen una seria de sanciones que en su generalidad son de carácter pecuniario.

ii. Sujeto pasivo

Como se mencionó en el capítulo anterior , no se efectúa una distinción relativa a éste, con lo cual para el legislador chileno resulta de forma indistinta sobre quien recaiga la acción típica, por el contrario, dentro del tratamiento que se efectúa en las legislaciones extranjeras, en la totalidad de ellas se encuentra un tratamiento especializado atendiendo a determinadas materias y en cuanto a la especial condición que poseen algunos de ellos, así se puede apreciar el tratamiento que efectúa Alemania considerando en su sección 303.b relativa al sabotaje informático al señalar "Si la operación de procesamiento de datos es de importancia sustancial para el negocio, empresa o de otra autoridad pública", es decir se tanto las empresas privadas como

públicas son merecedoras de protección especial cuando se vulnera sus negocios mediante la alteración de datos de importancia sustancial, asimismo algo similar se suscita en Francia en su artículo 323-2, donde se protege de forma especial al estado cuando éste se ve vulnerado por la conducta sometida a este estudio. En cuanto a España, el sujeto pasivo de la acción al igual que en Chile es de carácter indeterminado no haciendo ninguna mención especial en cuanto a los delitos de sabotaje informático.

iii. Faz objetiva

Relativo a la legislación chilena nos remitiremos a lo desarrollado anteriormente en el capítulo anterior. En cuanto a las legislaciones extranjeras se puede apreciar que el tratamiento que se efectúa es de manera similar ya que la gran mayoría de los verbos rectores que se utilizar para la tipificación del hecho ilícito son característicos de este tipo de delitos, así, en Alemania se utiliza "interferir" con las operaciones de procesamiento de datos que son de importancia sustancial a otro, al igual que en Francia, la cual replica, en su apartado 323-2 al señalar el hecho de "obstaculizar" o "perturbar" el funcionamiento de un sistema de tratamiento automatizado de datos, asimismo España en su artículo 264.1 y 264.2, con un tratamiento de similares características.

iv. Faz subjetiva

Como se señaló anteriormente, en Chile que el legislador estableció de manera expresa el ánimo que el sujeto debía poseer en sus artículos 1,3 y 4 al señalar la expresión "maliciosamente" subsumiendo el tipo a dolo, sin embargo en Chile producto de lo anterior se suscita la discusión del alcance que debe tener el dolo, ya sea dolo directo, de consecuencias necesarias, o dolo eventual. En cuanto al primer postulado autores como Huerta y Líbano consideran que se requiere que se efectué la acción con dolo directo[80] , el cual como postula el profesor Cury se configura cuando el objetivo perseguido por el agente es la realización del hecho típico[81], teniendo presente además que se debería incorporar el dolo de consecuencias seguras, el cual se configura cuando el agente se

[80]HUERTA, M. Y LÍBANO, C." Delitos informáticos", Ed. ConosurLtda, Santiago, 1996, p.296.
[81]CURY URZÚA, ENRIQUE, "Derecho Penal, parte general*",* Óp. Cit., p.316.

representa el hecho típico como una consecuencia segura de su actuar y, no obstante ello, obra[82], por último en cuanto al dolo eventual éste se configura, cuando quien, habiéndose representado la producción del hecho típico como una consecuencia posible de su acción, acepta en su voluntad esa alternativa para el caso de que se realice[83], situación la cual para algunos no se debiese incorporar, e incluso se debiese solo considerar dolo directo en la ejecución del acto.

A nuestro juicio la utilización por parte del legislador del ánimo doloso como un elemento necesario constituye una limitación demasiado amplia al tipo penal en cuestión, generando una serie de problemas relacionados con la real aplicación de la norma en la actualidad, sin embargo esta situación será abordada en el siguiente título.

v. En cuanto a la participación

Los sujetos en la ejecución del hecho típico en la legislación nacional no efectúa ningún tipo de distinción en el tratamiento de sus artículos, situación que se replica en España, sin embargo esta situación es diametralmente diferente en las restantes legislaciones en estudio, ya que en Francia se puede aprecia en su artículo323-4 que regula expresamente la participación en cualquier grupo o asociación formada establecido para la preparación del hecho típico, más conocidos en el medio informático y cibernético como "Bandas de Hackers o Piratas Cibernéticos, situación en la cual Alemania posee una regulación similar, en su sección 303.b inciso 4 numeral 2 al señalar, "En los casos especialmente graves en virtud del inciso (2) por encima de la pena será de prisión de seis meses a diez años 2.Actúa sobre una base comercial o como miembro de una banda cuyo objetivo es la comisión permanente de sabotaje informático"[84], así y al igual que Francia, se sanciona expresamente la ejecución de este hecho típico por un conjunto de sujetos, constituyendo una agravante para la pena base.

vi. Momento de ejecución del delito

Relativo a este tema se puede mencionar que en la legislación chilena se requiere el grado de consumado para que éste sea punible, situación en la cual, en la legislación

[82]Ibid., p.316.
[83]Ibid. P.317.
[84]StGB, Óp. Cit.

extranjera no es así, ya que Francia en su artículo 323-4, le proporciona un tratamiento de carácter amplio al señalar expresamente "la participación en cualquier grupo o asociación formada establecido para la preparación", con lo cual se sancionaría los actos preparatorios los cuales son aquellos que no se ha dado principio de ejecución al acto[85], constituyendo lo anterior una herramienta de punibilidad fuerte y potente para la sanción de los delitos informáticos, además se consagra la sanción en grado de tentativa de forma expresa en su artículo 323-7. Por otra parte en Alemania la tratativa a este delito se efectúa de manera más restringida y de menor amplitud, al señalar de manera expresa que se sancionar éste tipo de ilícito de en grado de tentativa en su sección 303.b inciso 3 al señalar que "la tentativa será castigada", sin embargo cabe mencionar que en su sección 263.a, la cual consagra la estafa informática, en su inciso tercero amplia la sanción a este ilícito al consagrar el hecho de la punibilidad en los actos preparatorios. Por último en cuanto a España relativo al sabotaje informático, y al igual que en Chile se sanciona en grado de consumado al no señalar ninguna mención especial en sus artículos.

B. Espionaje informático

i. Sujeto activo

En lo relativo a la figura de espionaje informático, La legislación chilena la contempla en los artículos 2 y 4 de la ley 19.223, en cuanto al sujeto activo del delito resulta ser indeterminado, como ya se expuso anteriormente en lo relativo al sabotaje informático, ya que en la totalidad de la norma se alude al sujeto activo como "el que". Igual situación ocurre con la legislación española en donde se señala en la mayoría de sus disposiciones al sujeto activo del delito como "el que", ejemplos de ello se podrán encontrar en los artículos 278 y 197, salvo en el segundo párrafo del apartado 3 del artículo 197, donde se señala expresamente como sujeto activo del delito a la persona jurídica y en el apartado 5 del mismo artículo donde se alude a "las personas encargadas o responsables de los

[85]CURY URZÚA, ENRIQUE, "Derecho Penal, parte general", Óp. Cit., pp.560-561.

ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros" . En el caso del legislador alemán sucede lo mismo, el sujeto activo resulta ser indeterminado al señalar alusiones tales como "quien", "todo aquel", "el que" en los artículos 202a, 202b y 202c. En cuanto a las distintas normas relativas a la temática en análisis, ahora bien, en el caso de la legislación francesa se hacen ciertas distinciones, que ya fueron expuestas con anterioridad, como sucede en el caso de comisión del delito en asociaciones de sujetos activos, o en casos donde la norma considera como sujetos activos a "personas físicas" de forma exclusiva.

ii. Sujeto pasivo

En lo relativo al sujeto pasivo, en la legislación chilena, como se dijo anteriormente, éste siempre será indeterminado, ya que el legislador no hace distinción alguna en este sentido, ahora bien, en las demás legislaciones analizadas, en el caso del legislador español, éste considera como regla general en esta materia que el sujeto pasivo es indeterminado en delitos de esta naturaleza, ahora bien, en el artículo 278, considera exclusivamente como sujeto pasivo del delito a la empresa, entendiéndose en el contexto del secreto de empresa. En cuanto al legislador alemán, éste al igual que las demás legislaciones considera que el sujeto pasivo es indeterminado por regla general en materia de espionaje informático, sin embargo, tiene en cuenta ciertas situaciones en las cuales considera exclusivamente al sujeto pasivo, como sucede en el caso del sabotaje informático expuesto anteriormente. El legislador francés por su parte también considera la regla general del sujeto activo indeterminado en lo relativo a la comisión del delito, sin embargo, en el párrafo 3 del artículo 323-1, en lo relativo al acceso fraudulento a un sistema de elaboración de datos, se considera exclusivamente al Estado como sujeto pasivo del delito.

iii. Faz objetiva

En cuanto al espionaje informático, el legislador chileno ha considerado en sus normas las siguientes expresiones: "apoderarse, usar o conocer", "interceptar", "interferir" o "acceder" y también "revelar" o "difundir", situación similar ocurre con la legislación comparada analizada. En el caso del legislador español, este considera

expresiones tales como "apoderarse", "interceptar", "utilizar" y "acceder". Por su parte, la legislación alemana considera actos tales como "conseguir", "interceptar" y también considera los actos preparatorios para la comisión del delito informático en lo relativo al espionaje. Finalmente, en cuanto al legislador francés, éste estima en esta materia actos tales como: "acceder", "permanecer de forma fraudulenta en todo o en parte de un sistema de tratamiento de información", "promover o proporcionar los instrumentos o elementos para la comisión de los delitos" y también la "tentativa".

iv. Faz Subjetiva

En relativo a esta materia, consideramos que el legislador chileno en el artículo 2 de la ley 19.223 señala expresamente el "ánimo de apoderarse, usar o conocer indebidamente", mientras que en el artículo 4 dispone "el que maliciosamente revele o difunda". Teniendo en cuenta lo anterior, podemos concluir que el legislador nacional consideró que la intencionalidad del sujeto activo es fundamental o esencial en cuanto a la aplicación de la norma. En cuanto al legislador español, éste en la mayoría de las normas relativas al espionaje informático no considera el ánimo del sujeto activo como requisito de aplicación de la norma respectiva, sin embargo, tiene en cuenta la intencionalidad en casos específicos, como por ejemplo en el apartado 1 del artículo 197 expresa "el que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento", situación similar ocurre con el apartado 7 del mismo artículo, el cual señala "si los hechos se realizan con fines lucrativos", asimismo el apartado 1 del artículo 278 dispone "el que, para descubrir un secreto de empresa", es decir, se considera la intencionalidad del sujeto activo en los casos antes señalados para la aplicación de la norma correspondiente. En cuanto al legislador alemán, también considera que el ánimo como regla general no debiese tener lugar en cuanto a la aplicabilidad de la norma, sin embargo, regula ciertas situaciones aisladas en donde considera el ánimo del sujeto activo, ejemplo de ello lo encontramos en la sección 263.a, en materia de estafa mediante ordenador o fraude informático la cual expresa "quien con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita". El legislador francés por su parte, en lo relativo a espionaje informático no consideró en ningún aspecto el ánimo del sujeto activo en cuanto a la aplicabilidad de la norma.

v. En cuanto a la participación

En Chile como se dijo anteriormente no se hace distinción alguna, puesto que en todos sus artículos el legislador colocó la expresión "el que", por lo tanto, el sujeto activo siempre es indeterminado. En cuanto al legislador español y el alemán, como se analizó anteriormente, emplean los mismos criterios que el legislador chileno en la materia. Sin embargo el legislador francés, a diferencia de los anteriores considera la situación del actuar del sujeto activo en grupos o asociaciones, y expresa en el artículo 323-4 "la participación en cualquier grupo o asociación formada establecida para la preparación, caracterizada por uno o varios hechos materiales, de uno o más delitos previstos en los artículos 323-1 a 323-3-1, será castigado…". En síntesis, dicha participación se puede manifestar tanto en delitos de espionaje como también en delitos de sabotaje informático.

vi. Momento de ejecución del delito

El legislador nacional ha considerado en todos los artículos relativos a los delitos informáticos que es requisito esencial para la perfección del delito que los actos descritos en los respectivos tipos penales se encuentren en la calidad de consumados por el sujeto activo. Situación similar ocurre con el legislador español, ya que al igual que Chile, considera en la totalidad de las normas analizadas con anterioridad que los actos expuestos en ellas se encuentren en calidad de consumados. Por su parte, el legislador alemán en concordancia con las legislaciones anteriores considera como regla general en todas sus normas que el delito se encuentre consumado para que éste se haya perfeccionado, sin embargo, en la sección 202.c relativo a los actos preparatorios de espionaje de datos y phishing se expresa "el que prepara la comisión de un delito bajo la sección 202 o la sección 202.b por producir, adquirir para sí o para otro, la venta el suministro a otro, difusión o cualquier otra forma accesible…". En el fondo, solo bastaría para la perfección del delito que el sujeto activo cometa actos que lo encaminen

a la consumación de su objetivo. Otra situación de características similares la podemos encontrar en el párrafo 3 de la sección 263.a que regula materias relativas a la estafa mediante ordenador o fraude informático, en donde el legislador alemán emplea la expresión "el que prepara un delito". Por último, la legislación francesa, al igual que las legislaciones anteriores ha considerado como regla general que se requiere que el acto descrito en los tipos penales se encuentre en calidad de consumado para que se haya perfeccionado el delito, pero admite excepciones a dicha regla, entre ellas podemos destacar la del artículo 323-3-1 "el sujeto por el solo hecho y sin causa justificada, promueve o proporciona los instrumentos o elementos para la comisión de los delitos señalados anteriormente por éste, como son el acceso fraudulento a un sistema de elaboración de datos, sabotaje informático y destrucción de datos, artículos 323-1 a 323-3 respectivamente…". Como se puede apreciar, el legislador francés considera en la presente sección los actos preparatorios para la comisión del delito y los sanciona, al igual que el legislador alemán. Otro caso excepcional del legislador francés lo podemos encontrar en el artículo 323-7 relativo al castigo en grado de tentativa al acceso fraudulento a un sistema de elaboración de datos.

Para concluir el presente título cabe señalar en primer lugar que el tratamiento sistemático de las legislaciones extranjeras se efectúa de manera distinta a la chilena, ya que como se pudo apreciar en el análisis efectuado en el capítulo segundo de la presente obra, en todas ellas, se realiza un tratamiento diferenciando entre la punibilidad del hecho típico relativa a los atentados contra el sistema de tratamiento de información que impliquen destruir, dañar, inutilizar, suprimir o alteración de un sistema de procesamiento de datos, con aquellos que alteren el funcionamiento de dicho sistema, es decir la sistematización que efectúan las legislaciones tanto de Francia, Alemania y España apunta a establecer un hecho típico más amplio, el cual es la alteración del sistema de tratamiento de la información, continuando con la especificación de las causales por los cuales se podría suscitar la alteración al sistema, por ejemplo Alemania señala en su sección 303.b "El que interfiere con las operaciones de procesamiento de datos". Continuando con la numeración de las causales, situación similar ocurre con Francia en su artículo 323-2 como se mencionó anteriormente, dotando de mayor amplitud la protección al establecer el hecho punible a la "obstaculización" o

"perturbación". En cuanto a España en su artículo 264.2 se efectúa un tratamiento similar al de Francia al señalar "El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno", efectuándose una protección expresa a dicha circunstancia, sin embargo cabe señalar que en el tratamiento que efectuó el legislador español en el presente tipo penal – y en general en la especial protección que efectúa relativa a los delitos informáticos – supedita la punibilidad del hecho a la gravedad del daño cometido por el sujeto activo de la acción.

En segundo lugar, en las legislaciones extranjeras se tipifican una serie de circunstancias las cuales en la legislación chilena no se mencionan, como son por ejemplo en Francia el artículo 323-3-1, que sanciona el solo hecho y sin causa justificada, de promover o proporcionar los instrumentos o elementos para la comisión de los delitos de acceso fraudulento a un sistema de elaboración de datos, sabotaje informático y destrucción de datos, además de sus artículos 323-5 y 323-6, una serie de sanciones agravantes tanto para personas naturales como jurídicas que van desde la prohibición por un periodo de cinco años de los derechos civiles y de ocupar cargos públicos o para realizar la actividad profesional para las personas naturales hasta el cierre definitivo o por un período de cinco años o instituciones de uno o más establecimientos de la empresa utilizada para cometer el delito, además de ser responsable de una multa entre otras, asimismo en Alemania regula un especial figura de estafa mediante ordenador o Fraude informático en la sección 263.a, el cual se analizó anteriormente, además del Phishing consagrado en su sección 202.b. asimismo el tratamiento efectuado por España relativo al delito informático se debe tener presente que éste los considera con un carácter de multi-ofensivos al incluir dentro de su tratamiento un serie de bienes jurídicos que no son propiamente la vulneración o alteración del sistema automatizado de datos, es decir, el legislador español incorpora a los delitos computacionales, como delitos informáticos según la clasificación que expusimos en el capítulo primero de la presente obra, con lo cual eso explicaría el tratamiento que efectúa éste en sus apartados ya que se incluyen una serie de bienes jurídicos, que van desde la intimidad de las personas, secreto empresarial 278, propiedad intelectual, entre otros.

Por último cabe señalar que el tratamiento que se efectúa en Chile como se señaló desde un comienzo es en una ley especial, situación la cual es diametralmente diferente en las legislaciones extranjeras ya que, como quedó establecido, el tratamiento de éstas se efectúa en el cuerpo normativo respectivo – Código Penal de cada país- y no en una ley especial como ocurre en la legislación chilena.

II. Problemática actual de la ley 19.223 y soluciones propuestas para su efectiva aplicación

En la actualidad, en nuestra legislación relativa a los delitos informáticos, existe una multiplicidad de problemas en lo relativo a su aplicación: en primer lugar, es menester señalar que en la sistematización de los artículos de la presente ley, carecen de una claridad que permita comprender adecuadamente el sentido y alcance de la misma, ejemplo de ello lo podemos encontrar en el artículo 1, donde se incorporan, tanto los atentados contra un sistema de tratamiento de información, ya sea destruyéndolo o inutilizándolo con los atentados a las partes o componentes físicos de dicho sistema, situación la cual se enmarca dentro de los delitos de tipificación común, de daños en este caso, por lo tanto, se confunde el delito informático propiamente tal con los delitos de daños a la propiedad. Además, cabe señalar que en el mismo artículo, se efectúa un tratamiento de punibilidad contra el funcionamiento del sistema y contra la destrucción de este mismo, situación la cual, podemos apreciar que en las legislaciones extranjeras se efectúa un tratamiento separado.

Para solucionar la presente problemática, y como se puede apreciar en lo expuesto en el párrafo anterior, resulta necesario hacer una distinción clara y precisa del alcance y naturaleza que contendrá la norma punitiva, así se debiesen establecer delitos contra el sistema de tratamiento de información propiamente tal por una parte, y por la otra, atentados que afecten el funcionamiento de dicho sistema en articulados por separado, además, se deberían incorporar una variedad de hechos ilícitos, los cuales no contempla la legislación chilena, como son el phishing, hacking, fraude informático, asociación para cometer delitos informáticos, actos preparatorios destinados a la comisión de delitos de

esta naturaleza (lo cual incluye la tentativa), además de un tratamiento especializado en cuanto a las personas jurídicas y naturales como sujetos, tanto activos como pasivos del delito, incluyendo agravantes cuando se efectúan dichas conductas en circunstancias que el legislador considere graves o que afecten sustancialmente los sistemas de tratamiento de información y los datos contenidos en ellos, lo cual proporcionaría la claridad y solución a la problemática mencionada con anterioridad.

En segundo lugar, en cuanto al alcance de la norma se puede apreciar, que en los artículos 1, 3 y 4 de la ley 19.223, se subsume la conducta típica a un ánimo determinado, el cual es el dolo, por lo que se efectúa una limitación de tal magnitud que impide la punibilidad de la mayoría de los actos señalados en los tipos penales correspondientes a la informática, ya que el dolo en la legislación nacional es de difícil probanza. Sin embargo, en la legislación comparada, no se señala ánimo especial alguno para la comisión del hecho típico como regla general, facilitando de este modo la aplicabilidad de la norma relativa a los delitos informáticos, postura a la cual nos adherimos en la presente obra como modo de solución a dicha problemática. Reforzando la presente idea, y a modo de ejemplo, se puede apreciar en el legislador francés, al señalar en su artículo 323-1, el cual establece que el acto será punible por el solo hecho de acceder o permanecer de manera fraudulenta en el sistema de tratamiento de información, lo mismo ocurre con el legislador alemán al señalar "Todo aquel que intercepta ilegalmente datos" en su sección 202.b. Por ello, y solo en casos excepcionales se efectúa alguna mención especial relativa al ánimo del sujeto activo y gravedad de la vulneración del bien jurídico, como se dispone en el artículo 303.b, numeral 2, al señalar que "el que interfiere con las operaciones de procesamiento de datos que son de importancia sustancial a otro, por: 2. Entrar a la transmisión de datos (sección 202a (2)) con la intención de causar daños a otro (espionaje informático)", lo cual constituiría una solución efectiva al alcance y ánimo de la norma jurídica, sin embargo, hay que tener en consideración que al efectuar un tratamiento legislativo de éstas características podría suscitar una aplicación exacerbada de la punibilidad de los hechos típicos relativos a los delitos informáticos, lo que podría traer consecuencias adversas en cuanto a su aplicación, debido a la gran cantidad de situaciones difíciles que se podrían originar por la propia naturaleza del delito informático, ya que éste quedaría supeditado a las

consideraciones de hecho que se originan en las circunstancias en las cuales se comete el delito, sin embargo, cabe señalar que en la actualidad, nuestra sociedad se encuentra en un proceso acelerado de incorporación de las nuevas tecnologías, en donde a diario se desarrollan diversas relaciones de una infinidad de índoles, tanto jurídicas, económicas, políticas, sociales, etc., lo cual, amerita de forma imperiosa una regulación de las presentes circunstancias.

Asimismo, y teniendo en cuenta lo expuesto anteriormente, sostenemos que en cuanto a los delitos de espionaje de datos contenidos en sistemas de tratamiento de información y todas sus respectivas sub clasificaciones, como también, en cuanto al acceso no autorizado o ilegítimo a dicho sistema expuesto en el primer capítulo de la presente obra, pensamos que sería una solución efectiva incorporarlos sin un ánimo especifico de dolo, sino que en su modalidad culposa a lo menos.

En tercer lugar, el legislador nacional se caracteriza por tratar esta materia de los delitos informáticos en una ley especial, mientras que la corriente mayoritaria en el tratamiento de este tipo de delitos la efectúa en sus Códigos Punitivos correspondientes, su justificación se encuentra, en primer lugar que por el hecho de adjuntar el tratamiento de dichos delitos en el Código punitivo proporciona un mayor entendimiento y alcance de la naturaleza misma del delito, ya que necesariamente se tendrá que marcar en algún título, sección o capítulo, lo cual ayudaría significativamente a solucionar dicha problemática, además, con ello se evitaría crear una confusión innecesaria en el tratamiento sistemático de la norma, ya que al poseer un tratamiento único en un solo cuerpo legal, disminuiría considerablemente la difusión de normas relativas al mismo tema en el ordenamiento jurídico correspondiente, teniendo presente el bien jurídico especial al cual hacemos alusión en los delitos informáticos, el cual es la pureza e idoneidad de la información, y que por lo demás no tiene regulación alguna en nuestro Código Penal.

Como consecuencia de lo anterior, se puede evidenciar un escaso tratamiento de la jurisprudencia en lo relativo a este tipo de materias, ya que la gran mayoría de ellos se subsume su punibilidad en otro tipo de delitos, como por ejemplo, los atentados contra la propiedad, la intimidad o privacidad, etc. A modo de ejemplo, se puede mencionar el

artículo que analiza la problemática de la aplicación de los delitos informáticos, en el caso de la empresa ATI Chile contra uno de sus empleados, el cual luego de ser despedido, lleva a cabo actos de alteración del sistema de procesamiento de datos de la empresa, accediendo ilegítimamente mediante hacking a su página de internet y alterando su contenido con mensajes ofensivos dirigidos a la empresa.[86]

[86] CLUNES, ALBERTO CONTRERAS, "Delitos informáticos: un importante precedente", Ius et Praxis v.9 n.1 Talca 2003, versión On-line ISSN 0718-0012, www.scielo.cl ,entrada desconocida, consultada 07 de Junio de 2013, URL: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122003000100023&lng=es&nrm=iso

Conclusión

A lo largo del desarrollo de la sociedad durante el los últimos cuarenta años se han podido apreciar los cambios vertiginosos que ésta ha sufrido producto del avance exorbitante de las tecnologías de la información, partiendo en un comienzo con sistemas de computadoras con softwares de operaciones simples los cuales derivaron, luego de un proceso complejo en los actuales sistemas de tratamiento de información, los cuales poseen una gama de operación de una complejidad que abarca una serie de situaciones que son de una incalculable magnitud. Además cabe señalar que estos cambios van de la mano con las evoluciones de la sociedad que en la actualidad avanza a pasos agigantados en los diversos ámbitos, y en especial en cuanto a las nuevas tecnologías.

Así, durante el desarrollo de la presente obra se plantearon una seria de interrogantes, las cuales son de vital importancia para poder dilucidar la complejidad de la metería a la cual nos estamos refiriendo, al establecer que se entiende por un delito informático, cuales son el sus elementos y clasificaciones, la naturaleza misma de éste, asimismo en el mismo orden de ideas se puede apreciar un nuevo bien jurídico de especial protección el cual es la idoneidad y pureza de la información que se encuentra contenida en los sistemas de tratamiento de datos, el cual no posee en la actualidad protección alguna en nuestro Código Penal, por ello en el año 1993 se implementó una ley respectiva a esta metería la cual si bien fue innovadora a nivel latinoamericano en ese momento, hoy en día necesita un planteamiento nuevo ante el progreso las nuevas tecnologías de la información.

Por ello, el objetivo principal de la presente obra fue abordar dicha problemática, así rescatamos la intención del el legislador nacional al intentar incorporar éste nuevo bien jurídico en el espíritu de la presente ley, sin embargo y como quedó expresado de forma manifiesta, el tratamiento efectuado en ella, posee una seria de errores los cuales van desde la poca claridad en la implementación y sistematización de sus articulados, hasta la incorporación de elementos los cuales son de tipificación y punibilidad relativa a la legislación penal general, podemos señalar solo un caso y a modo de ejemplo como es la incorporación de los atentados al soporte físico (hardware), el cual contiene el sistema de

tratamiento de la información en su artículo número 1 , situación como señalamos es una apreciación incorrecta al ser éste un delito de daños contra la propiedad , asimismo, la incorporación de un ánimo específico en la totalidad de sus apartados, si bien en el tiempo que se dictó la norma en análisis poseía una justificación necesaria por el desarrollo de éstas, en la actualidad el tratamiento que se debe tener en este tipo de materias es de mayor amplitud, ya que al igual que las corrientes más influyente relativas a estos temas, no se subsume de forma general el tipo penal a un ánimo especifico como el dolo, sino que se efectúa una aplicación de carácter general estableciendo una modalidad en la cual por el solo hecho de incurrir en el hecho ilícito se sancionaría dicha conducta, es decir, se incorpora de forma tácita la modalidad culposa del hecho típico, estableciendo de manera específica las conductas las cuales se efectuaren de manera dolosa, y por lo general se incorporan como una agravante del mismo hecho típico, sin embargo cabe señalar que estamos en pleno conocimiento que postular, este tipo de aplicación en nuestra legislación incurriría en un riesgo de considerables consecuencias, pero que sin embargo es menester regular de forma adecuada nuestra realidad contemporánea, mediante un tratamiento más amplio y preciso en la determinación de las conductas las cuales se incorporarán en la tipificación de los hechos ilícitos, además cabe señalar que se hace necesario que en un futuro tratamiento legislativo se deben incorporar diferentes ilícitos los cuales merecen una especial protección por el bien jurídico que estos ostentan.

En el mismo orden de ideas y sin olvidar la incorporación de los elementos necesarios en los tipos penales relativos a la materia de participación y momento de ejecución de los hechos ilícitos, constituyen elementos de suma importancia en una futura incorporación, teniendo presente en las diversas modalidades que se pueden efectuar este tipos de conductas ilícitas y los diversos grados de participación que pueden suscitarse en los delitos informáticos, así a modo de ejemplo, se debiesen incorporar especiales tratamientos a las operaciones efectuadas por bandas o "piratas cibernéticos", una vez que estos hayan llevado a cabo las conductas tipificadas en la legislación. Lo mismo en cuanto al grado de ejecución que subsume la legislación nacional, ya que no se hace mención especial alguna a ellas, situación a la cual como se puede apreciar en las

legislaciones extranjeras no es así, ya que en la mayoría de los casos analizados anteriormente se sancionaban a lo menos en grado de tentativa.

Por ello esperamos que en un futuro no muy lejano, este tipo de materias logren enraizarse en nuestra legislación de forma clara y precisa, otorgando las herramientas necesarias para solucionar dichas problemáticas teniendo presente la acelerada evolución tecnológica y social en la cual nos encontramos.

Bibliografía

Consultada

- CANALES NETTLE, PATRICIA, LOISEAU, VIRGINIE, "Delitos informáticos en la legislación de España, Francia, Alemania e Italia", Santiago, Chile, Biblioteca del Congreso Nacional, Departamento de Estudios, Extensión y Publicaciones, 2004.
- DAVARA RODRÍGUEZ, MIGUEL ANGEL, "Manual de derecho informático", Navarra, Editorial Aranzadi, 2008, 10. ed. rev. y puesta al día, 528 p.
- ETCHEBERRY ORTHUSTÉGUY, ALFREDO, "Derecho penal", Santiago, Chile, Editorial Jurídica de Chile, 1998, 3a. ed., rev. y actualizada.
- GARRIDO MONTT, MARIO, "Derecho penal: parte especial", Santiago, Chile, Editorial Jurídica de Chile, 2007.
- GARRIDO MONTT, MARIO, "Derecho penal", Santiago, Chile, Editorial Jurídica de Chile, 2005, 2a. ed. Actualizada.
- HERRERA BRAVO, RODOLFO, "Derecho informático", Santiago, Chile, Ediciones Jurídicas La Ley, 1999, 465 p.
- JAKOBS, GÜNTHER, "Derecho penal: parte general; fundamentos y teoría de la imputación", Madrid, Editorial Marcial Pons, 1a. ed, 1995, 1113 p.
- LABATUT GLENA, GUSTAVO, "Derecho penal", Santiago, Chile, Editorial Jurídica de Chile, 2000, 9a. ed. Actualizada.
- MIR, SANTIAGO, "Derecho Penal: Parte general", Buenos Aires, Editorial Montevideo Bdef, 2009, 8a ed, 788 p.
- ROXIN, CLAUS, "Derecho Penal: Parte general", Madrid, Editorial Civitas, 1997.
- TÉLLEZ VALDÉS, JULIO, "Derecho informático", México, 1996, Editorial McGRAW-HILL, 2a. ed, 283 p.
- VELÁZQUEZ BAUTISTA, RAFAEL, "Protección jurídica de datos personales automatizados", Madrid, Editorial Colex, 1993, 272 p.

Utilizada

- BELTRAMONE GUILLERMO, HERRERA BRAVO RODOLFO, ZABALE EZEQUIEL, "NOCIONES BÁSICAS SOBRE LOS DELITOS INFORMÁTICOS", PONENCIA PREPARADA EN EL X CONGRESO LATINOAMERICANO Y II IBEROAMERICANO DE DERECHO PENAL Y CRIMINOLOGÍA, CELEBRADO EN LA UNIVERSIDAD DE CHILE, AGOSTO DE 1998.
- CLUNES, ALBERTO CONTRERAS, "Delitos informáticos: un importante precedente", Ius et Praxis v.9 n.1 Talca 2003, versión On-line ISSN 0718-0012, www.scielo.cl, entrada desconocida, consultada 07 de Junio de 2013, URL: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122003000100023&lng=es&nrm=iso
- CODE PÉNAL FRANÇAIS, www.legifrance.gouv.fr, entrada del 12 de marzo del año 2013, consultada el 12 de marzo del año 2013, URL: http://www.legifrance.gouv.fr/affichCode.do;jsessionid=22D4A6DF9BAA3E2DFAF08A26560E15CF.tpdjo02v_1?idSectionTA=LEGISCTA000006149839&cidTexte=LEGITEXT000006070719&dateTexte=20130312.
- CÓDIGO PENAL ESPAÑOL, www.ub.edu, entrada del 17 de Enero de 2013, Consultada el 12 de Marzo de 2013, http://www.ub.edu/dpenal/CP_vigente_2013_01_17.pdf.
- CURY URZÚA, ENRIQUE, "Derecho Penal: parte general", Santiago, Chile, Ediciones Universidad Católica de Chile, 2009, 9a. ed.
- Diccionario Educativo Juvenil Larousse, México, 2001, 2a ed.
- Glosario de términos relacionados con los delitos informáticos, www.delitosinformaticos.com, entrada del 2 de marzo del año 2009, consultada el 11 de noviembre del 2012, URL: http://www.delitosinformaticos.com/03/2009/delitos/glosario-de-terminos-relacionados-con-los-delitos-informaticos#.UKAepOTglDs.
- HERRERA BRAVO, RODOLFO, "Reflexiones sobre la delincuencia vinculada con la tecnología digital (basadas en la experiencia chilena)", URL: http://rodolfoherrera.galeon.com/refxdel.pdf.
- HUERTA M., MARCELO, "Delitos informáticos", Santiago, Chile, Editorial Jurídica ConoSur Ltda, 1998, 2a. ed.
- Huerta, M. y Líbano, C." Delitos informáticos", Ed. ConosurLtda, Santiago, 1996
- JIJENA LEIVA, RENATO, "La protección penal de la intimidad y el delito informático"., Santiago, Chile, Ed. Jurídica de Chile, 1992.

- JOYANES, AGUILAR LUIS, "Fundamentos de programación, algoritmos, estructura de datos y objetos", 3a. ed., editorial Mc Graw Hill
- LÓPEZ PINTO, R. "Delito informático: bien jurídico protegido en la ley N°19.223", Revista Ad Libitum N°3. Universidad Central de Chile. 1994.
- MAGLIONA MARKOVICTH, CLAUDIO PAUL, "Delincuencia y fraude informático, derecho comparado y ley No. 19.223", Santiago, Chile, Editorial Jurídica de Chile, 1999.
- REAL ACADEMIA ESPAÑOLA, www.rae.es, entrada del año 2010, consultada el 31 de Mayo de 2013.
- REPÚBLICA DE CHILE, Ley 19.223, Tipifica figuras penales relativas a la informática, Valparaíso, 7 de Junio de 1993.
- StGB, en la versión promulgada el 13 de noviembre de 1998, Gaceta de Leyes Federales [Boletín Oficial Federal] I, p. 3322, modificado por el artículo 3 de la Ley de 2 de octubre de 2009, Boletín Oficial Federal I, p. 3214, www.gesetze-im-internet.de, entrada 2 de octubre del 2009, consultada el 13 de marzo del 2013, URL: http://translate.google.cl/translate?hl=es&sl=en&tl=de&u=http%3A%2F%2Fwww.gesetze-im-internet.de%2Fenglisch_stgb%2Fenglisch_stgb.html
- VERA QUILODRÁN, ALEJANDRO A, "Delito e informática, La informática como fuente de delito", Santiago, Chile, Ediciones Jurídicas La Ley, 1996.