CAPÍTULO 4

"(...) ladrón, trabajaba para otros: ladrones más adinerados, patrones que proveían el exótico software requerido para atravesar los muros brillantes de los sistemas empresariales, abriendo ventanas hacia los ricos campos de la información. Cometió el clásico error, el que había jurado no cometer nunca. Robo a sus jefes."

Neuromante

DELITOS INFORMÁTICOS

Ya hemos dejado en claro la importancia de la información en el mundo altamente tecnificado de hoy. También se ha dejado en claro cada uno de los riesgos "naturales" con los que se enfrenta nuestro conocimiento y la forma de enfrentarlos.

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La cuantía de los perjuicios así ocasionados es a menudo muy superior a la usual en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrirse o castigarse.

Es propósito de los capítulos siguientes disertar sobre los riesgos "no naturales"; es decir los que se encuadran en el marco del delito. Para ello deberemos dejar en claro, nuevamente, algunos aspectos.

4.1 LA INFORMACIÓN Y EL DELITO

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, 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 jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún."[1]

En 1983, la Organización e Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin e luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas"[2].

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define **Delito Informático** como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos."[3]

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma"[4].

[1] TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996 Pág. 103–104

[2] MOLINER, María. Diccionario de María Moliner Edición Digital. Copyright© 1996 Novel Inc.; Copyright© 1996 María Moliner.

[3] Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.

[4] CARRION, Hugo Daniel. Tesis "Presupuestos para la Punibilidad del Hacking". Julio 2001. w*ww.delitosinformáticos.com/tesis.htm*

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

1. En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.
2. La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

En este punto debe hacerse un punto y notar lo siguiente:

- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.
- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.
- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.
- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.
- La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

Julio Téllez Valdez clasifica a los delitos informáticos en base a dos criterios:

1. Como instrumento o medio: se tienen a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

   Ejemplos:

   - Falsificación de documentos vía computarizada: tarjetas de créditos, cheques, etc.
   - Variación de la situación contable.
   - Planeamiento y simulación de delitos convencionales como robo, homicidio y fraude.
   - Alteración el funcionamiento normal de un sistema mediante la introducción de código extraño al mismo: virus, bombas lógicas, etc.
   - Intervención de líneas de comunicación de datos o teleprocesos.

2. Como fin u objetivo: se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

   Ejemplos:

- Instrucciones que producen un bloqueo parcial o total del sistema.
- Destrucción de programas por cualquier método.
- Atentado físico contra la computadora, sus accesorios o sus medios de comunicación.
- Secuestro de soportes magnéticos con información valiosa, para ser utilizada con fines delictivos.

Este mismo autor sostiene que las acciones delictivas informáticas presentan las siguiente características:

1. Sólo una determinada cantidad de personas (con conocimientos técnicos por encima de lo normal) pueden llegar a cometerlos.
2. Son conductas criminales del tipo "cuello blanco": no de acuerdo al interés protegido (como en los delitos convencionales) sino de acuerdo al sujeto que los comete. Generalmente este sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional.
3. Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado se encuentra trabajando.
4. Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante.
5. Provocan pérdidas económicas.
6. Ofrecen posibilidades de tiempo y espacio.
7. Son muchos los casos y pocas las denuncias, y todo ello por la falta de regulación y por miedo al descrédito de la organización atacada.
8. Presentan grandes dificultades para su comprobación, por su carácter técnico.
9. Tienden a proliferar, por lo se requiere su urgente regulación legal.

María Luz Lima, por su parte, presenta la siguiente clasificación de "delitos electrónicos"[5]:

1. Como Método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
2. Como Medio: conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.
3. Como Fin: conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

4.2 TIPOS DE DELITOS INFORMÁTICOS

La Organización de Naciones Unidas (ONU) reconocen los siguientes tipos de delitos informáticos:

[5] LIMA de la LUZ, María. Criminalia N° 1–6 Año L. Delitos Electrónicos. Ediciones Porrua. México. Enero–Julio 1984.

1. Fraudes cometidos mediante manipulación de computadoras
    - Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.
    - La manipulación de programas: consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación.
    - Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude del que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.
    - Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Se basa en el principio de que 10,66 es igual a 10,65 pasando 0,01 centavos a la cuenta del ladrón n veces.
2. Manipulación de los datos de entrada
    - Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.
    - Como instrumento: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.
3. Daños o modificaciones de programas o datos computarizados
    - Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
    - Acceso no a autorizado a servicios y sistemas informáticos: estos acceso se pueden realizar por diversos motivos, desde la simple curiosidad hasta el sabotaje o espionaje informático.
    - Reproducción no autorizada de programas informáticos de protección legal: esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, se considera, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Adicionalmente a estos tipos de delitos reconocidos, el XV Congreso Internacional de Derecho ha propuesto todas las formas de conductas lesivas de la que puede ser objeto la información. Ellas son:

- “Fraude en el campo de la informática.
- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados o programas informáticos.
- Acceso no autorizado.
- Intercepción sin autorización.
- Reproducción no autorizada de un programa informático protegido.
- Espionaje informático.
- Uso no autorizado de una computadora.
- Tráfico de claves informáticas obtenidas por medio ilícito.
- Distribución de virus o programas delictivos.”[6]

4.3 DELINCUENTE Y VICTIMA

4.3.1 SUJETO ACTIVO

Se llama así a **las personas que cometen los delitos informáticos**. Son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que “entra” en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos en la materia los han catalogado como delitos de “cuello blanco” término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

La “cifra negra” es muy alta; no es fácil descubrirlos ni sancionarlos, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad. A los

[6] CARRION, Hugo Daniel. Tesis “Presupuestos para la Punibilidad del Hacking”. Julio 2001. w*ww.delitosinformáticos.com/tesis.htm*

sujetos que cometen este tipo de delitos no se considera delincuentes, no se los segrega, no se los desprecia, ni se los desvaloriza; por el contrario, es considerado y se considera a sí mismo "respetable". Estos tipos de delitos, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

4.3.2 SUJETO PASIVO

Este, **la víctima del delito**, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los delitos informáticos, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos.

Es imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra negra".

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

En el mismo sentido, podemos decir que con:

1. la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras;
2. alertas a las potenciales víctimas, para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática;
3. creación de una adecuada legislación que proteja los intereses de las víctimas;
4. una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas;

se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos, se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

4.4 LEGISLACIÓN NACIONAL

En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político–jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales e internacionales.

La ONU señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y los delitos informáticos se constituyen en una forma de crimen transnacional.

En este sentido habrá que recurrir a aquellos tratados internacionales de los que nuestro país es parte y que, en virtud del Artículo 75 inc. 22 de la Constitución Nacional reformada en 1994, tienen rango constitucional.

Argentina también es parte del acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio, que en su artículo 10, relativo a los programas de ordenador y compilaciones de datos, establece que:

- este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna, de julio 1971, para la Protección de Obras Literarias y Artísticas;
- las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual y que;
- para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que, "los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias"[7].

La Convención sobre la Propiedad Intelectual de Estocolmo (julio de 1967) y el Convenio de Berna (julio de 1971) fueron ratificados en nuestro país por la Ley 22.195 el 17 de marzo de 1980 y el 8 de julio de 1990 respectivamente.

La Convención para la Protección y Producción de Phonogramas de octubre de 1971**,** fue ratificada por la ley 19.963 el 23 de noviembre 1972.

La Convención Relativa a la Distribución de Programas y Señales de abril de 1994, fue ratificada por la ley 24.425 el 23 de diciembre de 1994.

Hay otros Convenios no ratificados aún por nuestro País, realizados por la Organización Mundial de la Propiedad Intelectual (OMPI)**,** de la que Argentina es parte integrante a partir del 8 de octubre de 1980.

Nuestra legislación regula Comercial y Penalmente las conductas ilícitas relacionadas con la informática, pero que aún no contemplan en sí los delitos informáticos:

1. La ley 111 de Patentes de Invención regula la protección a la propiedad intelectual.

[7] Artículo 61, Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas.

2. La ley Penal 11.723 de “Propiedad Científica, Literaria y Artística”, modificada por el decreto 165/94, ha modificado los Artículos 71, 72, 72 bis, 73 y 74 (ver Anexo I).

Por esta ley, en el país sólo están protegidos los lenguajes de bases de datos, planillas de cálculo, el software y su documentación dentro del mismo.

Si bien, en el decreto de 1994, se realizó la modificación justamente para incluir esos ítem en el concepto de propiedad intelectual, no tiene en cuenta la posibilidad de plagio ya que no hay jurisprudencia que permita establecer qué porcentaje de igualdad en la escritura de dos programas se considera plagio. Las copias ilegales de software también son penalizadas, pero por reglamentaciones comerciales.

A diferencia de otros países, en la Argentina la información no es un bien o propiedad, por lo tanto no es posible que sea robada, modificada o destruida.

De acuerdo con los art. 1072 y 2311 del Código Civil y 183 del Código Penal se especifica que para que exista robo o hurto debe afectarse una “cosa” y las leyes definen “cosa” como algo que ocupa lugar en el espacio; los datos, se sabe, son intangibles.

En resumen: si alguien destruye, mediante los métodos que sean, la información almacenada en una computadora no cometió delito; pero si rompió el hardware o un disquete será penalizado: en ese caso, deberá hacerse cargo de los costos de cada elemento pero no de lo que contenían. También se especifica (art. 1109) que el damnificado no podrá reclamar indemnización si hubiera existido negligencia de su parte.

Ahora, cabe preguntarse ¿En Argentina, qué amparo judicial se tiene ante hechos electrónicos ilícitos?. La respuesta es que el Código Penal argentino (con 77 años de vida) no tiene reglas específicas sobre los delitos cometidos a través de computadoras. Esto es así porque cuando se sancionaron las leyes no existía la tecnología actual y por lo tanto no fueron previstos los ataques actuales.

Dentro del Código Penal se encuentran sanciones respecto de los delitos contra el honor (art. 109 a 117); instigación a cometer delito (art. 209), instigación al suicidio (art. 83); hurto (art. 162), estafas (art. 172), además de los de defraudación, falsificación, tráfico de menores, narcotráfico, etc., todas conductas que pueden ser cometidas utilizando como medio la tecnología electrónica, pero nada referente a delitos cometidos **sobre** la información como bien.

El mayor inconveniente es que no hay forma de determinar fehacientemente cuál era el estado anterior de los datos, puesto que la información en estado digital es fácilmente adulterable. Por otro lado, aunque fuera posible determinar el estado anterior, sería difícil determinar el valor que dicha información tenía.

El problema surge en que los datos almacenados tienen el valor que el cliente o “dueño” de esos datos le asigna (y que razonablemente forma parte de su patrimonio). Esto, desde el punto de vista legal es algo totalmente subjetivo. Son bienes intangibles, donde solo el cliente puede valorar los “unos y ceros” almacenados.

Así, las acciones comunes de hurto, robo, daño, falsificación, etc. (art. 162 del Código Penal) que hablan de un apoderamiento material NO pueden aplicarse a los datos almacenados por considerarlos intangibles.

Hablar de estafa (contemplada en el art. 172 del código penal) no es aplicable a una máquina porque se la concibe como algo que no es susceptible de caer en error, todo lo contrario a la mente humana.

En función del código penal, se considera que entrar en un domicilio sin permiso o violar correspondencia constituyen delitos (art. 153). Pero el acceso a una computadora, red de computadoras o medios de transmisión de la información (violando un cable coaxil por ejemplo) sin autorización, en forma directa o remota, no constituyen un acto penable por la justicia, aunque sí el daño del mismo.

La mayor dificultad es cuantificar el delito informático. Estos pueden ser muy variados: reducir la capacidad informativa de un sistema con un virus o un caballo de Troya, saturar el correo electrónico de un proveedor con infinidad de mensajes, etc. Pero ¿Cuál de ellos es mas grave?.

Si se considera Internet, el problema se vuelve aún más grave ya que se caracteriza por ser algo completamente descentralizado. Desde el punto de vista del usuario esto constituye un beneficio, puesto que no tiene ningún control ni necesita autorización para acceder a los datos. Sin embargo, constituye un problema desde el punto de vista legal. Principalmente porque la leyes penales son aplicables territorialmente y no puede pasar las barreras de los países.

La facilidad de comunicación entre diversos países que brinda la telemática dificulta la sanción de leyes claras y eficaces para castigar las intrusiones computacionales.

Si ocurre un hecho delictivo por medio del ingreso a varias páginas de un sitio distribuidas por distintos países: ¿Qué juez será el competente en la causa?. ¿Hasta qué punto se pueden regular los delitos a través de Internet sabiendo que no se puede aplicar las leyes en forma extraterritorial?.

Ver una pantalla con información, ¿Es un robo?. Ante esta pregunta Julio C. Ardita[8] responde "(...) si, desde el punto de vista del propietario, si es información confidencial y/o personal es delito porque se violó su privacidad".

Si un intruso salta de un satélite canadiense a una computadora en Taiwan y de allí a otra alemana ¿Con las leyes de qué país se juzgará?.

Lo mencionado hasta aquí no da buenas perspectivas para la seguridad de los usuarios (amparo legal) en cuanto a los datos que almacenan. Pero esto no es tan así, puesto que si la información es confidencial la misma tendrá, en algún momento, amparo legal.

Por lo pronto, en febrero de 1997 se sancionó la ley 24.766 (ver Anexo I) por la que se protege la información confidencial a través de acciones penales y civiles, considerando información confidencial aquella que cumple los siguientes puntos:

[8] ARDITA, Julio César. Director de Cybsec S.A. Security System y ex–Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. *http://www.cybsec.com*

- Es secreta en el sentido que no sea generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información.
- Tenga valor comercial para ser secreta.
- Se hayan tomado medidas necesarias para mantenerla secreta, tomadas por la persona que legítimamente la controla.

Por medio de esta ley la sustracción de disquetes, acceso sin autorización a una red o computadora que contenga información confidencial será sancionado a través de la pena de violación de secretos.

En cuanto a la actividad típica de los hackers, las leyes castigan el hurto de energía eléctrica y de líneas telefónicas, aunque no es fácil de determinar la comisión del delito. La dificultad radica en establecer dónde se cometió el delito y quién es el damnificado.

Los posibles hechos de hacking se encuadran en la categoría de delitos comunes como defraudaciones, estafas o abuso de confianza, y la existencia de una computadora no modifica el castigo impuesto por la ley.

La División Computación de la Policía Federal no realiza acciones o investigaciones preventivas (a modo de las organizaciones estadounidenses) actúa en un aspecto pericial cuando el operativo ya está en marcha.

Este vacío en la legislación argentina se agrava debido a que las empresas que sufren ataques no los difunden por miedo a perder el prestigio y principalmente porque no existen conceptos claros para definir nuevas leyes jurídicas en función de los avances tecnológicos.

Estos problemas afectan mucho a la evolución del campo informático de la argentina, generando malestar en empresas, usuarios finales y toda persona que utilice una computadora como medio para realizar o potenciar una tarea. Los mismos se sienten desprotegidos por la ley ante cualquier acto delictivo.

Como conclusión, desde el punto de vista **social**, es conveniente educar y enseñar la correcta utilización de todas las herramientas informáticas, impartiendo conocimientos específicos acerca de las conductas prohibidas; no solo con el afán de protegerse, sino para evitar convertirse en un agente de dispersión que contribuya, por ejemplo, a que un virus informático siga extendiéndose y alcance una computadora en la que, debido a su entorno crítico, produzca un daño realmente grave e irreparable.

Desde la óptica **legal**, y ante la inexistencia de normas que tipifiquen los delitos cometidos a través de la computadora, es necesario y muy importante que la ley contemple accesos ilegales a las redes como a sus medios de transmisión. Una futura reforma debería prohibir toda clase de acceso no autorizado a un sistema informático, como lo hacen las leyes de Chile, Francia, Estados Unidos, Alemania, Austria, etc.

Lo paradójico (¿gracioso?) es que no existe sanción legal para la persona que destruye información almacenada en un soporte, pero si para la que destruye la misma información impresa sobre papel.

No obstante, existen en el Congreso Nacional diversos proyectos de ley que contemplan esta temática (ver Anexo II).

4.5 LEGISLACIÓN INTERNACIONAL

4.5.1 ALEMANIA

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica. Esta ley reforma el Código Penal (art. 148 del 22 de diciembre de 1987) para contemplar los siguientes delitos:

- Espionaje de datos (202a).
- Estafa informática (263a).
- Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).
- Alteración de datos (303a) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
- Sabotaje informático (303b).
- Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b).
- Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita. Esta solución fue también adoptada en los Países Escandinavos y en Austria.

4.5.2 AUSTRIA

Según la Ley de reforma del Código Penal del 22 de diciembre de 1987, se contemplan los siguientes delitos:

- Destrucción de datos (art. 126) no solo datos personales sino también los no personales y los programas.
- Estafa informática (art. 148) se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

4.5.3 CHILE

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La ley 19223 publicada en el Diario Oficial (equivalente del Boletín Oficial argentino) el 7 de junio de 1993 señala que la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco.

Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años.

El hacking, definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito.

Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años. Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.

4.5.4 CHINA

El Tribunal Supremo Chino castigará con la **pena de muerte** el espionaje desde Internet, según se anunció el 23 de enero de 2001.

Todas las personas "implicadas en actividades de espionaje", es decir que "roben, descubran, compren o divulguen secretos de Estado" desde la red podrán ser condenadas con penas que van de diez años de prisión hasta la muerte. ¿Castigo ejemplar?.

La corte determina que hay tres tipos de actividades donde la vigilancia será extrema: secretos de alta seguridad, los secretos estatales y aquella información que dañe seriamente la seguridad estatal y sus intereses. Se consideran actividades ilegales la infiltración de documentos relacionados con el Estado, la defensa, las tecnologías de punta, o la difusión de virus informático.

El Tribunal ha hecho especial énfasis al apartado del espionaje desde la red. A los llamados "criminales", además de tener asegurada una severa condena (la muerte), también se les puede... ¡confiscar los bienes!.

4.5.5 ESPAÑA

Este país quizás sea el que mayor experiencia ha obtenido en casos de delitos informáticos, en Europa.

Su actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP) aprobada el 15 de diciembre de 1999, la cual reemplaza una veintena de leyes anteriores de la misma índole, contempla la mayor cantidad de acciones lesivas sobre la información.

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el phreacking, la introducción de virus, etc.; aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos.

Así mismo su nuevo Código Penal establece castigos de prisión y multas "a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

4.5.6 Estado Unidos de América

El primer abuso de una computadora se registró en 1958 mientras que recién en 1966 se llevó adelante el primer proceso por la alteración de datos de un banco de Mineapolis. En la primera mitad de la década del 70, mientras los especialistas y criminólogos discutían si el delito informático era el resultado de una nueva tecnología o un tema específico, los ataques computacionales se hicieron más frecuentes. Para acelerar las comunicaciones, enlazar compañías, centros de investigación y transferir datos, las redes debían (y deben) ser accesibles, por eso el Pentágono, la OTAN, las universidades, la NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos.

Pero en 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985

Esta ley fue la base para que Florida, Michigan, Colorado, Rhode Island y Arizona se constituyeran en los primeros estados con legislación específica, anticipándose un año al dictado de la Computer Fraud y Abuse Act de 1986.

Este se refiere en su mayor parte a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero sólo es aplicable en casos en los que se verifiquen daños cuyo valor supere el mínimo de mil dólares.

En 1994 se adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986. Aquí se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos.

Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

El aumento en la cantidad de casos de hacking y la sensación de inseguridad permanente que generaron (fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas), cambiaron la percepción de las

autoridades con respecto a los hackers y sus ataques. Los casos que demostraron ese cambio fueron los del "Cóndor" Kevin Mitnicky y los de "ShadowHawk" Herbert Zinn hijo (ver Anexo II).

El FCIC (Federal Computers Investigation Commitee), es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente. El FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

Además existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias. Sus integrantes son "forenses de las computadoras" y trabajan, además de los Estados Unidos, en el Canadá, Taiwán e Irlanda.

4.5.7 FRANCIA

Aquí, la Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

- Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje Informático. Falsear el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

4.5.8 HOLANDA

Hasta el día 1 de marzo de 1993, día en que entró en vigencia la Ley de Delitos Informáticos, Holanda era un paraíso para los hackers. Esta ley contempla con artículos específicos sobre técnicas de Hacking y Phreacking.

El mero hecho de entrar en una computadora en la cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis meses de cárcel. Si se usó esa computadora hackeada para acceder a otra, la pena sube a cuatro años aunque el crimen, a simple vista, no parece ser peor que el anterior. Copiar archivos de la máquina hackeada o procesar datos en ella también conlleva un castigo de cuatro años en la cárcel. Publicar la información obtenida es ilegal si son datos que debían permanecer en secreto, pero si son de interés público es legal.

El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis meses a quince años, aunque el máximo está reservado para quienes causaron la muerte de alguien con su accionar. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos años de prisión pero, si se hizo vía remota aumenta a cuatro.

Los virus están considerados de manera especial en la ley. Si se distribuyen con la intención de causar problemas, el castigo puede llegar hasta los cuatro años de cárcel; si simplemente se "escapó", la pena no superará el mes.

El usar el servicio telefónico mediante un truco técnico (Phreacking) o pasando señales falsas con el objetivo de no pagarlo puede recibir hasta tres años de prisión. La venta de elementos que permitan el Phreaking se castiga con un año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo aumenta a tres. La ingeniería social también es castigada con hasta tres años de cárcel.

Recibir datos del aire es legal (transmisiones satelitales), siempre y cuando no haga falta un esfuerzo especial para conseguirlos; la declaración protege datos encriptados, como los de ciertos canales de televisión satelital. Falsificar tarjetas de crédito de banca electrónica y usarlas para obtener beneficios o como si fueran las originales está penado con hasta seis años. Aunque... hacerlas y no usarlas parece ser legal.

4.5.9 INGLATERRA

Luego de varios casos de hacking surgieron nuevas leyes sobre delitos informáticos. En agosto de 1990 comenzó a regir la Computer Misuse Act (Ley de Abusos Informáticos) por la cual cualquier intento, exitoso o no de alterar datos informáticos con intención criminal se castiga con hasta cinco años de cárcel o multas sin límite.

El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas.

El acta se puede considerar dividida en tres partes: hackear (ingresar sin permiso en una computadora), hacer algo con la computadora hackeada y realizar alguna modificación no autorizada.

El último apartado se refiere tanto al hacking (por ejemplo, la modificación de un programa para instalar un backdoor), la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del funcionamiento de la computadora.

Bajo esta ley liberar un virus es delito y en enero de 1993 hubo un raid contra el grupo de creadores de virus. Se produjeron varios arrestos en la que fue considerada la primera prueba de la nueva ley en un entorno real.

4.6 CONCLUSIÓN

Legislar la instigación al delito cometido a través de la computadora. Adherirnos, por nuestra parte, a los postulados de la ONU sobre los delitos informáticos, con el fin de unificar la legislación internacional que regule la problemática de la cibernética y su utilización tan generalizada en el mundo.

Desde la Criminología debemos señalar que el anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados, son un factor criminógeno que favorece la multiplicación de autores que utilicen los medios electrónicos para cometer delitos a sabiendas que no serán alcanzados por la ley.

No solo debe pensarse en la forma de castigo, sino algo mucho más importante como lograr probar el delito. Este sigue siendo el principal inconveniente a la hora de legislar por el carácter intangible de la información.

"Al final, la gente se dará cuenta de que no tiene ningún sentido escribir leyes específicas para la tecnología. El fraude es el fraude, se realice mediante el correo postal, el teléfono o Internet. Un delito no es más o menos delito si se utilizó criptografía (...). Y el chantaje no es mejor o peor si se utilizaron virus informáticos o fotos comprometedoras, a la antigua usanza. Las buenas leyes son escritas para ser independientes de la tecnología. En un mundo donde la tecnología avanza mucho más deprisa que las sesiones del Congreso, eso es lo único que puede funcionar hoy en día. Mejores y más rápidos mecanismos de legislación, juicios y sentencias...quizás algún día."[9].

[9] SCHNEIER, Bruce. Secrets & Lies. Página 28–29.

DELITOS INFORMÁTICOS 1

4.1 LA INFORMACIÓN Y EL DELITO 2

4.2 TIPOS DE DELITOS INFORMÁTICOS 4

4.3 DELINCUENTE Y VICTIMA 6

4.3.1 Sujeto Activo 6

4.3.2 Sujeto Pasivo 7

4.4 LEGISLACIÓN NACIONAL 8

4.5 LEGISLACIÓN INTERNACIONAL 12

4.5.1 Alemania 12

4.5.2 Austria 12

4.5.3 Chile 13

4.5.4 China 13

4.5.5 España 13

4.5.6 Estado Unidos de América 14

4.5.7 Francia 15

4.5.8 Holanda 15

4.5.9 Inglaterra 16

4.6 CONCLUSIÓN 16