ANÁLISIS DEL CONVENIO EUROPEO SOBRE EL CIBERCRIMEN

(Observaciones sobre el Convenio del Consejo de Europa, sobre el Cibercrimen, suscrito en Budapest, el 23 de noviembre de 2001)

Rodolfo Herrera Bravo
Master en Informática y Derecho, Universidad Complutense de Madrid

1. Generalidades sobre el Convenio Europeo sobre el Cibercrimen y el alcance de este estudio

Con la adopción del citado convenio del Consejo de Europa, en Budapest, el 23 de noviembre de 2001, culminó un largo proceso de estudio iniciado en 1997 en torno a la criminalidad desarrollada en el ciberespacio, estableciéndose un conjunto de reglas mínimas destinadas a frenar la amenaza creciente de las acciones delictivas cometidas principalmente a través de Internet, preocupación no sólo de los Estados signatarios, sino también del resto de los países que cada vez más se interconectan a las redes digitales, motivo por el cual esta convención no está limitada sólo a la firma de los Estados miembros de la Unión Europea, sino que busca la adhesión de otros para constituirse en una especie de resguardo mundial que armonice legislativamente los ilícitos penales por Internet.

De acuerdo a lo señalado en el Preámbulo del Convenio es posible distinguir un triple objetivo:
1) establecer la cooperación internacional para la prevención y persecución de los delitos cometidos mediante o a través de redes digitales y sistemas informáticos;
2) establecer facultades y técnicas comunes de investigación mejor adaptadas a las actuales tecnologías de información, permitiendo la armonización de normas procesales penales; y
3) lograr que los Estados signatarios desarrollen una legislación nacional coherente entre todos ellos, en la que se repriman las mismas conductas.

Bajo tal criterio, este análisis permitirá comparar el Convenio con la situación en que se encuentra el ordenamiento jurídico chileno, de importancia no sólo frente a una eventual adhesión a dicho Acuerdo Internacional o con ocasión de los efectos colaterales que pueden manifestarse a partir de las negociaciones bilaterales que se suscriban con algunos países signatarios de éste, sino también por la extraterritorialidad de las conductas que sanciona, las cuales pueden ser cometidas desde nuestro país y afectar con ello a personas situadas en diversos territorios o provenir desde el extranjero y alcanzar a víctimas que se encuentren en Chile.

En tal sentido, nuestra estudio comparativo se apoyará en el derecho actualmente vigente en Chile, recogido fundamentalmente en la ley Nº 19.223, que tipifica figuras penales relacionadas con la informática, no obstante que hoy existe un proceso de revisión de dicha normativa a través de algunos proyectos de ley en trámite, y que está decantándose hacia su reemplazo por un conjunto de tipos penales más completo que se incorporaría en el Código Penal.

2. Estructura del Convenio

El convenio se estructura en cuatro capítulos:

1) Definiciones, con los conceptos de "sistema informático", "dato informático", "proveedor de servicios" y "datos de tráfico";
2) Medidas a adoptar en los ordenamientos internos de los Estados parte;
3) Cooperación internacional; y
4) Disposiciones finales, sobre entrada en vigor del Convenio, la adhesión de Estados no signatarios, la posibilidad de que cada Estado especifique el territorio en que lo aplicará, la formulación de reservas, denuncias y otras normas similares.

En relación con las medidas a adoptar en el ámbito nacional, indicadas en el capítulo segundo, se subdividen en tres secciones:

1.- Medidas de derecho penal sustantivo, relativas a la tipificación armonizada de las conductas reprochables penalmente, como también ciertas cuestiones referidas a la forma de comisión del delito, la eventual responsabilidad de cómplices y encubridores y las sanciones que adopte cada Estado parte, que pueden ser no sólo privativas de libertad, en la medida en que sean efectivas, proporcionadas y disuasivas.

2.- Medidas de derecho procesal, con la particularidad de que no sólo son aplicables a la detección, investigación, persecución y condena de los autores de los delitos que tipifica el Convenio, sino también de cualquier otro delito cometido mediante un sistema informático o de cualquier ilícito cuyas pruebas se encuentren en soporte electrónico.

3.- Medidas sobre jurisdicción, referidas a que los Estados partes adoptarán las medidas necesarias para perseguir estos delitos cuando sean cometidos en su territorio, en buques o aeronaves con su bandera o que estén matriculados bajo sus leyes, y cuando sus nacionales cometan el delito en un territorio en donde sea punible la conducta cometida o en un territorio fuera del de los Estados signatarios. No

obstante, como se señaló precedentemente, los propios Estados signatarios pueden desarrollar el ámbito de aplicación.

En este informe, nos centraremos principalmente en los dos primeros puntos de este capítulo segundo, por ser los que nos permiten efectuar una comparación normativa más precisa.

3. Delitos tipificados en el Convenio Europeo sobre Cibercrimen

En cuanto a las conductas que sanciona penalmente, el Convenio distingue cuatro categorías:
i) delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos;
ii) delitos relacionados con la informática;
iii) delitos de contenido; y,
iv) delitos relativos a la vulneración de derechos de autor y conexos.

3.1. Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos

Dentro de esta categoría se tipifican 5 delitos:
a) el acceso ilegal a un sistema informático;
b) la intercepción ilegal;
c) la alteración de datos informáticos;
d) el sabotaje informático; y,
e) el abuso de dispositivos.

a) Acceso ilegal a un sistema informático

El delito de *hacking* consiste en acceder de manera indebida, sin autorización, a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso, no causando daños inmediatos y tangibles en la víctima.

En esta conducta la motivación no es causar daño a través de otros ilícitos, como el sabotaje o el espionaje informático, los cuales son obras de los denominados *crackers* más que de los *hackers*. Estos últimos persiguen satisfacciones personales, basadas en la burla de los sistemas de seguridad dispuestos, es decir, en logros exitosos frente a los retos intelectuales que se autoimponen.

Se trata de un delito de resultado que se consuma al momento de ser descifrados los códigos de acceso secretos, y no depende del conocimiento o ignorancia que pueda tener el sujeto pasivo sobre este hecho.

De acuerdo al Convenio, comete el delito de intrusismo o acceso ilegal aquél que sin autorización accede a un sistema informático y sin necesidad de otro motivo sancionable, como por ejemplo, el dañar o copiar la información.

El fundamento para que el mero acceso sea sancionable *per se*, sin necesidad de elementos adicionales, estriba en la vulneración al respecto de la vida privada consagrado como un derecho constitucional en la mayoría de los ordenamientos jurídicos y en los Convenios Internacionales sobre Derechos Humanos, como es el caso del Convenio Europeo de Derechos Humanos.

Por eso, pese a que existen opiniones que abogan por la atipicidad del *hacking*, basadas en el argumento de la no intencionalidad de dañar el sistema en que se ingresa, no siempre esa postura derivará en la absoluta impunidad de la conducta, porque no es admisible como tesis el que un *hacker* desconozca que su conducta no le está permitida por el sujeto pasivo, debido a la forma irregular en que ingresa. Además, los gastos en que incurren las empresas para adoptar mecanismos de seguridad de sus sistemas son de importancia, por lo que un *hacker* que intencionalmente rompe tales medidas, no está en un simple juego.

Más aún, si producto del acceso no autorizado se ingresa a información confidencial, violando de modo manifiesto derechos fundamentales, no será necesaria otra acción que esa, el ingreso, al igual que en la violación de correspondencia en que basta abrir la carta para cometer el delito, no se requerirá que su contenido sea leído, alterado, destruido o difundido, por ejemplo.

Por otra parte, su penalización autónoma tiene también un carácter preventivo, pues el acceso ilegal puede ser concebido como antecedente para la comisión de otros ilícitos más graves, en los cuales es necesario previamente acceder al sistema, como ocurre con figuras de sabotaje y fraude informáticos. En este caso, el mero acceso es conocido como *hacking* indirecto, y representa una especie de infracción básica que puede no ser sancionable en sí misma, ya que el legislador puede considerar sólo la pena aplicable al delito que motivó la conducta final —el daño o la defraudación, por ejemplo—, a menos que se le haya dado una sanción específica —produciéndose un concurso de delitos y aplicándose las penas de ambos— o constituyendo una circunstancia agravante.

En el caso del Convenio sobre Cibercrimen, y pese a que en varias legislaciones ya se ha penalizado el mero acceso ilegal, se tuvo en consideración que tanto en el ámbito material como en los elementos constitutivos del tipo, los diferentes ordenamientos

jurídicos varían considerablemente, por lo que se permite optar entre la tipificación del mero acceso ilegal (*hacking* directo) o el *hacking* indirecto o acceso ilegal cualificado por la concurrencia de elementos adicionales, por ejemplo, si se comete infringiendo las medidas de seguridad del sistema o respecto de computadores conectados en red. De este modo, los Estados signatarios podrían excluir de la sanción a los accesos no autorizados a computadores aislados sin utilizar otro sistema y tipificar sólo el acceso ilegal a sistemas informáticos en red, sea ésta pública o privada.

En el caso chileno, el *hacking* directo no está sancionado en la citada ley Nº 19.223, sino que está considerado el acceso como elemento del tipo del delito de sabotaje y de espionaje informáticos. No obstante, en los proyectos de ley se pretende incorporar como figura penal independiente.

b) Intercepción ilegal

Esta figura penal ha sido establecida para garantizar el respeto a la vida privada y al secreto de las comunicaciones, derechos protegidos en el mencionado Convenio Europeo de Derechos Humanos.

Lo que sanciona el Convenio es la interferencia ilegal, realizada por medios técnicos, en las transmisiones no públicas de datos informáticos, entendiendo el carácter no público según el modo de transmisión y no el contenido del dato transmitido.

Con este delito se identifica la intercepción de datos o mensajes transmitidos a través de redes informáticas con la vulneración de la inviolabilidad de las comunicaciones realizada mediante escuchas o grabación de conversaciones telefónicas, extendiendo la protección penal a las comunicaciones electrónicas.

La motivación para sustraer información confidencial o divulgarla sin autorización cuando los datos son reservados, puede o no ser el lucro, pero por lo general, son las grandes sumas de dinero que están dispuestos a pagar ciertas personas por obtener determinadas informaciones las que mueven a estos delincuentes.

No hay que confundir el espionaje informático, cometido por personas no autorizadas para acceder a la información que sustraen, con el delito de divulgación de secretos, que generalmente es cometido por el operador al cual se le ha previsto el acceso a ciertos datos, no de conocimiento público, y pese a ello, los entrega a otras empresas a cambio de un precio. Es el caso del operador que vende la base de datos de los clientes de una tienda comercial a la competencia, por ejemplo.

Para hacer frente a estos ataques se acude, en primer lugar, a las medidas de seguridad de la información tales como las técnicas criptográficas, el uso de llaves de seguridad, de tarjetas magnéticas de acceso y los dispositivos de reconocimientos biométricos, como la identificación de la palma de la mano o de las huellas digitales, el escáner de retina o iris, y el reconocimiento de voz.

Dentro de las técnicas de comisión de estos delitos de espionaje cabe destacar el *wiretapping* o pinchado de líneas, que consiste en una intercepción programada de las comunicaciones que circulan a través de las líneas telefónicas, con el objeto de 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 en una casetera, para luego ser demoduladas por el módem, quien las transforma a señal digital que puede ser ingresada al computador.

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.

Ahora bien, el espionaje informático que se recoge en el Convenio también está sancionado en Chile, a través de la ley Nº 19.223, en su artículo 2, al disponer que: "El que con ánimo de apoderarse, usar o conocer indebidamente 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", es decir, en el rango entre los 61 días y los 3 años.

En primer lugar, es interesante mencionar el desconocimiento del legislador nacional respecto de la trascendencia de un "hurto" de datos, ya que en el primer informe de la Comisión se le consideró un delito de menor relevancia que el anterior, porque en él "no se destruye nada".

Por otra parte, se exige para la perfección subjetiva del tipo, de un elemento motivacional necesario en el agente comisivo: la intención o ánimo de apoderarse, usar o conocer, indebidamente, la información contenida en un sistema de tratamiento de la misma. Por tal razón, no bastaría con el cumplimiento de alguna de las conductas tipificadas —interceptar, interferir o acceder al sistema—, sino que es necesario este ánimo en el agente.

De esta forma, el delincuente podrá incurrir en tres hipótesis. En la primera, se apoderará indebidamente de la información, al recabar aquélla que considere relevante y actuar como si tuviera derecho a ella, privando a su legítimo titular de la posibilidad de disponer de la misma. Advertimos que no es necesario que la use ni que se lucre con la información. La segunda hipótesis ocurre cuando el agente usa indebidamente la información, cuando se sirve de ella. Basta que utilice los datos, con o sin ánimo de lucro, no siendo necesario el apoderamiento. Y en la tercera, buscará conocer indebidamente la información, es decir, averiguar por el ejercicio de las facultades intelectuales la naturaleza, cualidades y relaciones de las cosas. Nuevamente podemos apreciar independencia de este motivo en relación con los dos anteriores, ya que se puede conocer la información, sin usarla ni apoderarse de ella.

Elemento común en estas hipótesis es el carácter indebido de las acciones, es decir, su realización sin derecho o sin autorización. Así lo indicó expresamente el senador Otero al señalar "que al agregarse en el artículo 2° los verbos "usar" y "conocer", ellos, sin duda, quedan regidos por el adverbio "indebidamente". Luego la normativa contemplaría como elementos del tipo "El que con el ánimo de apoderarse indebidamente"; "El que con el ánimo de usar indebidamente", y "El que con el ánimo de conocer indebidamente". O sea, el adverbio afecta las tres formas verbales".

Al respecto, el entonces diputado y actual senador Viera-Gallo aclaró a la Cámara el sentido de incluir originalmente la expresión "sin derecho" señalando que "significa que la persona no tiene la posibilidad legal de acceder; sin embargo, lo hace cometiendo un abuso [...] Obviamente, existen tres situaciones: en el primer caso, el sistema de tratamiento de información al que, simplemente, el público no tiene acceso porque es privado y nadie puede tenerlo, salvo el propietario o personas que él autorice; en el segundo, puede haber sistemas de información en el que, para acceder, se cobre una determinada cuota o pago, y pudiera ocurrir que alguien ingresara a este sistema burlando el pago correspondiente, y, en el tercero, existen sistemas de información que, además, están protegidos por ciertos resguardos de la seguridad nacional, relacionados con sistemas de información de las Fuerzas Armadas o de los aparatos de inteligencia". Por lo tanto, existen distintas situaciones; pero quien debe determinar, en última instancia, si la persona que accede tiene derecho, es el juez.

Sin embargo, la forma adverbial "indebidamente" es tremendamente dificultosa, ya que se presta para ser interpretada, a contrario sensu, como que existe un comportamiento de alteración o de inutilización de un programa o datos que sea debido (a nuestro juicio lo hay, por ejemplo, al utilizar un programa antivirus).

Posteriormente, en el Tercer Trámite Constitucional, Viera-Gallo vuelve a referirse sobre el alcance de esta expresión indicando que "el efecto de usar las expresiones "indebidamente", "sin autorización" u otras semejantes, es hacer inoperante la calidad de ilícitas que llevan en sí todas las conductas sancionadas por la ley y descritas como

delitos. En consecuencia, obligan a indagar la licitud o antijuricidad de la conducta, que es previa a la indagación de la culpabilidad. Ordinariamente, toda conducta descrita y sancionada por la ley es ilícita, y el que sostiene que está justificada o autorizada debe probarlo, pero si se emplean las expresiones "sin derecho" u otras semejantes, pasa a presumirse que el hecho es ordinariamente lícito y el peso de la prueba recae sobre quien sostiene que no lo es".

Por lo tanto, en el ánimo del sujeto se incorpora el conocimiento de que la información que desea apoderar, usar o conocer está restringida para él.

Ahora, sobre al análisis de los verbos rectores contenidos en este artículo, previamente advertiremos que Viera-Gallo señaló que "la idea, para que quede bien precisa, es que esta interceptación, interferencia o acceso al sistema se haga mediante métodos tecnológicos. No se trata de que una persona, por casualidad, entre a una sala donde hay un computador y lea en la pantalla lo que allí aparece, aunque lo haga con el ánimo de apoderarse de la información, sino que, utilizando métodos tecnológicos modernos realice algunas de las conductas tipificadas en el artículo 2".

La primera de estas conductas es el "interceptar", que significa apoderarse de una cosa antes que llegue al lugar o la persona a quien se destina. La interpretación correcta de este verbo rector tiene que considerar que el interceptar implica evitar que una cosa llegue a su destino. Así, si pese a la acción de todas formas la información llegara a su destino o destinatario, no se habría producido la intercepción.

Por su parte, el "interferir" quiere decir cruzar, interponer algo en el camino de una cosa, o en una acción. Más específicamente consiste en introducir en la recepción de una señal otra extraña y perturbadora. Acá no se impide, necesariamente, que la información llegue a destino.

Finalmente, la acción de "acceder indebidamente" a un sistema de tratamiento de la información puede ser entendida como la realización de pericias tendientes a introducirse en él, burlando todas las medidas de seguridad, con el fin de allegarse a la información reservada que contiene, recabarla y eventualmente utilizarla en beneficio o en perjuicio de terceros. Tales acciones son las ya comentadas a propósito del delito de *hacking* indirecto.

c) Interferencia o alteración de datos informáticos

Esta modalidad del sabotaje informático, que para efectos del Convenio se regula en forma independiente, tiene como finalidad la protección de los datos informáticos contra la destrucción, daño, supresión o alteración intencionales, con el objeto de

proteger el derecho fundamental a la propiedad, de modo similar a la penalización del delito de daños causados contra los bienes físicos.

Por ello, el Convenio castiga la conducta dirigida a causar daños, deteriorar o borrar datos situados en un sistema informático, ya que equivale a alterar negativamente la integridad o el contenido de la información, por ejemplo, cuando se introducen "gusanos" informáticos. No obstante, se permite que los Estados se reserven el derecho de requerir un nivel de seriedad o gravedad en los daños para su sanción, situación que exige que cada Estado determine, por ejemplo, que ciertos perjuicios merecen mayor castigo que otros, o que ciertos datos resultan más relevantes para su tutela que otros.

En la legislación nacional la figura se encuentra recogida dentro del delito de sabotaje informático del artículo 3 de la ley Nº 19.223, al señalar: "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".

Aunque para algunos autores este artículo sancionaría el delito de alteración de datos, separadamente del sabotaje, al igual que en la legislación francesa y alemana, creemos que esta figura es el delito de sabotaje informático, ya que no corresponde una distinción, debido a que implicaría hacer extensivo, erróneamente, este delito a un sabotaje sobre los equipos. En este sentido, la única clasificación que admitiría el sabotaje informático se daría entre aquél que es dirigido en contra de los datos relevantes contenidos en el sistema y el que apunta contra los programas o instrucciones dadas al computador para su funcionamiento, situación que no se logra advertir claramente en el legislador.

Es más, reafirma esta opinión la contradicción y confusión de los parlamentarios, quien en un mismo informe presentado por la Comisión a la Cámara sostuvieron, a raíz del artículo 1°, que la moción únicamente se refería al *software* —los programas y datos—, y más adelante, afirman que el proyecto busca proteger los activos informáticos —*hardware* y *software*— ante agresiones. Por ello, difícilmente podría sostenerse que el sentido del artículo 3° distingue entre la alteración de datos y la de programas.

Hay que agregar que el artículo 3° no trata únicamente la alteración, sino que también los daños y la destrucción de los datos, conductas constitutivas de los sabotajes informáticos.

Sin perjuicio de lo anterior, esta conducta es claramente distinta de la alteración de datos a que se refiere el inciso 2° del artículo 1, ya que ahora, la acción está dirigida intencionalmente a obtener el resultado y no como en el artículo 1, en que el resultado

logrado no es buscado por el agente, sino que se consigue como consecuencia de la comisión de un delito de daños clásico.

Respecto a los verbos rectores del tipo, en primer término se alude a "alterar", que significa cambiar la esencia o forma de una cosa. Tal expresión comprenderá conductas tales como el ingreso de datos erróneos o *data diddling*, a través de las distintas técnicas de manipulación de la entrada, el borrado de datos verdaderos, transformaciones y desfiguraciones de los datos, por ejemplo, a través de los comunes virus informáticos, y, en general, toda conducta que implique cambiar la información contenida en un sistema de tratamiento de la misma sin destruirla.

Aunque en toda alteración se producirá por una manipulación de los datos, debe ser entendida en este caso en términos generales, para no confundir este delito con el de fraude informático o manipulación indebida de datos, tomada en sentido estricto, ya que acá no se acompaña el elemento del ánimo de lucro, sino sólo el de perjudicar a un tercero. Es más, este último delito no se encuentra tipificado en la ley N°19.223, existiendo una importante omisión del legislador que se tratará de subsanar con los proyectos de ley en trámite.

También se recurre a la acción "dañar", esto es, maltratar o echar a perder una cosa, se entiende como una conducta destinada a perjudicar la integridad de la información, lo que plantea la noción de un perjuicio, maltrato o afectación de una cosa. Con tal perjuicio se afectará el fin u orientación específica del mismo, a través de una conducta transitoria y reversible.

Además, se emplea el verbo "destruir", que quiere decir deshacer, arruinar o asolar una cosa. Implica un concepto amplio, que a diferencia del "dañar", es permanente e irreversible, cuya entidad se traduce en la pérdida de los datos a través de su desfiguración.

En fin, con tales acciones ilícitas y penas de presidio que van desde los 541 días hasta los 3 años, se busca brindar una protección al interés en la utilización de datos en perfecto estado.

d) Interferencia de sistemas o sabotaje informático

El Convenio sanciona el hecho de obstaculizar de manera dolosa y seria el uso legítimo de un sistema informático, incluidos los sistemas de telecomunicaciones. Para ello, la obstaculización está referida a la realización voluntaria de acciones que interfieren en el funcionamiento adecuado del sistema, a través de la inserción, transmisión, alteración, daño o supresión de datos informáticos.

La figura de sabotaje del sistema, contrariamente a la alteración de los datos, exige que la obstaculización necesariamente sea seria para que merezca sanción penal, sin embargo, el Convenio dispone que a cada Estado parte le corresponde determinar qué tipo de conducta alcanza la gravedad necesaria para poder ser calificada de "seria".

De este modo, podría estimarse que el daño causado supere cierta cantidad para ser serio, como podría ocurrir con el *spamming*, dado por su alto impacto tanto técnico como económico; o cuando el daño colateral por el mal funcionamiento es masivo como ocurre con acciones terroristas de denegación de servicio en sistemas críticos o puntos neurálgicos de la sociedad, ocasionadas normalmente por virus que infectan sistemas y se replican por miles y que encierran instrucciones para que se efectúen peticiones de respuesta de un servidor específico en un mismo momento, provocando con ello su colapso y posterior caída.

Las técnicas de sabotaje son diversas, por lo que podemos mencionar a modo de ejemplo, los *crash programs* o programas de destrucción progresiva, que son rutinas construidas dentro de programas de aplicación o dentro del sistema operativo, que permiten borrar un gran volumen de datos en un breve período, activándose con bastante posterioridad, por ejemplo, al momento en que el programador que lo crea abandona la empresa.

También son comunes las *time bombs, logics bombs* o bombas lógicas de actuación retardada, es decir, programas que persiguen la destrucción o modificación de datos en un momento futuro determinado, ya que contienen instrucciones que chequean la fecha diariamente permitiéndoles mantener oculta la época de caducidad programada al instalarlo en el sistema del usuario. El programador que instala una bomba de tiempo puede estar motivado por venganza, maldad o ánimo de lucro, ya que se puede utilizar para extorsionar exigiendo una suma de dinero a cambio de eliminar estos gérmenes destructivos.

Existen algunos fabricantes de software que, en una práctica absolutamente reprochable, introducen estas bombas lógicas en sus productos con el fin de asegurar el pago adeudado o evitar copias ilegales. Aquí, pese a que en los contratos de compraventa de software, generalmente sólo se conceden licencias de uso conservando la empresa el dominio del programa, el hecho de que el propio dueño programe estas bombas lógicas no le quita ilicitud a la acción, ya que los efectos perjudiciales por esta autotutela se radican en el patrimonio de una persona distinta, quien en virtud de un título legítimo utiliza el programa.

Por esta razón, al no ser agregado el código fuente en un contrato de compraventa de software, por ejemplo, el comprador se encuentra en desventaja al no poder acceder al lugar en el que comúnmente puede haber sido introducida precedentemente la bomba

lógica, la cual se activará en virtud de indicaciones precisas como la presencia o ausencia de un dato, de una hora, un nombre o un código.

Se han encontrado estas bombas a raíz de los contratos de mantenimiento, ya que el proveedor del servicio puede ser el mismo fabricante del programa. Así, en caso que el usuario decida poner término a sus servicios de mantenimiento, no renueve el contrato o no pague derechos adeudados, se activarían estos programas. También se ha dado el caso en que se detonan bombas lógicas que inutilizan un programa, permitiéndole al proveedor atribuir el hecho a una falta de mantenimiento imputable al usuario, o bien que detonan cada cierto tiempo para así cobrar mantenciones extraordinarias provocadas.

Por último, y entre otras técnicas, aparecen los virus, programas computacionales que pueden 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 señaladas y las que se emplean para manipular el sistema, son virus, es decir, programas.

Damos esa explicación ya que los autores escasamente dan definiciones precisas, ello debido a la gran variedad de virus que existen y que se crean diariamente, las múltiples formas de actuar y las alteraciones que persiguen, y los lugares del sistema en que se alojan.

Sin embargo, para hacer una distinción entre los virus y los demás programas de sabotaje informático, nos basaremos en que los primeros generalmente se adhieren al programa que infecta, en cambio los segundos tienen entidad propia.

Los virus informáticos usualmente se diseñan para realizar dos tareas: replicarse de un sistema informático a otro, y para situarse dentro de un computador, de tal modo que le sea posible modificar o destruir programas y datos, interfiriendo los procesos normales del sistema operativo.

Finalmente, hay autores que mencionan a los “gusanos”, que 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. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las de un virus, por ejemplo, podría dar instrucciones al sistema computacional de un banco para que transfiera continuamente dinero a una cuenta ilícita, antes de que se destruya, como en los fraudes informáticos.

El delito de sabotaje informático está tipificado —aunque no sin ser objeto de múltiples críticas— en el artículo 1 de la ley Nº 19.223, al establecer: “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", con una causal agravante si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, aplicándose la pena señalada, en su grado máximo.

En primer lugar, a diferencia de lo que se ha escrito hasta ahora respecto a la ley N°19.223, no creemos que el inciso 1 de este artículo tipifique al sabotaje informático, sino más bien trata un delito de daños tradicional sobre los bienes corporales muebles que integran un sistema de tratamiento de información. La razón se debe a que al haber circunscrito el delito informático únicamente para los atentados contra el soporte lógico de un sistema de tratamiento de información, es decir, programas —o sea, instrucciones— y datos relevantes, y al hacer mención expresa a los datos en el inciso 2°, pensamos que el inciso 1° apunta en dirección del soporte físico, las partes o componentes del sistema, objeto no comprendido dentro de los "delitos informáticos".

En segundo término, esta norma distingue entre la acción dirigida contra el sistema de tratamiento de información en sí mismo, o una parte de él, y contra su funcionamiento.

De tal manera, el sistema informático —referido sólo al *hardware* según la redacción del artículo— puede sufrir un atentado directo que le cause daños permanentes o irreversibles, a través de las acciones destinadas a destruirlo o inutilizarlo. En tal caso, los verbos rectores del tipo serán el "destruir", esto es, el deshacer, arruinar o asolar una cosa material —en este caso el *hardware*—; y el "inutilizar", que significa hacer inútil, vana o nula una cosa, por ejemplo, si luego del ataque el sistema no sirve para el procesamiento de datos o ve limitada su utilidad, sin necesidad de destruirlo.

Ahora bien, si el ilícito se dirige contra el funcionamiento del sistema informático, buscando "impedir", "obstaculizar" o "modificar" la ejecución de las funciones que le son propias al sistema, hay que entender previamente que éste funcionará si operan conjunta y adecuadamente sus componentes lógicos —programas o instrucciones— y físicos —*hardware* o equipos—, y dejará de hacerlo cuando dicha interacción se rompa a consecuencia de diversas acciones, sean dolosas, negligentes o lícitas, por lo que surge un nuevo desacierto del legislador al contemplar en el tipo de un supuesto "delito informático" a una situación de hecho muy amplia y poco clara.

Es decir, primero habría que distinguir si el sistema deja de funcionar a consecuencia de un atentado contra el soporte lógico —las instrucciones dadas al computador— o contra los equipos, con lo que llegamos nuevamente a la conclusión propuesta de estimar como delito tradicional de daños a los ataques dirigidos contra el *hardware* y que ocasionen el mal funcionamiento del sistema, y sólo tratar como delito de

sabotaje informático el ilícito penal que atente contra el soporte lógico o programas, afectando las funciones que deba ejecutar el computador.

En este último caso, si la intención del legislador fue tratar a los programas o soporte lógico al referirse al "funcionamiento" del sistema informático, habría sido más adecuado aludir a "los atentados contra las instrucciones u órdenes lógicas que permiten el funcionamiento de un sistema de tratamiento automatizado de información".

Cuando se ataca el funcionamiento del sistema los verbos rectores que se aprecian son tres: "impedir", que significa estorbar, imposibilitar —en forma absoluta, creemos— la ejecución de una cosa; "obstaculizar", esto es, impedir o dificultar la consecuencia de un propósito, por ejemplo si el sistema no puede cumplir normalmente las operaciones de transformación de los datos en información procesada; y "modificar", es decir, transformar o cambiar una cosa mudando alguno de sus accidentes, por lo que bastaría con que no funcione de la forma prevista por el titular para que se realice esta acción, siendo de cargo del juez, auxiliado por peritos, determinar si el funcionamiento del sistema dejó de ser idóneo para satisfacer los requerimientos específicos del usuario y para lo cual fue diseñado.

Un tercer comentario, extensivo para los demás artículos de la ley, se refiere al sujeto activo. Al emplearse la expresión "el que" no se restringe el tipo penal a un sujeto calificado, por ejemplo, por el nivel de conocimientos técnicos que posea o el cargo que desempeñe.

Como cuarta idea que surge de la exégesis de este artículo, y al igual que en el 3° y 4°, la doctrina se ha visto dividida ante la supuesta inclusión en el tipo de un elemento subjetivo adicional derivado de la expresión "maliciosamente".

Un último comentario al artículo se refiere a la causal de agravamiento de la responsabilidad, contenida en el inciso segundo. Se señala que si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena de presidio menor en su grado máximo. Es decir, la pena original de este delito, que va desde los 541 días hasta 5 años de presidio, se debería aplicar ahora a partir de los 3 años y un día como mínimo.

En este caso, el sujeto activo del delito de daños no persigue directamente el afectar los datos contenidos en el sistema, es decir, alterarlos o modificarlos —hecho que refuerza nuestra interpretación del inciso 1°—, pero como es previsible que esto puede ocurrir por tales acciones, se sanciona el resultado obtenido aunque no haya sido querido por su autor. Sin perjuicio de ello, para algunos es irrelevante este inciso, porque para atentar contra la información o manipular datos generalmente se

requiere el uso normal y correcto de las instrucciones, no destruirlas, inutilizarlas u obstaculizarlas.

No obstante, en los proyectos de ley en trámite se busca corregir estos errores.

e) Abuso de dispositivos

Este delito —que no encuentra su símil en nuestro derecho—, sanciona conductas específicas, tales como fabricar, vender, usar, importar y distribuir dispositivos de acceso principalmente diseñados o adaptados para el abuso de redes o sistemas informáticos, por ejemplo, decodificadores de claves de acceso.

Para que se cometa esta conducta delictiva es necesario que su autor persiga una finalidad determinada que se oriente a facilitar los ataques contra la confidencialidad, integridad y disponibilidad de sistemas o datos informáticos.

No cabe duda que estos delitos estarán vinculados al mercado negro de la fabricación y distribución de los equipos de acceso u otros dispositivos que se requieren, por lo que el Convenio, con el fin de prevenir consecuencias más graves, prohíbe fabricar, distribuir y vender estos dispositivos con anterioridad a la comisión del delito contra los sistemas informáticos.

Por lo tanto, desde el momento en que se tipifica penalmente la mera posesión de estos dispositivos con independencia de su utilización, podemos concluir que se trata de un delito de peligro, pese a que los Estados parte pueden imponer exigencia adicionales mínimas para que se configure el delito, por ejemplo estableciendo que sea necesario poseer un cierto número de estos equipos.

Por último, existe en el Convenio una cláusula específica que excluye del delito los casos en que se trate de dispositivos creados para la realización de pruebas autorizadas de seguridad informática.

3.2. Delitos asociados a la informática

Esta categoría incluye dos tipos de delitos basados en la manipulación: el fraude y la falsificación informáticas, los cuales pueden ser cometidos mediante redes digitales. En este tipo de delitos la red es un instrumento de la comisión, pero no su objeto mismo y debe tipificarse específicamente su comisión mediante un sistema informático porque los tipos penales tradicionales no resultan, en general, aplicables a las perpetradas en medio informático. Por ejemplo, en el caso del fraude asistido por

computador faltará el elemento del engaño exigido en las estafas y en el caso de la falsificación de documentos informáticos faltará la diferencia entre original y copia.

Una característica propia del fraude y la falsificación informáticas es que el número potencial de víctimas es muy alto, por lo que se habla de macro-victimización. Su inclusión en el Convenio sobre Cibercrimen refleja el hecho de que los bienes jurídicos tradicionales no están suficientemente protegidos en muchos ordenamientos contra las agresiones delictivas derivadas del abuso de las tecnologías de información.

Se han multiplicado las oportunidades de cometer delitos económicos tales como el fraude de tarjetas de crédito. Los activos representados o administrados a través de redes o sistemas informáticos resultan también de interés para los delincuentes capaces de llevar a cabo manipulaciones electrónicas susceptibles de producir un resultado similar a aquellas manipulaciones fraudulentas que afectan a los bienes de la víctima del tipo penal tradicional. Este delito consiste principalmente en la realización de manipulaciones mediante la inserción en el sistema de datos inexactos o mediante manipulaciones de programas u otras interferencias llevadas a cabo durante el procesamiento de datos, con la intención de que tenga lugar una transferencia ilegítima de propiedad en perjuicio de tercero, su legítimo propietario.

La falsificación informática tiene por finalidad la tipificación armonizada de una infracción paralela a la falsificación de documentos tangibles. Lo que persigue su inclusión es completar posibles lagunas jurídicas que pudieren resultar de ciertos elementos del o de los tipos tradicionales de falsedad que dificulten o impidan su aplicación a los documentos digitales. La manipulación de datos informáticos puede tener para un tercero las mismas consecuencias graves que la falsificación física, siempre que la víctima sea inducida a tomar sus decisiones con el engaño de los datos falsificados. La falsificación informática implica la creación o alteración no autorizada de datos almacenados con el fin de que adquieran un valor de prueba en el curso de una transacción jurídica, la cual descansa en la autenticidad de la información puesta de manifiesto por tales datos, induciéndose a engaño.

3.2.1. Delitos de Fraude Informático

Debido a que la mayoría de los delitos informáticos se comete a través de acciones arteras destinadas a intervenir los sistemas de tratamiento de información para servir intereses propios o ajenos, la doctrina entiende que la manipulación de datos es un ilícito general y comprensivo de las distintas conductas criminógenas de carácter informático.

Sin embargo, preferimos acotar el ámbito del delito de manipulación indebida de datos o fraude informático, a un tipo delictual específico, donde será característica la

existencia de un perjuicio patrimonial directo en la víctima y un ánimo de lucro en el sujeto activo, unido a un engaño generalmente realizado a través de la ocultación.

Como adelantamos, es frecuente que tales delitos sean cometidos por los mismos trabajadores de empresas, bancos, instituciones financieras, servicios públicos o compañías de seguros, contra quienes generalmente se delinque. Pero no se puede desconocer la amplitud de otras posibilidades que la telemática brinda, junto con la cada vez más masiva utilización de cajeros automáticos por el público.

En relación con las modalidades comisivas debemos distinguirlas de acuerdo a la fase de procesamiento de información en la cual se aplican las técnicas delictuales. Así, puede afectar el *input* o entrada de datos (*data diddling*), a través de la introducción de datos falsos al computador con el objeto de defraudar, por ejemplo, obteniendo pagos por servicios inexistentes, aumentando el saldo a favor en las cuentas bancarias, o alterando la contabilidad de una empresa.

La falsedad de los datos introducidos puede ser causada por omisiones o por alteraciones de la realidad, totales o parciales, con lo cual el dato deja de ser representativo de ésta. Pero pese al carácter apócrifo del material introducido a la máquina, su procesamiento se realiza normalmente, generando un resultado correcto. Lo reprochable es la agresión que se realiza al buen uso que la técnica informática necesita para el procesamiento de la información.

Afortunadamente, estas manipulaciones en la entrada de datos son fáciles de detectar gracias a la contabilidad y auditoría permanente.

Las manipulaciones también puede recaer en los programas, cuando el sistema recibe una o más operaciones de transformación, tales como, clasificación, distribución, cálculo o resumen, realizándose así, el procesamiento de datos. Con estas manipulaciones es posible que datos verdaderos que han entrado correctamente, sean alterados en su tratamiento arrojando resultados falsos, gracias a la modificación, eliminación o agregación de algunos pasos del programa.

A diferencia de las manipulaciones en la entrada, éstas son extremadamente difíciles de detectar y prevenir. Si consideramos que su desarrollo puede demorar un tiempo prolongado, realizando pequeñas modificaciones en la estructura y ordenamiento del programa y agregando alteraciones que encubren esos cambios, las auditorías difícilmente encuentran discrepancias inexplicables en las cuentas. Precisamente, por esa permanencia en el tiempo y aptitud natural y técnica para mantenerse en ejecución por períodos prolongados se los califica como delitos continuados.

Las técnicas que con más frecuencia menciona la doctrina son los troyanos y el *rounding down.* Los primeros consisten en introducir dentro de un programa de uso

habitual, una rutina o conjunto de instrucciones, no autorizadas, para que dicho programa actúe en ciertos casos de forma distinta a como estaba previsto.

Así, en determinadas circunstancias puede ejecutar erróneamente un cálculo, por ejemplo, desviando partidas hacia cuentas ficticias. También podría perseguir la impresión de documentos no autorizados o no imprimir documentos reales. Es frecuente utilizar este método para introducir una modificación al programa de tratamiento de cuentas corrientes de manera que cada vez que se consulte el saldo de una determinada cuenta lo multiplique por una cantidad aumentando el cupo y permitiendo la autorización de pagos o transferencias por un importe muy superior al saldo real.

No obstante ser muy difícil de detectar, ya que el programa normalmente funciona en forma correcta, es vital el implantar técnicas de prevención.

Por otra parte, el *rounding down*, es muy fácil de realizar pero difícil de descubrir, y consiste en introducir o modificar ciertas instrucciones de ejecución en un programa con el objetivo de extraer de las cuentas pequeñas cantidades de dinero nominal, transfiriéndolas automáticamente a una cuenta corriente que ha contratado el delincuente bajo un nombre falso, o a través de interpósita persona, por lo general.

Además, se comete mediante el redondeo de los intereses de las cuentas bancarias o depósitos a plazo, aproximando las cantidades centesimales a la unidad, produciéndose con ello la cuadratura de los balances.

Por último, están las manipulaciones en el *output* o en la salida de datos mediante la intervención en la parte mecánica de la emisión de datos procesados, por ejemplo, intervenir el cable telefónico para interceptar datos y manipularlos. Lo mismo se puede producir en el video, la impresora u otros dispositivos de salida. Sin embargo, en este caso y a diferencia de los anteriores, los datos introducidos al computador son verdaderos y hay ausencia de manipulación durante la ejecución del programa.

Aunque el fraude informático y la falsificación informática no están tipificados en la ley Nº 19.223, se pretenden incorporar en los proyectos en trámite.

3.3. Delitos de contenido

La tercera categoría de delitos son los relativos a los contenidos, que incluyen una serie de conductas relacionadas con la pornografía infantil y la pedofilia. En consecuencia tipifica varios comportamientos que van desde la posesión hasta la distribución de material pornográfico infantil, cubriendo todos los eslabones de la cadena.

En este sentido, el Convenio tiene como objetivo reforzar las medidas de protección de la infancia, inclusive, la protección de los niños contra la explotación sexual, y ello mediante la modernización de las normas penales de manera de limitar en forma más eficaz la utilización de sistemas informáticos en la comisión de delitos sexuales contra los niños.

Se penalizan de este modo la producción, distribución y posesión electrónicas de pornografía infantil. La mayoría de los Estados ya castigan penalmente la producción y distribución físicas de material pornográfico infantil —en Chile se encuentra en trámite un proyecto de ley al respecto—. Con el incremento de la utilización de Internet como principal medio para comerciar con este tipo de producto, el Convenio considera indispensable insertar disposiciones específicas en una norma internacional para combatir esta nueva forma de explotación sexual y riesgo para la infancia.

Cabe agregar que el 28 de enero de 2003 se suscribió en Estrasburgo, un Protocolo Adicional a dicha Convención, concerniente a la penalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos.

Al respecto, dicho Protocolo Adicional complementa lo anterior incluyendo como delito la utilización de Internet para la expresión, distribución y venta de materiales de naturaleza racista o xenófoba o apologética de partidos, movimientos o asociaciones nazis o filonazis, uno de los ejemplos más repugnantes de abuso de las tecnologías de información.

3.4. Delitos relativos a la vulneración de derechos de autor y conexos

La cuarta y última categoría de los delitos del Convenio comprende las infracciones al derecho de autor y conexos cometidas a través de redes digitales. Se trata de combatir, por ejemplo, la distribución a escala comercial de copias ilegales de obras protegidas por los derechos de autor causantes de perjuicios económicos considerables para el titular de los mismos. Nos encontramos, por consiguiente, con una infracción similar a las recogidas por el grupo anterior, es decir, de contenido, con la apreciable diferencia de que en el caso presente el contenido reproducido o distribuido es perfectamente legítimo.

Las infracciones de los derechos de propiedad intelectual son muy frecuentes en Internet, lo cual preocupa a los titulares de los derechos y también a aquellos que trabajan profesionalmente en las redes digitales. La reproducción y distribución a través de Internet de obras protegidas, sin consentimiento del titular de derechos de autor, son extremadamente frecuentes e incluyen obras literarias, fotográficas, musicales, audiovisuales y otras. Gracias a la tecnología digital las copias pueden

realizarse con pasmosa facilidad con lo cual la reproducción y distribución de estas obras a través de Internet adquiere inmediatamente una gran escala.

La industria de fabricación de *software* sufre anualmente enormes impactos económicos causados por la copia no autorizada de programas. Lamentablemente la normativa que existe no logra disuadir al delincuente, debido a que éste se ve estimulado a "piratear" gracias a la facilidad con que se pueden copiar los programas, la no existencia de sistemas de seguridad que efectivamente eviten o al menos, detecten la "piratería", el alto precio que se debe pagar por un *software* legítimo, y por la difusión masiva de un hecho calificado por el común de la gente como público y notorio: el pirata no es sancionado.

La "piratería" es un delito informático que, según el legislador chileno, persigue no solo la reproducción, sino también el plagio, distribución, comunicación, transformación, exportación o importación de *software*, 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.

En relación con esto último, el bien jurídico que se protege es el derecho de propiedad intelectual que tiene el fabricante, razón por la cual es común que estos delitos se tipifiquen en las leyes que protegen el derecho de autor.

De acuerdo a la definición, la "piratería" informática puede cometerse mediante la realización de distintas acciones, a saber: la reproducción (sacar copias de un programa utilizando un sistema informático); el plagio (copiar en lo substancial obras ajenas, dándolas como propias. Aclaremos que, a menos que se le haya vedado expresamente por el autor, un cesionario de los derechos de explotación del programa podrá realizar versiones sucesivas de éste o derivados del mismo sin constituir plagio); la distribución y comunicación; la importación y exportación; y la transformación (referida a la traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente).

El derecho comparado sanciona el delito de piratería de programas se cometa o no, con ánimo de lucro. Dicha motivación la determina la explotación del material "pirateado", agravando en algunas legislaciones la responsabilidad penal. Sin embargo, estas medidas penales, por su naturaleza de *ultima ratio*, tienen un carácter subsidiario de la protección civil o mercantil de los programas de computador.

Debido a que la ley Nº19.223, sobre Delitos Informáticos, no contiene esta figura, a continuación indicaremos nuestras observaciones sobre la norma que sí lo recoge: la ley Nº17.336, sobre Propiedad Intelectual.

Según nuestra interpretación a la ley N°17.336 sobre Propiedad Intelectual, el delito de "piratería" de *software* o copia no autorizada de programas se sancionaría en el artículo 79 letra a) y en el 80 letra b), con dos figuras penales. Esto, sin perjuicio de la acción civil de indemnización.

En primer término, de acuerdo al artículo 79 letra a) de la citada ley, "cometen delito contra la propiedad intelectual y serán sancionados con la pena de presidio menor en su grado mínimo [desde 61 a 540 días] y multa de 5 a 50 unidades tributarias mensuales, los que, sin estar expresamente facultados para ello, utilicen obras de dominio ajeno protegidas por esta ley, inéditas o publicadas, en cualquiera de las formas o por cualquiera de los medios establecidos en el artículo 18".

Esto significa que sólo el titular del derecho de autor del programa —el programador, su empleador, quien lo encargó para su comercialización, o el cesionario, según el caso—, y quien esté expresamente autorizado por él —mediante una licencia de uso, principalmente—, tendrán derecho a utilizar dicha obra. Los demás, incurrirían en las sanciones civiles y penales correspondientes.

La utilización puede consistir en la publicación de la obra —editándola, grabándola, ejecutándola, exhibiéndola, o empleando cualquier otro medio de comunicación al público, actualmente conocido o que se conozca en el futuro—, en su reproducción por cualquier procedimiento, en su adaptación a otro género o su utilización en cualquier otra forma que entrañe una variación, adaptación o transformación de la obra originaria, incluida la traducción, o bien, en su ejecución pública a través de cualquier medio.

Del tenor literal del artículo 79 letra a) se entiende que la utilización puede ser hecha a título gratuito u oneroso, no es necesario que le reporte un provecho al infractor, y tampoco se requiere que éste haya tenido ánimo de lucro o intención de perjudicar al titular del derecho. Por ello, la pena no depende del monto del perjuicio causado ni del lucro obtenido.

Además, como no todas las formas de utilización establecidas en el artículo 18 deben publicitarse al público en general —únicamente en caso de publicar o ejecutar la obra—, entendemos que constituye delito la reproducción, total o parcial, de un programa informático para fines privados.

Por lo tanto, toda copia de un programa que no sea expresamente autorizada por el titular de los derechos de autor en la licencia, será una violación a la Ley de Propiedad Intelectual y constituirá un delito de copia ilegal. Sin perjuicio de ello, no se configurará tal delito en dos casos excepcionales contemplados en el artículo 47, inciso 2° y 3° de dicha ley: cuando se permite copiar o adaptar el programa por ser

esencial para su uso en un computador determinado o para fines de respaldo y sin destinársele a un uso diverso.

Por su parte, el artículo 80 letra b) de la ley N° 17.336, castiga como delito contra la propiedad intelectual merecedor de presidio o reclusión menores en su grado mínimo —61 a 540 días—, al que en contravención a las disposiciones de esa ley o a los derechos que ella protege, intervenga, con ánimo de lucro, en la reproducción, distribución al público o introducción al país de programas computacionales, y a los que adquieran o tengan con fines de venta tales programas, infringiendo la ley. Si hay reincidencia la pena se aumenta en un grado pudiendo llegar hasta 3 años.

Con este artículo, criticado por muchos tanto desde el ámbito penal —por no describir claramente la conducta y con ello, atentar contra el principio de legalidad— y desde el derecho autoral —por sancionar al "pirata" informático sólo si actúa con ánimo de lucro—, el legislador buscó otorgar una protección amplia al titular del derecho de autor en nuestro país.

Finalmente, respecto a las modalidades delictivas, la copia de archivos y de programas se ha visto facilitada por distintas técnicas, como la compresión de datos, y por dispositivos periféricos de entrada y salida que permiten almacenar rápidamente gran cantidad de información, por ejemplo, la totalidad de un disco duro. A ello se agregan los *cracks* o programas craqueadores que torna vulnerable a un *software* pese a contar con medidas anticopia.

4. Medidas de derecho procesal, orientadas a la investigación y obtención de pruebas

Esta sección es el complemento instrumental de las normas de derecho sustantivo necesario para investigar y obtener pruebas en los casos de delitos informáticos, situación que suele no abordarse en las legislaciones que establecen leyes específicas, como ocurre en el caso chileno, por ejemplo. Su importancia se manifiesta en la dificultad para aplicar en el entorno digital ciertas normas sobre investigación que han sido pensadas para los delitos tradicionales, además de la problemática relativa a la conservación y presentación de pruebas electrónicas admisibles ante los tribunales de justicia.

Por ese motivo, el Convenio tiene como uno de sus objetivos el que los Estados parte se doten de reglas comunes en materia procesal que permitan una persecución eficaz de los delitos cometidos contra o a través de redes digitales y la obtención de las pruebas de delitos tradicionales cuando éstas se hallen en soporte electrónico. El camino seguido es, principalmente, adaptar al medio informático las medidas pre-

existentes en el mundo físico, o crear nuevas medidas propias de la investigación del delito informático, tales como la custodia inmediata de datos.

Además, dado que los datos fluyen en las comunicaciones electrónicas en red, se dispone la utilización en la investigación de los delitos informáticos de medidas que son tradicionales en la obtención de información a través de las telecomunicaciones, tales como la intercepción de datos de tráfico y de contenidos en tiempo real.

De este modo, el Convenio trata las siguientes facultades y medidas:

- Conservación inmediata de datos informáticos almacenados
- Conservación inmediata y revelación parcial de datos de tráfico
- Mandatos de exhibir
- Registro y decomiso de datos informáticos
- Intercepción de datos de tráfico en tiempo real
- Intercepción de datos de contenido en tiempo real

1) Conservación inmediata de datos informáticos almacenados

En primer término, la facultad de ordenar la conservación inmediata de datos se aplica exclusivamente a aquellos datos que son pre-existentes, es decir, aquellos que han sido recogidos y/o almacenados con anterioridad en un sistema informático, por ejemplo, por el proveedor de servicios de acceso a Internet a los efectos de facturación.

Cabe hacer presente que esta medida suscitó gran debate durante la elaboración del Convenio, ya que originalmente se consideró la posibilidad de imponer a los proveedores de servicios la obligación de almacenar o recoger con carácter general ciertos datos que pudieran ser necesarios ulteriormente a los efectos de una investigación penal —idea que se ha puesto sobre la mesa en más de una oportunidad en los proyectos de ley en trámite—. Sin embargo, los proveedores de servicios y la industria informática objetaron los costos excesivos que tal obligación implicaría y rehusaron participar en el control de los delitos informáticos, labor que estimaron no debe recaer en las empresas privadas. A ello se suman las opiniones que advirtieron que una obligación general de archivar datos puede ser contraria al derecho a la vida privada y al secreto de las telecomunicaciones, además de infringir la legislación europea sobre protección de datos de carácter personal.

Por consiguiente, el Convenio terminó por referirse a la conservación de datos y no incluyó obligación alguna de archivar, almacenar o coleccionar datos de un tipo u otro. En realidad se limitó a conferir a las autoridades encargadas de perseguir el cibercrimen la facultad de requerir, en el marco del procedimiento penal específico ya

abierto, la conservación de aquellos datos que se encuentren previamente archivados, almacenados o coleccionados y que pudieran ser necesarios para la identificación de los autores o como prueba.

En cuanto a la supuesta equivalencia entre las expresiones "conservación de datos" y "archivo de datos", jurídicamente tienen un contenido claramente diferenciado, ya que conservar implica guardar o custodiar datos previamente almacenados o archivados, protegiéndolos contra cualquier riesgo o amenaza que pudiera alterar o degradar su calidad o estado presente, y archivar, en cambio, quiere decir guardar en posesión de uno para un uso futuro aquellos datos que están siendo producidos en el momento presente. El archivo equivale al almacenamiento de datos, y la conservación consiste en garantizar su seguridad y su integridad.

Se puede requerir la conservación tanto de datos de tráfico como de materiales ilegales, pruebas, etc., por el tiempo necesario hasta un máximo de 90 días, que pueden ser renovables. Además, la obligación de custodiar impuesta al proveedor de servicios puede llevar consigo la obligación de mantener en secreto tanto la orden de conservación como la existencia misma de un procedimiento penal abierto y ello durante todo el período de vigencia de la orden.

En la mayoría de los países los procedimientos de conservación de datos son novedosos. Consisten en un método de investigación criminal cuya utilidad es evidente ante el cibercrimen, sobre todo en relación con las infracciones cometidas a través de Internet, porque los datos informáticos, por su alta volatilidad son fáciles de manipular y modificar, y se pueden perder datos susceptibles de probar la infracción si el almacenamiento no se lleva a cabo correctamente, si los datos son alterados intencionalmente para destruirlos o si su destrucción tiene lugar en el marco de operaciones normales de borrado de datos considerados inútiles.

Uno de los medios provenientes del derecho procesal tradicional útiles para preservar la integridad de los datos es la entrada y registro en los locales y en el sistema informático del poseedor de los datos. Ahora bien, cuando el custodio de los datos es digno de confianza, la conservación adecuada de los datos puede quedar garantizada de manera más expeditiva mediante una orden de conservación dirigida a la entidad en cuestión. Cabe advertir que una orden de conservación siempre resultará menos lesiva para el funcionamiento y la reputación de la empresa en cuestión que una operación de entrada y registro policial.

En segundo lugar, hay que recordar que los delitos informáticos son, a menudo, cometidos mediante la transmisión de comunicaciones a través de redes digitales. La identificación de la fuente o del destino final de tales comunicaciones puede permitir la identificación del autor o autores.

Finalmente, la conservación de datos puede permitir probar la actuación criminal independientemente de que se trate de delitos informáticos o tradicionales.

La orden de custodia de datos es una medida preliminar que se adopta frecuentemente en los primeros momentos del procedimiento a la espera de que puedan adoptarse otras medidas jurídicas que permitan a las autoridades encargadas de la investigación acceder a los datos en cuestión u obtener que éstos sean divulgados. Por lo tanto, la adopción de dicha medida no implica que las autoridades puedan tener acceso inmediato a cualquiera de los datos bajo custodia sino que el poseedor de los mismos está obligado a protegerlos hasta que se produzca la medida complementaria. Los 90 días de plazo máximo de custodia deberían ser suficientes para que las autoridades puedan adoptar tales medidas complementarias, el registro, el embargo, la autorización judicial de acceso a los datos o el mandato de exhibir. No obstante, hay que precisar que las solicitudes de auxilio judicial internacional relativas a una orden de conservación inmediata de datos serán válidas durante un período de al menos 60 días con el fin de que la parte requirente pueda presentar una solicitud de registro, embargo, de acceso u obtención de los datos por medio similar, o de divulgación de los datos sometidos a conservación.

2) Conservación inmediata y revelación parcial de datos de tráfico

Lo señalado precedentemente también es aplicable a la medida de conservación inmediata de datos de tráfico, con la particularidad de que el destinatario de una orden no sólo está obligado a conservar los datos durante el tiempo especificado sino también a revelar inmediatamente ciertos datos de tráfico, señaladamente aquellos que permitan a las autoridades conocer a los proveedores de servicios que intervinieron en la transmisión de la comunicación desde su origen hasta su destino, reconstruyendo de este modo el camino seguido por el autor del delito.

3) Mandatos de exhibir

El mandato de exhibir permite a las autoridades obligar a una persona que se encuentre en el territorio de ese Estado a suministrar aquellos datos pre-existentes que se especifiquen o a un proveedor de servicios a facilitar los datos de sus suscriptores. En lugar de utilizar medidas coercitivas, tales como el registro y decomiso de datos en relación con terceros ajenos a la comisión del delito, el Convenio opta por establecer medidas de investigación alternativas que permitan obtener la información incurriendo en un riesgo menor de interferir en el ejercicio de los derechos fundamentales, en particular del derecho a la privacidad. Este mecanismo del mandato a exhibir resulta particularmente apropiado para obtener la cooperación de determinados particulares o empresas poseedores de datos de interés para la

investigación criminal en cuestión, a las autoridades judiciales, tales como los proveedores de servicios de Internet, quienes necesitan una base jurídica para poder divulgar los datos en su posesión sin incurrir por ello en responsabilidad contractual.

4) Registro y decomiso de datos informáticos

El registro de un sistema informático y decomiso de datos es el equivalente digital de la tradicional entrada y registro de domicilio con recogida de los instrumentos y efectos del delito, por lo que muchas de las características de la medida prevista para el mundo físico permanezcan en las medidas utilizables en el medio digital, como por ejemplo, respecto de las condiciones para obtener una autorización judicial. Sin embargo, existen diferencias desde el momento en que los datos son intangibles y no pueden ser transportados de la misma manera, además de que pueden no encontrarse en el computador concreto que se registra, ya que resultan accesibles en el sistema al que éste pertenece o son accesibles a distancia a través de una red digital. Por ello, los Estados signatarios pueden verse obligados a adoptar disposiciones complementarias en materia de copias de los datos encontrados en el sistema registrado o en materia de extensión de la orden de entrada y registro a computadores o sistemas informáticos conectados a aquel computador o sistema originalmente objeto de la orden.

El poder de decomisar datos informáticos almacenados incluye la posibilidad de embargar el hardware y de utilizar o embargar los programas necesarios para acceder a los datos. Además, se pueden utilizar medidas de aseguramiento de los datos incautados para que permanezcan en el estado en el que se encontraban en el momento de practicarse la medida, inclusive mediante su extracción del sistema en el que se encontraban los datos.

5) Intercepción de datos de tráfico y contenido en tiempo real

Sin duda, el Convenio ha presentado fuertes opositores principalmente por la facultad de intercepción en tiempo real de datos de tráfico y de datos de contenido, que se contempla, por ser la más invasiva de derechos. Dichas medidas pueden ser llevadas a cabo tanto por las autoridades penales competentes como por los propios proveedores de servicio a solicitud de las autoridades.

Los datos que se pueden obtener son de dos tipos: de tráfico y de contenido, entendiendo por los primeros a aquellos datos relativos a una comunicación a través de un sistema informático, producidos por este último por ser un elemento de una cadena de comunicación y que indiquen el origen, destino, itinerario, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

No obstante, en muchos ordenamientos jurídicos nacionales, tal distinción es inexistente, pero el Convenio la ha mantenido debido a que el ejercicio de los poderes de intercepción de datos de contenido podría entrañar riesgos mayores de ingerencia en el derecho a la privacidad y el secreto de las comunicaciones. De este modo, ha previsto la posibilidad de que los Estados parte limiten en su derecho interno la utilización de la intercepción de datos de contenido en tiempo real solamente a los procedimientos relativos a infracciones graves, a definir por el derecho nacional.

Igual que en el caso de la obligación de conservación, el ejercicio de los poderes de intercepción en tiempo real, sea de datos de tráfico o de contenido, puede ir acompañado de la imposición de una obligación al proveedor de servicios de mantener tal ejercicio en secreto.

5. Cooperación internacional

Atendido que el Convenio tiene como uno de sus objetivos el facilitar la aplicación internacional de aquellas nuevas facultades y medidas que se atribuyen a las autoridades penales para la investigación interna de la delincuencia informática, esta sección permitirá la puesta en funcionamiento de formas rápidas y eficaces de cooperación internacional, indispensables para la investigación, persecución y represión penal del cibercrimen.

En tal sentido, las autoridades de cada Estado signatario deberán de ser capaces de llevar a cabo cualquiera de las medidas de investigación previstas a solicitud de otro Estado parte y transmitir el resultado rápida y eficazmente. Para ello, además de las formas tradicionales de cooperación —extradición y auxilio judicial mutuo—, el Convenio dispone que los Estados parte aplicarán los poderes y procedimientos específicos previstos a requerimiento de los demás Estados parte, como nuevas formas de auxilio judicial mutuo.

El Convenio dispone que los Estados signatarios se otorgarán ayuda mutua en la mayor extensión posible, minimizando los obstáculos que pudieren existir para el flujo rápido y armonioso de la información a través de las fronteras. Cabe destacar que el ámbito de la cooperación en virtud del Convenio no está circunscrito a los procedimientos relativos a los delitos definidos en él, sino que resulta aplicable a las investigaciones y procedimientos penales relativos a cualquier delito cometido a través de un sistema informático y cuyas pruebas se encuentren en forma digital.

Asimismo, se establece la obligación para los Estados parte de poner en pie una red de asistencia internacional específica para la represión del cibercrimen, a saber una red permanente de puntos de contacto (bajo la modalidad de funcionamiento 24x7). El establecimiento de esta red permanente de asistencia y contacto, que completa pero

no sustituye los canales tradicionales de la cooperación internacional, es uno de los resortes más importantes del Convenio para conseguir que los Estados actúen coordinadamente en la aplicación de la legalidad en el ciberespacio, atendiendo oportunamente y con eficacia los requerimientos de los demás Estados parte.

Por último, cabe agregar que el Convenio no regula las investigaciones transfronterizas en red, por ejemplo mediante los registros transnacionales de sistemas informáticos, pues los negociadores no lograron ponerse de acuerdo en las modalidades de esta forma de cooperación internacional, cuya utilización afecta a intereses nacionales primordiales y, en último término, a la soberanía nacional de los Estados. El Convenio se limita a autorizar a cada Estado parte a acceder o recibir datos informáticos almacenados en un sistema informático fuera de su territorio si tales datos son accesibles al público o si así lo autoriza la persona legalmente autorizada a divulgarlos.

6. Conclusiones

El Convenio sobre Cibercrimen constituye un instrumento internacional de aspiraciones globalizadoras frente al cual nuestro sistema jurídico guarda cierta armonía desde el punto de vista de las figuras penales de derecho sustantivo que se sancionan, tanto por nuestro derecho vigente como por las próximas modificaciones que se realizarán para actualizar la materia.

Sin embargo, no compartimos medidas instrumentales de investigación y de cooperación internacional similares a las que se mencionan en el Convenio, siendo un tema pendiente de abordar por nuestro legislador. No obstante, que el Convenio viene a armonizar a posteriori las legislaciones y prácticas nacionales pre-existentes de los Estados signatarios, en nuestro caso es el Derecho Internacional el que nos debe impulsar a la adopción de medidas nacionales acordes con el progreso tecnológico.

Finalmente, cabe hacer presente que el citado Convenio no ha estado carente de críticas y opiniones encontradas, que lo consideran como un medio para anular los derechos individuales de los usuarios de las redes, razón por la cual cualquier adopción de medidas, sobre todo instrumentales, deberá considerar los argumentos de los opositores para evitar incorporar un régimen jurídico policial que menoscabe nuestros derechos fundamentales a través de ingerencias excesivas y, por lo tanto, ilegítimas.