Delitos Informáticos y la Ley 19.223

Camila Paz Espinoza Correa
Estudiante de derecho
Universidad San Sebastián

Profesor patrocinante: Guillermo Silva

Resumen: En el presente trabajo se examinan los delitos informáticos en su materia conceptual y ejecutiva para luego adentrarse en un estudio que esbozo sobre el análisis de la Ley 19.223, que tipifica los delitos informáticos en Chile, donde se detallarán sus falencias y propondrán posibles soluciones o ideas para su modificación o derogación con miras a la creación de una nueva ley que realmente sirva en razón de la realidad virtual en la cual estamos inmersos hoy en día.

*****

I. Introducción

En la actualidad el uso de las redes sociales, sistemas, herramientas y plataformas computacionales en línea o electrónicos se ha hecho cada vez más recurrente, por el avance y difusión que ha tenido Internet desde la década de los 70 en su nacimiento hasta la fecha, ya completamente globalizado, accesible a todos y en todo lugar.

Hoy se vuelve indispensable esta herramienta para la difusión de conocimientos, comunicación, investigación o incluso para resguardar información relevante. Lo que conllevó su difusión masiva extremadamente rápida y, que implicó, en consecuencia, la infracción de derechos de las personas, tales como la infracción a la intimidad de nuestros datos personales, el nacimiento de la criminalidad informática y la infracción a la propiedad intelectual entre otros.

Dada la importancia y efectos que ha tenido el mundo electrónico o telemático, en el presente escrito expondré qué son los delitos informáticos, las formas de comisión y sus implicancias y, luego de ello, denotaré un análisis que efectué de la Ley 19.223 que tipifica los delitos informáticos en nuestro país, expondré acerca de los tipos de delitos que contempla, sus elementos y características, y posterior a ello, las respectivas críticas que formulo sobre la base del presente análisis y en razón de su materialización en casos concretos, de manera que terminaré planteando propuestas de mejoras o quizás, para la visión de algunos, derechamente su modificación.

II. Delitos informáticos o cibercrímenes

Antes de comenzar cualquier tipo de análisis de delitos telemáticos, debemos tener claro de qué estamos hablando, por ende, comenzaré por esbozar el concepto de delito informático de Jijena Leiva, que me parece que es el más completo e ilustrativo. Así entendemos por delito informático "aquella conducta típica, antijurídica, con intención dolosa o por negligencia, cometida contra el soporte lógico de un sistema informático o de tratamiento automatizado de información, generalmente mediante elementos computacionales." [1]

De este modo, el contenido del delito se puede configurar de la siguiente forma:

1) La conducta humana: este elemento esencial de un delito se expresa en el tipo delictivo a través del verbo rector, el cual puede desarrollarse como una actuación positiva (acción) o como inactividad (omisión).

   En el caso de los delitos informáticos, el sujeto activo o hechor del delito lo cometería cuando destruya, inutilice, use indebidamente, revele, difunda, modifique, altere, suprima, desestabilice, interfiera o aproveche la información contenida en un sistema de tratamiento automatizado de la misma o al mismo sistema en sí, sin el consentimiento de la persona natural o jurídica perjudicada.

2) El sujeto activo: nos referimos a la persona que ejecuta el delito. En general, no existen exigencias especiales en relación con el sujeto activo. De esta manera, puede ser hechor de esta conducta delictual cualquier persona, indiferente de su condición.

3) El sujeto pasivo: es la persona natural o jurídica que se ve afectada directamente con la conducta delictiva por ser el titular del bien jurídico que se pretende tutelar.

4) El objeto jurídico: es el bien jurídico que se pretende proteger.

5) En el caso de los delitos telemáticos, los bienes jurídicos comúnmente afectados son la intimidad o privacidad de datos personales, la honra, el patrimonio, la fe pública, etc.

6) El bien jurídico afectado dependerá de la naturaleza de la información interceptada, modificada, suprimida, etc., para constatar qué bien jurídico se transgredió.

[1] Jijena Leiva, Renato, *Delito, Pena y Proceso: Libro Homenaje a la memoria del profesor Tito Solari Peralta*. P. 148

7) Los autores C. Magliona y M. López postulan que los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir, *se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo"*[2].

8) Objeto "material": es referido a la cosa o persona sobre la cual recae la conducta delictiva, en el ámbito de delitos informáticos ya dejamos de hablar o comprender el objeto material en su sentido concreto o literal, aquí hablamos más bien de un objeto inmaterial, ya que el objeto es intangible, electrónico, es un soporte lógico de datos y programas. No son bienes u objetos apropiables físicamente, sino son tan solo impulsos electromagnéticos.

9) Medio de ejecución: este tipo delictual se ejecuta a través de un soporte lógico, informático, telemático o, si se quiere, sistema computacional.

Luego de definir y enmarcar claramente qué entendemos y comprendemos por delitos informáticos, expondré cómo se puede ejecutar o llevar a cabo este tipo de delitos, es decir, cuáles son sus modalidades o formas de cometerlo. De esta manera recogeré algunas formas de comisión de delito telemático de la clasificación de los mismos que realiza el señor Acurio del Pino[3], así, los delitos informáticos pueden ser:

1) De fraude: Son aquellos delitos cometidos para alterar o manipular tanto los datos como los programas de un sistema computacional, dentro de ellos se encuentra:

   a) *Data diddling*: Es la introducción de datos falsos o manipulación de datos del sistema lógico. El caso más común de este tipo es la de producir o manipular datos de entrada de un computador para que genere movimientos falsos, cambie, modifique o altere las transacciones de una empresa.

   b) *Trojan horses* o caballos de Troya: Es la modificación de programas existentes en el sistema computacional o insertar programas nuevos. Esta forma de manipulación de programas lo que hace es insertar instrucciones encubiertas en un programa telemático para que realice una función no autorizada al mismo tiempo que está funcionando normalmente el sistema de tratamiento automatizado de datos.

---

[2] Reyes Echandía, Alfonso, *La Tipicidad*, Universidad de Externado de Colombia, 1981.

[3] ACURIO DEL PINO, Santiago (2011): *Delitos informáticos: Generalidades* [consultado el 18 de agosto de 2013], Disponible en: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

c) *Rounching down*: En este modus operandi el interesado lo que hace es sacar o retirar datos o información reiteradamente en transacciones financieras de una cuenta determinada, de manera que el programa manda la instrucción de remitir dinero de esa cuenta a otras cuentas corrientes.

d) Falsificaciones informáticas: Procede cuando se alteran datos del sistema de tratamiento automatizado de información ya almacenados. Esta forma de comisión se da cuando las fotocopiadoras de alta resolución reproducen un documento original y luego lo alteran, creando documentos falsos sin tener que recurrir al original.

e) Manipulación de los datos de salida: Consiste en codificar información electrónica falsificada. Este modo suele referirse en la falsificación de instrucciones que se le hacen a los cajeros automáticos.

f) *Phishing*: Esta forma de delito tiene como objetivo robar la identidad al sujeto pasivo, y ello lo logra mediante la recopilación de datos como las contraseñas, información de sus cuentas y datos personales en general, todo mediante engaño. Este tipo de engaño se realiza generalmente a través de correos electrónicos o ventanas emergentes.

2) De sabotaje informático: es la acción de borrar, suprimir o modificar sin autorización los datos de un sistema lógico informático con la intención de obstaculizar o inutilizar el funcionamiento normal del mismo. Se puede cometer de las siguientes maneras:

a) *Logic bombs* o bombas lógicas: Es la programación de la destrucción o modificación de datos en un momento del futuro.

b) Gusanos: Es una infiltración en programas de procesamiento de datos con el objetivo de modificar o destruir aquellos datos legítimos. Se diferencia del virus porque éste no puede regenerarse.

c) Virus informáticos y *malware*: Los virus informáticos son elementos informáticos que se reproducen y se extienden dentro del sistema informático a que acceden.

Los *malware* usan la misma técnica y lo que hacen es desactivar los controles informáticos del computador y comienzan a propagar códigos maliciosos.

d) "Ciberterrorismo": Es el acto telemático que tiene por fin desestabilizar un país o aplicar presión a un gobierno determinado utilizando cualquier forma ya descrita de delito informático.

e) Ataques de denegación de servicio: Aquí lo que hacen es utilizar la mayor cantidad de recursos del sistema lógico para que nadie más pueda usar el sistema.

3) De espionaje informático: Es la obtención ilícita, dolosa y sin autorización de datos o información relevante y de programas o software computacionales.

   a) *Data leakage*: también llamada fuga de datos, es la divulgación no autorizada de los datos confidenciales de una empresa realizada por un *hacker*.

   b) Copia ilegal o hurto de programas o software: este es un delito sancionado en la Ley 17.336 de Propiedad Intelectual.

4) *Piggybacking and impersonation*: En esta forma de operar hay un concurso de delitos: el delito de suplantación de personas o nombres y el delito de espionaje informático. Aquí el delincuente utiliza la suplantación de personas para cometer otro delito informático. También es llamado parasitismo informático y suplantación de personalidad.

5) De acceso no autorizado a servicios informáticos:

   a) *Trap doors*: Consiste en introducir interrupciones en la lógica de los programas con el fin de ir comprobando, en un proceso complejo, las operaciones o resultados intermedios y producir salidas de control o guardar esta codificación. Se le llama también puertas falsas.

   b) *Superzapping*: Es un programa que tiene por fin la alteración, copia, utilización o eliminación de los archivos del computador, aunque éste esté protegido. Algunos lo conocen por el nombre de la llave maestra.

   c) *Wiretapping*: La interferencia de líneas o *wiretapping* es, como dice su nombre, la interferencia de las líneas telefónicas de transmisión de datos con el objeto de extraer la información que viaja por éstas, esto se puede hacer por medio de un radio, módem o impresora.

   d) Delitos de *hackers* en general: Son las personas que aprovechan la falta de rigor de las medidas de seguridad de las páginas web o plataformas digitales para obtener acceso a las mismas: Son aquellas personas que lo hacen desde un lugar externo al propio entorno telemático de la persona natural o jurídica afectada.

Cuando estos actos ilícitos tienen por fin destruir, eliminar o inutilizar el sistema de tratamiento automatizado de datos o la información contenida en sí, es cuando hablamos propiamente de delitos digitales de *cracking*.

En suma, en estricto rigor, los delitos informáticos no son más que formas nuevas de cometer fraude o estafa en un sentido amplio, es decir, dentro del marco de los delitos telemáticos, la diferencia conceptual de la noción tradicional de fraude que conocemos es que en este contexto los delitos informáticos no se restringen o limitan al ánimo de lucro con una connotación pecuniaria o contra el patrimonio de otro, sino que va más allá, hay variedad de bienes jurídicos que pueden ser afectados, no sólo el patrimonio de una persona, sino la privacidad de sus datos personales, la honra, etcétera. Sin duda que no es posible aplicar el delito de fraude tradicional "a secas", porque aquí no existe un engaño directo a una persona habiéndola inducido a error, lo que ocurre, en cambio, es que se engaña al sistema lógico de tratamiento de datos. Y no por eso vamos a entender que el objeto material de la criminalidad informática es el *hardware* o computador físico en sí, el objeto material evidentemente es el soporte lógico o sistema informático.

III. Delitos informáticos en Chile

Para comenzar el análisis de la Ley 19.223 debemos conocer qué describe esta ley. De esta manera prescribe:

> "***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."*

De esta manera, la Ley 19.223 tipifica en Chile los delitos informáticos contemplando dos tipos de delitos telemáticos, que son el sabotaje informático y

el espionaje informático. El primero contemplado en los artículos 1º y 3º de la presente ley y el segundo integrado en los artículos 2º y 4º de la misma.

Ya analizamos cada uno de esos tipos penales, pero no está de más centrarlos en una idea respectivamente para contemplar sus correspondientes críticas, así:

El sabotaje informático, contemplado en los artículos primero y tercero de la respectiva ley, comprende conductas típicas y antijurídicas en razón del objeto que se afecta o atenta con la acción típica y, puede ser un sistema de tratamiento de información, sus partes o componentes o los datos contenidos en el mismo sistema. Se puede cometer a través de su destrucción, inutilización, obstaculización, modificación o daño.

Si analizamos separadamente el tipo delictual del artículo primero con el del artículo tercero, nos daremos cuenta de lo siguiente: el artículo 1º de la Ley lo que hace es regular como objeto material del delito al *hardware* o soporte físico del sistema telemático, es decir, contempla como delito la destrucción o inutilización de un "sistema de tratamiento de información o sus partes o componentes…", aquí cabe todo tipo de sistema de tratamiento de información al no explicitarse que debe ser un sistema de tratamiento de información automatizado, en consecuencia, si yo lanzo un celular contra la pared y éste se destruye, tal conducta recaería en este tipo penal. Junto con ello, si uno coteja esta norma descrita tal cual está con la historia de la ley y sus discusiones en sala en las respectivas Cámaras, se declara que la supresión de la expresión "automatizado", que se tenía en cuenta en el proyecto original, de todos los tipos penales de la ley se hizo porque los señores parlamentarios pensaron que si ampliaban los tipos penales no dejarían afuera otros tipos penales que eventualmente pudiesen surgir gracias al avance veloz de la tecnología en nuestra era, empero dejaron tan amplia la tipificación de aquellos, que lo hicieron extensivo a todos los sistemas de tratamiento de información independiente de su naturaleza, por ende, podríamos pensar que se pueden circunscribir en ella los sistemas de tratamiento de información mecánicos, electrónicos, informáticos y manuales.

En el inciso segundo del mismo artículo primero habla de las consecuencias de la conducta descrita en el inciso primero, pero lo deja igualmente amplio, ya que se remite a lo descrito precedentemente, por lo tanto, tampoco hace diferenciación entre la naturaleza de los datos afectados, y realmente ¿son todos los datos importantes o relevantes para ser dignos de ser protegidos bajo una ley penal? ¿No habría que hacer esta distinción entre los datos que son relevantes para la persona afectada producto de la conducta descrita en el tipo?

Luego en el artículo tercero describe que será penado todo aquel que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de trata-

miento de información: de nuevo planteo ¿todo tipo de datos? ¿Es entonces la destrucción de cualquier soporte lógico lo relevante?

En los artículos 2º y 4º de la ley se estipula la penalización del espionaje informático, es decir, contempla delitos informáticos que deben ser con "apoderamiento indebido de la información contenida en un sistema de tratamiento de la misma" y, en el número 4º "el que maliciosamente revele o difunda los datos contenidos (…)"

El artículo segundo no distingue tampoco qué tipo de información es la que tiene que ser objeto de uso o conocimiento "indebido", por lo que se puede desprender que puede ser cualquier tipo de información: relevante o insignificante. Y junto con ello, ¿existe el conocimiento indebido? ¿No nos estaremos refiriendo en realidad simplemente a la intercepción y uso de los datos en cuestión, vale decir, intercepción y uso indebido de datos?

En el inciso primero del precepto cuarto se sanciona al que "maliciosamente revele o difunda los datos contenidos en un sistema (…)", también es un tipo penal muy amplio: no se especifica qué tipo de datos son objeto de revelación o difusión. Seguido a ello, ¿cuál es la diferencia entre revelar y difundir? ¿Implica que revelo la información a terceros solamente o que sólo la uso en beneficio propio? Luego en el inciso segundo se refiere al responsable del sistema, quien tendrá una pena mayor por incurrir en el tipo y, frente a ello: ¿qué entendemos por responsable del sistema? ¿Todos los que trabajan en un sistema se entienden responsables del mismo?

En fin, todas estas críticas planteadas no son antojadizas, nacen en razón de la poca reflexión sobre el tema y de la desinformación técnica del mismo, ya que si uno ahonda en la historia legislativa de la presente norma, más se da uno cuenta de que "el legislador" no entendió qué estaba legislando. Así se puede constatar en la historia legislativa con las siguientes afirmaciones:

1. *La idea matriz o fundamental del proyecto es proteger la calidad, pureza e idoneidad de la información en cuanto tal (…)*[4]: ¿Estamos hablando de un bien jurídico nuevo? ¿El bien jurídico protegido es la calidad, pureza e idoneidad de la información? ¿No será que son bienes jurídicos ya conocidos por todos, como la protección de los datos personales, intimidad, honor, propiedad, etc.?

2: Tres artículos de cuatro que conforman la ley exigen en su concurrencia que el hecho haya sido causado con malicia; así se exige un dolo específico,

[4] Historia legislativa, Página 8

una voluntad de ejecutar un hecho típico por parte del ciberdelincuente, teniendo éste el conocimiento de los elementos objetivos del tipo y de la ilicitud de la acción ejecutada. Lo que hacen estos preceptos entonces es doblar la carga de la prueba y exigirle a la víctima del delito que pruebe que el hechor obró maliciosamente. Esto provoca, en consecuencia, que los tipos penales contemplados resultarían inaplicables a la mayoría de las situaciones. Recordemos por lo demás que nuestra legislación penal subentiende el dolo eventual si nada describe el tipo. Y junto a ello, ¿tendríamos que pensar que los delitos informáticos no pueden ser causados por negligencia?

3. La Ley 19.223 no contempla la mayoría de las figuras informáticas delictivas que se cometen, no se tipifica entre ellas el *hacking* ni el fraude informático que como ya vimos contienen diversas formas de efectuarlos.

4. Además, según un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos[5], en promedio, el noventa por ciento de los delitos telemáticos son ejecutados por empleados de la propia empresa afectada, los denominados *Insiders*[6]. Y en este sentido, ¿tendrá que tener este sujeto activo una pena más alta por haber una agravante de responsabilidad como el abuso de confianza? No se contempla tampoco este tipo situaciones en la ley.

IV. Casos

Existen en Chile dos casos emblemáticos a la fecha en relación con el tema analizado, éstos son: causa Rol N° 3951-12 Vargas contra Valenzuela C. y Campos B. y la causa Rol N° 4245-08 Sky Chile CPA contra Merino M. Relataré brevemente sólo el primero de ellos, ya que es símbolo de la mala interpretación de la Ley 19.223 por parte de algunos abogados.

En el caso los hechos fueron los siguientes: "un oficial del grado de capitán le pidió a otro capitán que le facilitase un *pendrive* para obtener unos antecedentes. Obtenido el *pendrive,* fue hasta su oficina y sin autorización accedió al computador personal de la subteniente Vargas, que ocupaba un escritorio al lado del suyo, pero que en ese momento no estaba en el lugar. Una vez que ingresó, accedió a un archivo oculto y copió en el *pendrive* unas fotografías íntimas de la mencionada subteniente. Acto seguido se reunió con el oficial

[5] *Revista Internacional de Política Criminal* Nos. 43 y 44, Manual de las Naciones Unidas sobre Prevención y control de delitos informáticos, 1994.
[6] Los *insiders* se contraponen a los *outsiders,* que cometen el delito informático desde una actividad externa.

que le había prestado el *pendrive*, y junto a otros tres oficiales fueron hasta la oficina de otro capitán en donde vieron las fotografías en su computador. Posteriormente el dueño del *pendrive*, también capitán, en su domicilio particular accedió al mismo dispositivo en su computador y abrió un archivo oculto que tenía por nombre "porno" y vio otras fotografías de la subteniente en las cuales mantenía relaciones sexuales con su novio"[7]. Los capitanes, condenados por sentencia de dos de mayo de dos mil doce, dedujeron un recurso de casación en el fondo fundado en las causales 3ª y 7ª del artículo 546 del Código de Procedimiento Penal, es decir, por aplicación errónea de la ley penal, porque la sentencia califica como delito un hecho que la ley penal no considera como tal y por haberse violado las leyes reguladoras de la prueba, influyendo substancialmente en lo dispositivo de la sentencia. Es en este momento, con la defensa de los abogados, en donde nosotros vemos concretamente a qué nos referimos cuando se crea una ley que puede dar diversas interpretaciones erróneas y con justificación. Los abogados dieron, entre otros, los siguientes argumentos: (1) hay una causal de atipicidad en el hecho, ya que el sentido final de la ley es sancionar el espionaje y el sabotaje informático y revelar o difundir se ha entendido como la emisión de datos o de información por medios al alcance de un número importante e indeterminado de personas y en el caso se trata de unas fotos personales que fueron conocidas por un número reducido de personas, de manera que no se cumple el requisito de publicidad; (2) falta el objeto material del delito, es decir, los datos contenidos en un sistema de información, porque aquí hablamos de un *pendrive* y esto es sólo un dispositivo portátil; (3) no hay antijuridicidad material por falta de afectación del bien jurídico, ya que no se puso en peligro el bien jurídico que señala la ley, que es la calidad, pureza e idoneidad de la información, y (4) las conductas efectuadas por los defendidos no tenían por finalidad afectar el sistema de tratamiento de datos contenidos en el equipo computacional de la ofendida, por ende, no pueden ser encuadradas en el tipo invocado.

De esta manera, los ministros de la Segunda Sala de la Corte Suprema tuvieron que replantear el poco análisis que hizo el legislador plasmado en las actas de su historia y adquiridas por estos abogados, así, establecen en esta resolución ideas claras y correctas de qué era lo que se estaba protegiendo, de que el bien jurídico era la protección de los datos sensibles e íntimos y que la conducta ilícita no había sido sólo la afectación al sistema de tratamiento de información, sino a la difusión de la información obtenida ilícitamente. De forma tal que el presente recurso fue rechazado.

[7] Resolución emitida por la Segunda Sala de la Corte Suprema el 20/03/2013 rechazando el recurso de casación en el fondo deducido por los condenados S.C.B. y S.V.C. Considerando cuarto.

V. Conclusiones o palabras finales

En suma, a pesar de la legislación de delitos informáticos contemplada en dispersas leyes como son la Ley 19.927 de Pornografía infantil[8], la Ley 17.336 de Propiedad intelectual, Ley 20.009 en cuanto clonación de tarjetas de crédito y la presente ley cuestionada número 19.223, es indiscutible que estamos lejos de proteger a las víctimas de estos delitos por notorias inexactitudes e insolvencias de la legislación chilena en la materia.

Para superar estas deficiencias legislativas es necesario que nuestro legislador al momento de elaborar y discutir proyectos de ley se inmiscuya en el tema con mayor profundidad y se capacite en el mismo objeto de discusión con técnicos especialistas para no incurrir en faltas graves, como es el caso de proteger, por ejemplo, el propio *hardware*, que a mi juicio sería un "compucidio", cosa totalmente absurda. Empero lo anterior, en el presente caso hay que reconocer que el proyecto original ingresado por la comisión a discusión fue mucho más apropiado que la ley aprobada y las precisiones que hizo el Ejecutivo también fueron bastante acertadas, pero, a pesar de ello, los parlamentarios al ser ignorantes en el tema y no querer incurrir, a propósito, en lagunas legales dejando afuera casos, que según ellos, no contemplarían por el veloz avance que tiene la tecnología, lo modificaron a su criterio y como consecuencia fue precisamente lo que provocaron…una ley que se torna muchas veces letra muerta por no poder ser aplicable.

Junto con lo anterior, en leyes que impliquen materias más técnicas, se debiera también capacitar a los jueces y a los fiscales con el objeto de otorgarle el verdadero sentido la ley y lograr el propósito o fin esperado: hacer justicia y proteger los bienes jurídicos transgredidos.

Empero, al ya tener una ley sobre delitos informáticos, lo que nos queda es poner atención en la laguna legislativa que deja y, en conjunto, darles consideración a las Convenciones que se han acordado a nivel mundial, como el Convenio sobre la Ciberdelincuencia[9], que cuenta con el apoyo de diferentes organizaciones internacionales, donde Chile no se ha adherido aún.

Teniendo en cuenta lo ya expresado, podemos afirmar que la ley no fija límites claros en su tipificación delictual y, como consecuencia, se torna ambigua y muchas veces, como ya afirmé, hasta inaplicable por no poder lograr encuadrarla en las situaciones que se presentan en la realidad cuando se han vulnerado bienes

[8] Específicamente en cuanto a su regulación telemática: art. 374 ter.

[9] Convenio sobre la Ciberdelincuencia, realizado en Budapest, 23.XI.2001. Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF

jurídicos importante en las personas, desde organizaciones gubernamentales, empresas o persona natural.

Los cuestionamientos no dejan de surgir si seguimos cotejando la normativa con la realidad digital, ya que si vamos más allá del acto realizado y nos centramos en el autor del hecho, podemos visualizar que muchas de las veces son grupos delictivos organizados o bien es un autor intelectual distinto del que ejecuta el delito informático el que induce a otro sujeto para que lo cometa; y este caso, nuevamente, no se encontraría dentro de los tipos delictuales descritos en la norma vigente.

Además de todo lo mencionado en materia legislativa, también hay un déficit en la dedicación que se hace a nivel gubernamental del tema ya que sólo US $200 millones se destinan en Chile para la seguridad informática versus US $60 mil millones que gastan promedio en Norte América y Europa[10]. Ello porque tienen plena conciencia de que las consecuencias son millonarias y catastróficas por los daños que estos delitos pueden causar tanto a las personas naturales y jurídicas como al propio gobierno, conciencia que en Chile aún no se crea.

Creo necesario decir que en el presente estudio no me adentré en los castigos o penas que se le imponen al autor del delito informático, porque recaería en un círculo vicioso, al no estar bien delimitado el tipo, la pena tampoco lo está debido a que ésta tiene que estar relacionada directamente con la acción u omisión cometida, ya que varía su sanción en razón de la ejecución del hecho en sí, de las circunstancias que rodean el hecho, de los involucrados en el mismo, si hubo o no concurso de delincuentes, si hubo o no instigación, si existe o no relación entre el hechor y la persona natural o jurídica afectada, etcétera, toda pena contemplada debería depender de los aspectos que rodean al tipo y su gravedad debería incidir en los aspectos antes descritos.

Bibliografía

Ley 19.223. Tipifica figuras penales relativas a la informática, Diario Oficial 07 de junio de 1993

Historia de la Ley 19.223, Disponible en: http://www.leychile.cl/Consulta/portada_hl?tipo_norma=XX1&nro_ley=19223&anio=2013

ACURIO DEL PINO, Santiago (2011) [consultado el 18 de agosto de 2013], Disponible en: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[10] Datos entregados por McAfee y CSIS. Disponible en: http://www.emol.com/noticias/economia/2013/09/17/620336/chile-destina-solo-el-5-de-su-presupuesto-en-tecnologia-a-la-seguridad-informatica.html. Consultada el 20/09/13

Convenio sobre la Ciberdelincuencia [consultado el 20 de agosto de 2013], Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF

DE SOLA QUINTERO, RENÉ: "Delitos informáticos" [consultado el 18 de agosto de 2013], Disponible en: http://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf

HUERTA, Marcelo (1998): *Delitos Informáticos* (Santiago, Editorial Jurídica ConoSur Ltda.), p.: 314.

JIJENA LEIVA, Renato (2008): "Delitos informáticos, Internet y Derecho", *Delito, Pena y Proceso: Libro Homenaje a la memoria del profesor Tito Solari Peralta*, (Ed.), pp. 145 – 162.

JIJENA LEIVA, Renato (1992): *Chile: Protección Penal a la Intimidad y los Delitos Informáticos* (Editorial Jurídica de Chile), pp. 123.

MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena (1999): *Delincuencia y Fraude Informático* (Editorial Jurídica de Chile), p. 273.

MAGLIONA, Claudio *Derecho y Tecnologías de la Información,* artículo "Análisis de la Normativa sobre delincuencia informática en Chile", Fundación Fernando Fueyo Laneri Universidad Diego Portales, Santiago 2002, p. 384

Revista Internacional de Política Criminal N^{os} 43 y 44, Manual de las Naciones Unidas sobre Prevención y control de delitos informáticos, (1994).

10° Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, Viena, (10 a 17 de abril de 2000), [consultada el 18 de agosto de 2013]. Disponible en: www.uncjin.org/Documents/congr10/10s.pdf

11° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, (18 a 25 de abril de 2005), Bangkok, Tailandia [consultada el 18 de agosto de 2013] Disponible en: http://www.unis.unvienna.org/pdf/05-82113_S_6_pr_SFS.pdf y http://www.unis.unvienna.org/pdf/05-81509_S_1_SFS.pdf

12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, (12 a 19 de abril de 2010) [18/08/2013], Disponible en: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf

Página web del Poder Judicial de Chile: http://poderjudicial.cl/

Datos que entrega McAfee en conjunto con CSIS para determinar el porcentaje que destinan los gobiernos alrededor del mundo en torno a la seguridad informática, estadística mostrada en www.emol.com