Apreciaciones generales sobre los delitos informáticos

Claudio Patricio Ossa Rojas.
Abogado/ Director Académico de la Asociación de Derecho e Informática de Chile (ADI).

I.- Introducción

La revolución que han significado las innovaciones tecnológicas recientes han revelado la incapacidad experimentada por las normas establecidas por el Derecho Penal tradicional. Este conjunto de normas punitivas han visto superada su capacidad para enfrentar la aparición de numerosas conductas disvaliosas impensadas en otras épocas. El fenómeno descrito dejó al descubierto la necesidad de realizar un proceso de adaptación de los sistemas normativos, los que han debido crear las correspondientes figuras típicas para incriminar las conductas de reciente aparición.

La informática si bien ha servido de puente comunicador entre los avances tecnológicos y el acceso masivo a las diversas fuentes de información, trajo aparejada la aparición de nuevas formas de delinquir y, a su vez, ha permitido el perfeccionamiento de las ya existentes. Los sujetos activos de esta modalidad de delincuencia se han caracterizado por recurrir al uso instrumental de ordenadores para cometer sus fechorías y actualmente han diversificado sus medios de comisión a través de las redes telemáticas,(1) que interconectan estos dispositivos.

De acuerdo a lo expuesto anteriormente, consideramos que la aparición de estas nuevas conductas ilícitas abarcan las acciones tendientes a atacar bienes propiamente informáticos, entendiéndose por tales los que sólo tienen la posibilidad de existir en un entorno informático, como también los ataques a bienes no propiamente informáticos, mediante el uso de la tecnología informática.

Nos previene Téllez que para intentar una definición de este tipo de delincuencia denominada comúnmente como “delitos informáticos”, es necesario tener en cuenta que ello “no es labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de “delitos” en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión “delitos informáticos” esté consignada en los Códigos Penales” y precisa al respecto que de acuerdo a este análisis se pueden distinguir una definición típica y otra atípica para estas conductas:

“son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin “ (Concepto Atípico)
“conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin” (Concepto Típico).(2)

Así las cosas podríamos definir en un sentido genérico al delito informático como cualquier conducta ilegal, no ética o no autorizada atentatoria tanto contra bienes propiamente informáticos como tradicionales, que se realice mediante el uso y/o la aplicación de tecnologías informáticas.

En atención a lo anterior, es necesario estudiar las conductas que se desarrollan en relación a estos delitos por los sujetos activos de éstos, con el fin de determinar un posible marco legislativo que las regule, otorgando la necesaria seguridad y resguardo que demanda la sociedad actual.

II.- Descripción de los comportamientos de los sujetos activos y sus distintas manifestaciones.

Para hacer un estudio sistemático de las conductas que se relacionan con los delitos informáticos, distinguiremos diversos grupos de sujetos activos, los que delimitaremos de acuerdo a los medios y las formas utilizadas por estos para su ejecución. Así, podemos distinguir las siguientes conductas:

1.- Phreaking.
2.- Hacking.
3.- Trashing.
4.- Atentados contra la Propiedad Intelectual.

A continuación, pasaremos a revisar cada una de ellas brevemente.

1.- Phreaking.

Consiste en el acceso no autorizado a sistemas telefónicos para obtener gratuidad en el uso de las líneas, con el objeto de lograr conexión mantenida por esta vía a las redes informáticas, ya sean nacionales o internacionales.

Esta conducta, se relaciona con los delitos informáticos a través del ataque de los phreakers hacia sistemas de telefonía, los que si son considerados en su conjunto, pueden fácilmente llegar a comprometer la funcionalidad de los más grandes sistemas de telecomunicaciones coordinados a través de redes de ordenadores, los que, a través de la utilización de softwares especializados manejan las comunicaciones que se desarrollan por esta vía. Sin embargo, esta conducta no es nueva, ya que fue practicada desde los inicios de la telefonía, pero el ataque en ese entonces, apuntaba al quebrantamiento de sistemas de carácter analógico y no digital, y por consiguiente no podría relacionarse con delitos informáticos.

Dentro de las actuales manifestaciones de phreaking podríamos distinguir:

a) Shoulder-surfing: esta conducta se realiza por el agente mediante la observación del código secreto de acceso telefónico que pertenece a su potencial víctima, el cual lo obtiene al momento en que ella lo utiliza, sin que la víctima pueda percatarse de que está siendo observada por este

sujeto quien, posteriormente, aprovechará esa información para beneficiarse con el uso del servicio telefónico ajeno.

b) Call-sell operations: el accionar del sujeto activo consiste en presentar un código identificador de usuario que no le pertenece y carga el costo de la llamada a la cuenta de la víctima. Esta acción aprovecha la especial vulnerabilidad de los teléfonos celulares y principalmente ha sido aprovechada a nivel internacional por los traficantes de drogas(3)

c) Diverting: consiste en la penetración ilícita a centrales telefónicas privadas, utilizando éstas para la realización de llamadas de larga distancia que se cargan posteriormente al dueño de la central a la que se ingresó clandestinamente. La conducta se realiza atacando a empresas que registren un alto volumen de tráfico de llamadas telefónicas, con el fin de hacer más difícil su detección.

d) Acceso no autorizado a sistemas de correos de voz: el agente ataca por esta vía las máquinas destinadas a realizar el almacenamiento de mensajes telefónicos destinados al conocimiento exclusivo de los usuarios suscriptores del servicio. A través de esta conducta el sujeto activo puede perseguir diversos objetivos:

d.1) Utilizar los códigos de transferencia de mensajería automática manejados por el sistema.
d.2) Lograr el conocimiento ilícito de la información recibida y grabada por el sistema.

e) Monitoreo pasivo: por medio de esta conducta el agente intercepta ondas radiales para tener acceso a información transmitida por las frecuencias utilizadas por los teléfonos inalámbricos y los celulares.

2.- Hacking.

Esta conducta se refiere al acceso no autorizado que realiza el sujeto activo a un sistema de información atentando contra el sistema de seguridad que este tenga establecido. La finalidad del actuar del agente (Hacker) puede ser diversa, ya que buscará a través de ella conocer, alterar o destruir la información contenida en el sistema ya sea parcial o totalmente.

Frente a este grupo de sujetos, la doctrina ha postulado dos posiciones:
- Posición mítica: considera a estos sujetos como individuos de corta edad, por lo general adolescentes de posición social media, aparentemente inofensivos, ausentes de toda conciencia de estar obrando mal, a menudo sugestionados por el síndrome de “Robin Hood” y con un coeficiente intelectual muy alto. Su personalidad presenta la característica particular de ser inestable. Su figura cobró importancia a raíz del intrusismo en sistemas de información que en un comienzo realizaron adolescentes norteamericanos y europeos, los que, en un afán lúdico ingresaban a sistemas de información para luego huir sin causar mayores daños. Lamentablemente, las conductas observadas por estos sujetos fueron convirtiéndose paulatinamente en actividades muy riesgosas, tanto para los sistemas como para la seguridad interna y externa de los países en que actuaban, ya que muchas veces sus jugarretas pusieron

en graves aprietos a sistemas altamente sofisticados, produciendo efectos negativos en distintos lugares del planeta, debido a la posibilidad de desplazamiento con que contaban a través de las redes informáticas.

- Posición realista: incorpora a los sujetos considerados por la posición mítica, pero agrega a otros sujetos que, si bien no poseen avanzados conocimientos tecnológicos relativos a la informática, pueden realizar conductas propias de la delincuencia informática. Esta apreciación vino a poner de manifiesto que, los casos más serios de delincuencia informática, podían ser llevados a cabo por sujetos que trabajan en el mundo de la informática, de edades superiores a los míticos hackers inicialmente descubiertos y que no presentan ni la mitad de inteligencia que se les atribuía a estos. Entre estos sujetos se ha incluido además a aquellos que no necesariamente desempeñan sus labores en entidades relacionadas con sistemas informáticos, pero que ingresan a ellos de un modo irregular.

El resultado de las consideraciones aportadas por quienes sustentan esta posición realista ha permitido la inclusión dentro de los hackers de los sujetos conocidos como insiders, que son aquellos individuos que acceden sin autorización a un sistema de información que les es muy cercano debido a una relación laboral, actual o reciente, que les ha permitido el conocimiento de las formas posibles para realizar los ataques que estimen convenientes logrando el ingreso libremente, con la finalidad de utilizar la información contenida por el sistema para fines propios.

3.- Trashing.

Esta conducta tiene la particularidad de haber sido considerada recientemente en relación a los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas. Estas acciones corresponden a una desviación del procedimiento conocido como reingeniería social.

Estas actividades pueden tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada.

4.- Atentados contra la propiedad intelectual.

En una primera aproximación, se debe aclarar que bajo el concepto de propiedad intelectual se deben considerar dos aspectos que algunos ordenamientos jurídicos tratan en forma separada. El primero de ellos se regula bajo los conceptos que comprende la Propiedad Industrial, así estas actividades delictivas podrían afectar a la información relativa a la obtención de la protección de derechos de propiedad industrial (marcas, patentes de invención o de procedimientos, diseños industriales y modelos de utilidad), a la manejada durante el correspondiente procedimiento de reconocimiento de estos derechos y a la que tenga relación con estos una vez adquiridos. El

segundo aspecto, comprendido en estas conductas, se refiere al atentado en contra de los derechos autorales, tanto en sus aspectos morales, patrimoniales o mixtos.

III.- Reacciones adoptadas frente al desarrollo de estas conductas.

En un principio, se observa una reacción a nivel privado frente a las primeras manifestaciones de invasión no autorizada por los sujetos agentes de las conductas descritas, procediéndose al fortalecimiento de los mecanismos de seguridad de los sistemas que se vieron afectados, pero simultáneamente se producía de parte de los transgresores un perfeccionamiento en sus técnicas de intromisión lo que, se tradujo en una rápida superación de estas nuevas defensas.

Posteriormente, ante esta realidad se consideró muy necesaria la participación del Estado y sus organismos, para consolidar la adecuada complementación de los mecanismos de seguridad privados con normativas que establecieran una clara regulación y sanción de estas conductas.

Fruto de este esfuerzo mancomunado, se comenzó a observar el nacimiento en distintas partes del mundo de legislación referida a estos tópicos, incorporando las correspondientes figuras típicas introduciéndolas en el Ordenamiento Jurídico respectivo a través de la modificación del Código Penal o creando Leyes Penales Especiales. En este sentido particular trascendencia tendrían en su oportunidad las normativas de Estados Unidos contenidas en la Federal Computer Crime Act (1984) y la Computer Fraud and Abuse Act (1986), y la correspondiente a Gran Bretaña conocida como Computer Misuse Act (1990).

La legislación norteamericana contemplaba expresamente los siguientes comportamientos:
- abuso que afecte a cuestiones de seguridad nacional,
- utilización no autorizada de los sistemas informáticos del Gobierno,
- abuso informático sobre instituciones financieras,
- acceso informático con intención de defraudar, mediante el cual se obtenga cualquier cosa de valor (que no sea el uso del computador),
- acceso que se realice con la intención de alterar, dañar o destruir información contenida en un sistema de información, o para impedir su uso por quien está autorizado para ello, y
- traficar con cualquier código secreto o información similar que afecte al comercio interestatal o a los computadores del Gobierno Federal.

En esta legislación se contemplaban sanciones de multa hasta los US$ 250.000, penas privativas o restrictivas de libertad de hasta 5 años y decomiso del material utilizado en la comisión del delito.

Por su parte, la Ley de Gran Bretaña sancionaba cualquier intento, con éxito o no, de alterar datos informáticos con intención criminal. Estas actuaciones podrían ser penalizadas con hasta 5 años de cárcel, multas y decomiso.

Dentro de nuestra realidad más cercana en Chile, a partir de 1993, se hace un primer intento de regulación de los delitos informáticos a través de la Ley 19.223.En ella se tipificaron las figuras penales relativas a la informática y se contemplaron, a través de sus cuatro artículos, sólo sanciones de presidio las que pueden ir desde los 61 días hasta los cinco años de reclusión. Esta iniciativa, si bien nos parece un avance, consideramos que aún es manifiestamente insuficiente, ya que, a nuestro entender, sería fundamental realizar su complementación con una legislación que no tenga el carácter de reactiva y contemple un mayor número de conductas ilícitas, con la suficiente flexibilidad para permitir su adecuación a los rápidos avances tecnológicos que se observan en este campo. Aquí se debe dejar en claro que, en ningún caso nuestra apreciación apuntaría a generar leyes penales en blanco ya que ello, obviamente, sería improcedente.

IV.-Conclusiones.

El grado de difusión de la informática es, sin lugar a dudas, un factor que determina el origen de nuevas formas delictivas. Nos vemos enfrentados así, con la otra cara de la moneda de los beneficios ampliamente reconocidos que los medios informáticos han aportado al desarrollo de la humanidad. Es así que, el uso generalizado del ordenador por cualquier tipo de persona, aún sin particulares conocimientos técnicos, y la extensión de las redes telemáticas nos seguirán planteando una serie de innumerables desafíos jurídicos ante el perfeccionamiento de las conductas descritas y la aparición de otras nuevas en el futuro cercano. Sobre todas estas posibilidades debiéramos seguir reflexionando y adoptar una serie de determinaciones que nos permitan generar medidas jurídicas preventivas que faciliten disuadir a los potenciales agentes, ya que, tampoco es aconsejable utilizar en forma desmedida la técnica legislativa de recurrir en exceso a herramientas represivas de carácter penal, pues siempre debemos recordar que este es un recurso que debe utilizarse sólo en último término.

Para lograr el objetivo antes señalado deberá tenerse particular atención en el estudio acabado de los agentes de los comportamientos que hemos analizado, pues, se debe rescatar que, muchos de ellos presentan una especial habilidad para la realización de estas conductas ejecutándolas muchas veces a la velocidad del rayo, lo que plantea grandes dificultades para su detección oportuna. Si bien lo anterior podría hacer pensar que lo más aconsejable sería generar normas penales para reprimir estas actividades y así evitar a los órganos del Estado posibles frustraciones ante cualquier intento preventivo o de sanción fallidos, no debe olvidarse que el intento de reinserción social de estos individuos debiera privilegiarse antes que el confinamiento de ellos, ya que, los Estados que no generan políticas de reinserción de quienes delinquen no bajan necesariamente sus índices de delincuencia.4 Adicionalmente, la autoridad política y judicial podría a través de la aplicación de medidas preventivas (por ejemplo: colaboración técnica o delación compensada entre agentes descubiertos con las instituciones policíacas) o de sanciones penales leves, manejar de mejor manera los antecedentes que permitieran reducir la denominada “cifra negra u obscura” respecto de la criminalidad informática, que, es aquella constituida por todas aquellas acciones delictivas que no llegan al conocimiento de las autoridades por falta de acceso a la información adecuada.

En consideración a lo expuesto, es evidente que cada vez se hace más necesaria una detallada regulación jurídica en estas materias, ya que, a través de su adecuada difusión se pueden establecer formas más eficientes de prevención que permitan evitar el aumento de las conductas ilícitas y en caso de fracasar en la implementación y acogida social de estas políticas, que en tal sentido se implementen, debiera en último término recurrirse a las medidas legalmente establecidas que permitan la represión y el castigo más adecuados. Es por ello que, no nos queda más que sostener que, es de suma urgencia incentivar a la sociedad toda, para que ella a través de sus representantes reclame algo que actualmente no se observa, que es ni más ni menos que la Ley debe ponerse al día con la tecnología.

NOTAS

1 Red Telemática: se refiere a la aplicación de la informática en redes de telecomunicaciones. Las redes de conexión pueden ser locales, metropolitanas, nacionales o internacionales.

2 Téllez Valdés, Julio. Derecho Informático. Pág. 103 y 104. Ed. McGraw Hill / Interamericana de México S.A. de C.V. Serie Jurídica. 1996

3 Respalda esta afirmación los asombrosos resultados alcanzados en la Comunidad Autónoma de Cataluña (España) que a través de políticas de reinserción social instauradas en el recinto penal de Cuatre Esquinas tiene índices de reincidencia bajísimos una vez que los delincuentes cumplen sus condenas (menos del 50%) frente a los índices que presenta uno de los recintos penales más modernos del Estado de Nueva York (EEUU) que con mayores recursos económicos pero con políticas de confinamiento más represivas no logra bajar los índices de reincidencia de una forma significativa (reinciden alrededor del 85% de los excarcelados).

BIBLIOGRAFIA.

1.-Ale, Rafael y Cuellar, Fernando. Teleinformática. Editorial McGraw-Hill/Interamericana de España S.A. 1988.

2.-Clough, Bryan y Mungo, Paul. Los Piratas del Chip. La mafia informática al desnudo. Documentos.Ediciones B. Grupo Zeta. Barcelona, España.1992.

3.-Falcon, Enrique.¿Qué es la Informática Jurídica?. Del Ábaco al Derecho Informático. Editorial Abeledo-Perrot. Bs. Aires, Argentina.1992.

4.-Frosini, Vittorio. Informática y Derecho. Editorial Temis S.A. Bogotá, Colombia.1988.

5.-Guerrero M., María Fernanda y Santos M., Jaime Eduardo. Fraude Informático en la Banca. Aspectos Criminológicos. Editorial Jesma. Santafé de Bogotá, Colombia.1993.

6.-Gutiérrez F., María Luz. Fraude Informático y Estafa. Editor Ministerio de Justicia de España. Secretaría General Técnica. Centro de Publicaciones. Madrid, España.1991.

7.-Jijena L., Renato. Chile, la protección penal de la intimidad y el delito informático. Editorial Jurídica de Chile.1992.

8.-Ossa R., Claudio P. Incidencia de los medios informáticos en la comisión de delitos. Ponencia presentada en el Primer Congreso Nacional de Estudiantes de Derecho "Nuevos desafíos del Derecho Penal".Concepción, Chile.9 al 11 de Septiembre de 1994.

9.-Ossa R., Claudio P. y Valenzuela A., Carolina:

9.1.-La problemática de la privacidad en torno al manejo de la información en bases de datos computacionales. Ponencia presentada al VI Congreso Nacional y Latinoamericano de Derecho Penal y Criminología. Córdoba, Argentina.9 al 12 de Septiembre de 1993.

9.2-Breves consideraciones acerca de las relaciones existentes entre el Derecho de Autor, las Bases de Datos y el Derecho a la Privacidad. Trabajo Ganador del Primer Premio del "Concurso Internacional para Estudiantes de las Cátedras de Derecho de Autor de Universidades de Países Latinoamericanos", organizado por el Instituto Interamericano de Derecho de Autor. Santiago de Chile. Julio de 1995.

9.3.-Las Bases de Datos: Un Arma Silenciosa que puede afectar gravemente determinados Derechos Humanos. Ponencia presentada en el VI Congreso Latinoamericano Universitario de Derecho Penal y Criminología. Tucumán, Argentina.26 al 29 de Mayo de 1994.

10.-Ossa R., Claudio P. y Reimberg N., Frank. Delitos Informáticos: una aproximación al estudio psicológico de determinados segmentos etáreos. Ponencia presentada al VI Congreso Latinoamericano Universitario de Derecho Penal y Criminología. Tucumán, Argentina.26 al 29 de Mayo de 1994.
11.-Shallis, Michael. El Ídolo de Silicio. La revolución de la informática y sus implicaciones sociales. Biblioteca Científica Salvat N° 29.Salvat Editores S.A. Barcelona, España.1986.
12..-Sterling, Bruce. The Hacker Crackdown. Edición Electrónica de circulación libre por INTERNET. Copyright Bruce Sterling.1992-1994.
13.- Téllez Valdés, Julio. Derecho Informático. Pág. 103 y 104. Ed. McGraw Hill / Interamericana de México S.A. de C.V. Serie Jurídica. 1996