UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
CARRERA DERECHO

MONOGRAFIA

"LA NECESIDAD DE MODIFICAR LOS ARTÍCULOS 363 bis. Y ter. DEL CÓDIGO PENAL REFERENTE A LOS DELITOS INFORMÁTICOS"

POSTULANTE: RICARDO CHUQUIMIA FLORES

TUTORA: Dra. KARINA INGRID MEDINACELI DIAZ

LA PAZ – BOLIVIA
2011

AGRADECIMIENTOS

A MÍ QUERIDA MADRE:
Norah Flores Quisbert
Gracias por darme la vida,
Por quién soy y por enseñarme,
Los valores y principios que necesito
para la vida y lograr mis objetivos.

A NUESTRA UNIVERSIDAD Y
FACULTAD DE DERECHO:
“Con toda gratitud”

"LA NECESIDAD DE MODIFICAR LOS ARTÍCULOS 363 bis. Y ter. DEL CÓDIGO PENAL REFERENTE A LOS DELITOS INFORMÁTICOS"

CAPITULADO

INTRODUCCIÓN.

En nuestros días, el uso de la tecnología informática sin duda ha traído grandes beneficios en el desarrollo de todas las actividades del hombre facilitándonos a través de una computadora muchas de nuestras tareas tales como transacciones o préstamos en instituciones financieras, la consulta de bibliotecas enteras en todo el mundo, el guardar información personal, la celebración de contratos informáticos, el uso de diversos medios de comunicación como la telefonía inalámbrica y celular, o simplemente el uso de la computadora como medio de entrenamiento.

Sin embargo, la delincuencia también ha hecho uso de todos los medios informáticos para alcanzar sus fines ilícitos, constituyéndose en lo que muchos han llamado la delincuencia informática, utilizando las computadoras para cometer fraudes, robos, abusos de confianza, fraudes financieros, extorsiones, falsificaciones, amenazas y una gran variedad de ilícitos nuevos.

Esta es la problemática que enfrenta actualmente nuestra legislación y esa también es motivo de nuestra investigación que pretenderá hacer conocer la necesidad de que nuestro ordenamiento jurídico se ponga a la par de estos Delitos Informáticos para una adecuada regulación de los mismos.

Es por todo aquello que en el Capitulo Primero analizaremos todos los conceptos, características y clasificaciones que diferentes autores dieron a los Delitos Informáticos.

En el Capítulo Segundo se pretende llevar a cabo una descripción del delincuente informático así como también de los diferentes ilícitos informáticos existentes.

En el Capitulo Tercero veremos todos los esfuerzos que se hacen a nivel internacional como en nuestro país para poder combatir adecuadamente este

nuevo fenómeno delictivo, en virtud de que esta problemática afecta a todo el mundo.

Por ultimo en el Capitulo Cuarto se destacaran propuestas acerca de cómo combatir adecuadamente en nuestro país a los delitos informáticos.

No cabe duda que lo novedoso y cada vez más avanzado de los Delitos Informáticos requiere de también innovaciones para su tratamiento en todos los sentidos tanto desde el aspecto técnico investigativo, como el jurídico, siendo éste último campo el que se concentra esta investigación.

CAPITULO I

LOS DELITOS INFORMATICOS

El progreso tecnológico que ha experimentado la sociedad, supone una evolución en las formas de infringir la ley, dando lugar, tanto a las diversificaciones de los delitos tradicionales como la aparición de nuevos actos ilícitos. Esta situación ha motivado un debate en torno a la necesidad de diferenciar o no los delitos informáticos del resto y de definir su tratamiento dentro del marco legal.

1.1. CONCEPTO Y DEFINICION DE DELITOS INFORMATICOS

Davara Rodríguez (2008: 350), define al Delito informático como:

> *La realizaciónn de una acción que, reuniendo las características que delimitan el concepto dedelito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware y software.*

Julio Téllez Valdés (2004: 163) conceptualiza al delito informático en forma típica y atípica, entendiendo que en la forma típica son:

> *Las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y la forma atípica actitudes ilícitas en que se tienen a las computadoras como instrumento o fin.*

El Convenio de Cyber-Delincuencia del Consejo de Europa de fecha *23.XI.2001*, define a los delitos informáticos como

> *Los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos.*

Conviene destacar entonces, que diferentes autores y organismos han manifestado diferentes apreciaciones para señalar las conductas ilícitas en las que se utiliza la computadora, esto es "delitos informáticos", "delitos electrónicos",

"delitos relacionados con la computadora", "crímenes por computadora", "delincuencia relacionada con el computador". Tal como podemos notar en las definiciones establecidas por autores anteriores, no existe una definición de carácter universal propia de delito informático, sin embargo, debemos resaltar que han sido los esfuerzos de especialistas que se han ocupado del tema y han expuesto conceptos prácticos y modernos atendiendo entornos nacionales concretos, pudiendo encasillar parte de los temas en esta área de la criminalística. Es preciso señalar que la última definición brindada por el Convenio de Cyber-delincuencia del Consejo de Europa anota especial cuidado en los pilares de la seguridad de la información: la confidencialidad, integridad y disponibilidad.

El delito informático involucra acciones criminales que en primera instancia los países han tratado de poner en figuras típicas, tales como: robo, fraudes, falsificaciones, estafa, sabotaje, entre otros, por ello, es primordial mencionar que el uso indebido de las computadoras es lo que ha creado la necesidad imperante de establecer regulaciones por parte de la legislación.

1.2. CARACTERISTICAS DEL DELITO INFORMATICO.

De acuerdo a las características que menciona en su libro Derecho Informático el Dr. Julio Téllez Valdés (2004: 163), en donde se podrá observar el modo de operar de estos ilícitos:

- Son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

- Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.
- Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada

o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

- Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.
- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- En su mayoría son imprudenciales y no necesariamente se cometen con intención. Ofrecen facilidades para su comisión a los mentores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

El autor español Davara Rodríguez (2008: 361-363), establece que este tipo de delitos al ser cometidos por medios informáticos o telemáticos y tener estos unas características especiales, los delitos informáticos poseen peculiaridades que les hacen de alguna manera "sui generis" en cuanto a la forma de ser cometidos y en cuanto a la detección de los mismos, llegando en algunos casos, prácticamente imposible descubrir el beneficio producto de du actividad ilícita. Enunciaremos como propias y especiales de este tipo de acciones ilícitas, y comunes a todas ellas, las siguientes características:

1. **Rapidez y acercamiento, en tiempo y espacio, su comisión**.
   La facilidades en el tratamiento y proceso de la información, con la posibilidad de realizar programas que actúen retardados o controlados en el tiempo,

aprovechando las funciones del sistema operativo del ordenador, que permite "activar" o "desactivar" determinadas ordenes de la maquina, de esta dinámica, incluso flexible, dependiendo de una u otro circunstancia prevista de antemano, así como la utilización de las comunicaciones para poder, en tiempo real o fuera del alcance o control del operador del computador, actuar en la forma deseada, permiten preparar acciones dolosas en perjuicio de otro, en tiempo y espacio distantes.

Estos delitos pueden ser realizados por una persona que se encuentra distante del lugar donde son cometidos, y llevando a cabo una actividad diferente e incompatible con los mismos en el momento que son ejecutados.

Debido al acercamiento en espacio que proporcionan las comunicaciones y a la posibilidad de actuación sobre los programas que pueden ser activados para actuar en un momento retardado, incluso meses, del momento en que se preparo la acción, se puede lograr que la persona que lo haya realizado se encuentre lejos y como ya hemos indicado, en una actividad incompatible con la realización del ilícito.

Es esta una característica que dificulta, en múltiples ocasiones, la localización de la actividad y su relación con los hechos, llegando incluso a ocultar al verdadero impulsor y al que realiza la acción.

2. **Facilidad para encubrir el hecho.**

Esas mismas facilidades enunciadas en el apartado anterior, y su utilización en la comisión del delito, ofrecen unas condiciones optimas para encubrir el hecho.

Es posible modificar, por ejemplo, un programa para que realiza una actividad ilícita en beneficio del autor y establecer una rutina software que vuelva a modificar el programa, en forma automática, una vez realizado el hecho dejándole tal y como se encontraba al principio.

De esta forma, ni visualmente, ni con el análisis del programa, ni con el estudio del proceso, seria posible detectar lo que ha ocurrido y como ha sido

cometida. Pero como el resultado será la producción de un beneficio para su autor y un perjuicio para otro, es posible que no se pueda nunca comprobar que el hecho producido ha sido uno de los ilícitos que hemos considerado como delito informático.

De otra parte, es difícil vincular ala persona que ha cometido el hecho con el mismo, y su relación causa y efecto que podría dar como resultado su implicación y responsabilidad penal. A ello hay que añadir la falta de especialización en esta materia y la necesidad de profesionales que pudieran incluso mediante la preparación de actividades informáticas que fueran determinando en espacios de tiempo las funciones realizadas por el computador a modo de "trampas" tratar los programas en la definición y localización de procedimientos atípicos.

3. **Facilidad para borrar las pruebas.**

   Existe una gran facilidad para borrar todas las pruebas que hace prácticamente imposible detectar la acción cometida.

   Esta facilidad proviene, a veces, de la pertenencia del delincuente a la plantilla profesional de la empresa en la que se encuentra el computador con el que se ha cometido el delito y ello facilita la actuación, con carácter incluso "profesional" en el borrado de las pruebas.

   En ocasiones, debido a la flexibilidad y dinámica propia del procesamiento informático, que permite detectar una determinada actividad o proceso con posterioridad a su realización, y en otras ocasiones, debido a la facilidad para hacer desaparecer en forma fraudulenta, por medio de la manipulación de programas y datos incluso a distancia las actividades, operaciones, cálculos, o procesos que han sido efectuados.

   De otra parte, las pruebas que se pudieran conseguir en estos aspectos, estarían en muchas ocasiones en soporte magnético o basadas en actividades informáticas o telemáticas, con todas las dificultades, ya conocidas, de originalidad y validez de los documentos obtenidos por medios electrónicos,

o que se encuentren en soportes magnéticos susceptibles de tratamiento automatizado.

Son estas tres características especiales en la comisión de un delito informático, las que inducen a pensar en la necesidad de un tratamiento autónomo que estudie, legisle e investigue en forma independiente, en la que se incluya, las acciones delictivas cometidas por medios informáticos, y su implicancia con otras ya definidas y estudiadas en el Derecho penal, por sus particularidades y características realmente diferentes e independientes.

1.3. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

A continuación se detallara las diversas clasificaciones que han dado expertos en la materia sobre el Delito Informático, así como la que se ha formulado en materia informática aplicada a estos ilícitos:

Téllez Valdés (2004: 165-167), clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio y como fin u objetivo.

1. Como instrumento o medio: en esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.).

d) Lectura, sustracción o copiado de información confidencial.

e) Modificación de datos tanto en la entrada como en la salida.

f) Aprovechamiento indebido o violación de un código para penetrar a un

sistema introduciendo instrucciones inapropiadas.

g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

h) Uso no autorizado de programas de computo.

i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.

l) Acceso a áreas informatizadas en forma no autorizada.

m) Intervención en las líneas de comunicación de datos o teleproceso.

2. Como fin u objetivo: en esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a los dispositivos de almacenamiento.

d) Atentado físico contra la máquina o sus accesorios.

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

El Dr. Miguel-Ángel Davara Rodríguez (2008: 352-360), autor español clasifica a los Delitos Informáticos de la siguiente manera:

a) Acceso y manipulación de datos y
b) Manipulación de los programas.

Atendiendo a ello, considera que determinadas acciones que se podrían encuadrar dentro de lo que hemos llamado el delito informático, y que para su estudio, las clasifica, de acuerdo con el fin que persiguen, en seis apartados:

1. Manipulación en los datos e informaciones contenidas en los archivos y soportes físicos informatices ajenos.

La manipulación, de cualquier tipo o en cualquier forma, de los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos, se dará para poder encuadrarla en este apartado, cuando se persiga obtener un beneficio económico o de otro tipo para la persona que la realiza, o para que se realiza y en perjuicio de otro.

Lógicamente, sin estar autorizado para ello, suprimiéndolos o modificándolos, destruyéndolos o inutilizándolos o en algunos casos, no incidiendo sobre ellos y dejándolos tal y como están pero inutilizándolos para otras actividades que realicen distinto proceso y se logre con ello un beneficio injusto para el delincuente y un perjuicio determinado para un tercero.

La manipulación de los datos puede ser cometida en cuatro faces diferentes:

a) Almacenamiento de los datos.
b) Procesamiento de los datos.
c) Retroalimentación (feedback) con resultados intermedios a los otros.
d) Transmisión de los resultados del proceso, ya sea en el mismo ordenador a ficheros distintos ya sea por comunicaciones o acceso periféricos en los que se depositan.

2. Acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello.

El acceso, mal intencionado o no, de buna persona no autorizada, a los datos que se encuentran en soportes informáticos, se esta produciendo, cada ves mas, motivado por la falta de seguridad de los sistemas y de formación de las personas que en ellos operan, facilitando mas, si cabe, por las modernas técnicas de comunicación que permiten el conocimiento, manejo y transferencia de información entre sistemas, con máximas garantías y mínimo riesgo. –en el tema que tratamos, solamente tiene interés el acceso mal intencionado, como por ejemplo, obteniendo una lista de clientes o resultados de un competidor o conociendo la información que un tercero procesa o envía por medios telemáticos, o la información que simplemente almacena, mediante el acceso a sus ordenadores o archivos informáticos, ya sea por medios de comunicaciones, ya sea por la introducción de programas, en el ordenador del afectado, que realicen una copia de otros programas o de resultados de proceso o de investigación.

En este tipo de delitos podría estar clasificado en lo que denominaríamos "*espionaje industrial"* si lo que se lo que se logra el acceso por medios informáticos, es el conocimiento de secretos industriales o actuaciones de la competencia, con los que conseguir un beneficio para el delincuente y en perjuicio de otro.

3. Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas.

En ocasiones, se realiza esta acción sin que se pueda determinar ni su origen, ni su autoría, ni lo que es mas triste, su finalidad. La introducción de programas, o partes de programas e incluso solamente de unas instrucciones que al ser ejecutadas producen un efecto perjudicial para el titular de los datos e información almacenada puede traer consecuencias de difícil estimación y perjuicios irreparables para el

titular de los datos, de los programas o del sistema. Es, sin duda, una intromisión, ilegitima, en un derecho básico del titular.

Este es el caso de los conocidos "*virus informáticos",* consistentes en rutinas, instrucciones o partes de programas que se introducen a través de un soporte físico que los contiene, o través de la red de comunicaciones, actuando en el momento, o con efecto retardado y destruyendo datos, información o programas y en ocasiones, toda la información contenida en el computador.

4. Utilización del ordenador y/o los programas de otras persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro.

Nuevamente pueden intervenir en la realización de acción dolosa las comunicaciones para acceder a los datos y permitir la utilización de los programas y computadores de otra persona o en otro caso, se lograra mediante el abuso de la confianza depositada en alguien que, bajo una relación laboral o amistosa, tiene acceso a la utilización de programas o computador, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro, ya sea en el domicilio de la sociedad o empresa, o accediendo a distancia por medio de las telecomunicación o mediante lo que sea dado a llamar el *hurto de tiempo.*

Este es el caso de determinados empleados de instalaciones informáticas, que utilizan los programas y el computador de su empresa para realizar trabajos de servicios a terceros con un evidente lucro para ambos y en perjuicio de la empresa titular de los computadores y programas.

5. Utilización del ordenador con fines fraudulentos

Las posibilidades de tratamiento de la información por medios mecanizados, así como la potencia y velocidad de los cálculos que en los computadores se puede realizar, permiten disponer de un elemento óptimo para la manipulación fraudulenta de datos, con la realización de complejos cálculos e, incluso, la posibilidad de enmascaramiento de información.

La utilización de nuestro propio computador para defraudaciones, e incluso para ofrecer servicio de defraudaciones, como puede ser el enmascaramiento de datos cálculos complejos para eludir obligaciones fiscales, escondiendo información y otras muchas cuya relación no viene al caso, convierten a esta actividad en una de las mas que se realiza, a veces sin ser detectada, par la comisión de delitos por medios informáticos.

6. Agresión a la "privacidad" mediante la utilización y procesamiento de datos personales con fin distinto al autorizado.

La potencial agresividad a la intimidad de la persona y a su propia imagen, o a la denominada privacidad, mediante la utilización y procesamiento de datos personales que se tiene legalmente para un fin determinado utilizándolos para un fin distinto de aquel para el que se está autorizado, así como la utilización del resultado del proceso y nuevo tratamiento automatizado de esos datos personales con fines y para actividades distintas de las que justificaron su obtención y almacenamiento.

El autor Nacional José Alfredo Arce Jofré (2003: 147-148) clasifica los Delitos Informáticos de cuerdo *al medio* y *al fin.* Para poder encuadrar una acción dolosa o culposa dentro de este tipo de delitos, *el medio* por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática y telemática, y *el fin* que se persiga deba ser la producción de un beneficio al sujeto o autor del ilícito; una finalidad deseada que causa un perjuicio a otro, o a un tercero.

En ese sentido encontramos que los delitos informáticos pueden ser tan nuevos tipos penales introducidos en el Código Penal, cual es el caso del los artículos 363 bis y ter y los delitos cometidos con ayuda de las computadoras con relación a tipos penales ya existentes.

Sobre lo expuesto hace la siguiente clasificación:

Delitos contra el sistema: Aquí la computadora y la información es el objeto del delito. Se puede atacar:

- Hardware: es el soporte físico, las maquinas en si mismas.
- Software: es el soporte lógico, constituido por los programas que permiten a las computadoras cumplir con sus funciones.

Delitos mediante el sistema: La computadora es el instrumento para cometer el delito. Así pues se puede lesionar los siguientes bienes jurídicos:

- Patrimonio
- Privacidad
- Seguridad supra-individual

Desde otro tipo de enfoque, podemos hacer la siguiente clasificación:

a) Desde el punto de vista subjetivo.- ponen el énfasis en la pretendida peculiaridad de los delincuentes que realizan estos supuesto de criminalidad.

b) Desde un punto de vista objetivo.- Considerando los daños económicos perpetrados por las conductas criminalistas sobre los bienes informáticos.

c) Los fraudes.- Manipulaciones contra los sistemas de procesamiento de datos, donde citar:

- Los daños engañosos (Data diddling)
- Los "Caballos de Troya" (Toya Horses)
- La técnica de salami (Salami technique/Rounching Down

d) El sabotaje informático:

- Bombas Lógicas (Logic Bombs)
- Virus Informáticos

e) El espionaje informático y el robo o hurto de software:

- Fuga de datos (Data Leakage)

f) El robo de servicios:

- Hurto del tiempo del ordenador.
- Apropiación de información residuales (Scavenging)
- Parasitismo informático (Piggybacking)
- Suplantación de personalidad (impersonation)

g) El acceso no autorizado a servicios informáticos:

- Las puertas falsas (Trap Doors)
- La llave maestra (Superzapping)
- Pinchado de líneas (Wiretapping)

La insuficiencia de los planteamientos subjetivos y objetivos han aconsejado primar otros aspectos que puedan resultar más decisivos para delimitar la criminalidad informática.

Atentados contra la fase de entrada (input) o de salida (output) del sistema, a su programación, elaboración, procesamiento de datos y comunicación telemática.

1.4. SUJETOS DEL DELITO INFORMATICO.

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así , el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo.

1.4.1. SUJETO ACTIVO.

El sujeto activo es aquel individuo que comete el ilícito en agravio de la victima o sujeto pasivo. Para algunos doctrinarios los delitos informáticos pueden considerarse como delitos de "cuello blanco", entendiéndose por tales aquellas conductas delictivas perpetradas por gente con un estatus socioeconómico elevado y con preparación técnica o profesional en alguna ciencia. En efecto determinados ilícitos como el *hacking* requieren de un conocimiento especial en materia de informática, sin embargo, con la masificación de los servicios informáticos en línea, tales como los servicios gubernamentales, prácticamente cualquier persona puede accesar y utilizar con relativa facilidad servicios de telecomunicaciones y navegar en el ciberespacio donde se pueden obtener sin mayor restricción sofisticadas herramientas de programación para cometer voluntaria e involuntariamente, determinados delitos, situación que incide en el creciente numero d ataque llevados a cabo por legos o personas inexpertas.

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.

1.4.2. SUJETO PASIVO.

Por lo que toca a los sujetos pasivos de los delitos informáticos, cualquier usuario o prestador de servicios informáticos puede ser victima de los mismos.

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.

En primer término tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias y gobiernos que usan sistemas automatizados de información, generalmente conectados a otros (Idem: 149).

1.5. BIEN JURIDICO PROTEGIDO.

A partir de los avances tecnológicos, se está configurando, a nivel internacional, un nuevo bien jurídico, "la Información". Los derechos a manejar la información y a preservar una esfera de intimidad tienen su fundamento en la propia naturaleza del ser humano, por ello constituyen derechos fundamentales, que deben ser garantizados y regulados. La información es el contenido de los mensajes transmitidos por la informática; sin embargo, la evolución tecnológica, el almacenamiento, el tratamiento, y la transmisión de datos mediante sistemas de procesamiento, le ha dado un nuevo significado y valor, concediendo a su poseedor una ventajosa situación respecto a los demás. Se menciona con frecuencia el dicho "la información es poder"; esto quiere decir que quien sepa más tiene más ventajas frente a los otros. El derecho a la información se remonta al periodismo. La materia

del derecho de la información: el dato o conocimiento es un bien que puede ser objeto de regulación jurídica.

Probablemente, el plantear la información como un bien jurídico susceptible de amparo hace algunos años hubiera sido objeto de controversia, empero, actualmente las sociedades están más que nunca comprometidas con el fenómeno informático y ello conlleva la necesidad de su defensa, si deseamos un país preparado para recibir el desarrollo. Esto se logrará otorgándole a la información el valor económico, que le corresponde. Si pretendemos justificar la urgencia de una tutela adecuada, ésta debe derivarse del fracaso o ausencia de otros medios (Ricardo M. Mata y Martín, 2001: 150).

Bolivia, en efecto, carece de una legislación preventiva apropiada, cuenta tan sólo con un capítulo sobre delitos informáticos, ubicado en el Código Penal, compuesto por dos artículos, cuya información es muy general, y el Decreto Reglamentario de Software que, en cierta manera, revisa lo que son programas de ordenador y bases de datos pero cuya protección se centra en los derechos de autor correspondientes a los creadores de programas de software. La presencia en nuestro ordenamiento de estas normas es un avance; sin embargo para abordar la problemática socio jurídica originada por la presencia de la informática. Ahora bien, por su carácter transnacional, estos delitos están en nuestra realidad nacional. Por esto, el derecho penal debe ser copartícipe de la evolución mediante la confección de leyes específicas capaces de regular este ámbito.

1.6. EXTRATERRITORIALIDAD.

En el ámbito internacional, los efectos del crimen informático son transfronterizos; nos referimos a, lo que es delito en un país puede no serlo en otro. Esto con lleva un problema respecto a la competencia jurisdiccional, que obliga al derecho internacional dar solución a estos conflictos, determinando cuál es el

derecho aplicable en los casos de infracciones de este tipo y cuál es la jurisdicción competente. Una de las características que nos trae esta era de la información es que no hay límites de tiempo ni espacio.

Esta extraterritorialidad de los actos lesivos y la dificultad de encuadramiento personal de los sujetos activos presenta un cuadro difícil de resolver en la mayoría de las situaciones prácticas, a lo que debe agregarse la casi imposibilidad de identificar a los transgresores en forma fehaciente durante sus actividades en la red.

Por otro lado, pero no por ello de menor importancia, es el hecho de que existen conductas posibles on line y off line, ya que de unas pueden derivar las otras.

Pues bien, toda esta intrincada red de conductas lesivas y su posible protección penal, debe ser analizada por partes para su comprensión exhaustiva y para evitar la creación de normas que pudieren resultar perfectas en teoría pero totalmente inútiles en la práctica.

No es este un tema menor, ya que la posibilidad de incompetencia de los jueces, la imposibilidad de extradición, la garantía del juez natural reconocida por los tratados internacionales de derechos humanos y otras anexas, como el debido proceso y el in dubio pro reo, presentan límites infranqueables para una legislación que no haya sido debidamente planificada en función de todas y cada una de ellas para otorgar una protección efectiva a los damnificados y cumplir la función preventiva de que se nutre el derecho penal.

Es claro que si los posibles infractores comprenden las imposibilidades de aplicación de las normas penales será muy fácil para ellos evadirlas y resultar así en la directa inaplicabilidad del sistema penal.

Todas estas precauciones deben tenerse en cuenta al proponer la protección penal de cualquier conducta en internet o que pueda nacer de su aplicación, pero especialmente en aquellos que devienen en daños directos a los damnificados, ya que la imposibilidad de aplicación deviene en una repetición de conductas que en definitiva perjudican a todo el conjunto social al producir una espiral descendente

en los contenidos de la red, ya que sin una adecuada protección de los derechos involucrados, es claro que en poco tiempo los autores se negarán a exponer sus creaciones en la red por el riesgo que ello implica para sus derechos patrimoniales, como asimismo, la mayoría de los navegantes tomarán en su defensa medidas que pueden resultar en una verdadera ley de la selva o en la venganza privada.

Estos pequeños ejemplos no surgen por cierto de la imaginación del autor del presente, sino en verdad de las experiencias recientes en algunos casos de otros delitos en la red, como el sonado del virus I LOVE YOU que como fue introducido desde Filipinas por un natural de ese país resultó impune cuando los daños causados a la administración y el gobierno de los EEUU resultaron cuantiosos.

Este es un claro ejemplo de que una legislación, por buena que sea puede resultar totalmente inútil si no prevé las implicancias de las nuevas tecnologías en referencia a la ubicación de los autores y su posible o no comparecencia en juicio ante los tribunales competentes para la aplicación de ellas con referencia al caso concreto.

CAPITULO II
LA DELINCUENCIA INFORMÁTICA

En el presente Capítulo se analizarán algunos temas de gran importancia a nivel internacional en torno a los Delitos Informáticos tales como los delincuentes informáticos, las diversas formas de comisión de estos ilícitos y sus medios utilizados para realizarlos.

2.1. EL DELINCUENTE INFORMÁTICO.

En este presente apartado se presentarán los sujetos activos que

intervienen en los Delitos Informáticos e ilícitos cometidos por medios informáticos.

2.1.1. EL HACKER.

El Hacker puede ser definido como un. *"Intruso o Pirata informático",* que en muchas ocasiones pueden ser vistos como los mismos programadores o personas inadaptadas que sólo se dedican a cometer ilícitos con las computadoras, o bien éste término es utilizado para denominar a toda aquella persona, experta en una rama de la informática y las telecomunicaciones como programación, software y hardware, además cuentan con características especiales que detallamos a continuación:

- Su objetivo es adquirir conocimientos para ellos mismos de manera autodidacta.
- Son personas minuciosas con la tecnología, analizándola, descubriéndola hasta dominarla, modificarla y explotarla.
- Se consideran obsesivos y compulsivos por acumular conocimiento y tener lo mejor en la tecnología.
- Poseen un alto nivel de conocimiento informático
- Nunca divulgan los conocimientos obtenidos.
- No existe edad entre los Hackers.
- No tienen gustos en especial, no tienen una vestimenta específica y no siguen un estereotipo de película norteamericana.
- Actúan de manera inadvertida muchas veces consideran a un buen Hacker cuando nunca son atrapados.

El Hacking es la acción realizada por los Hackers para introducirse en sistemas y redes privadas o públicas, con lo que se ha convertido en algo muy común con la extensión de la computadora personal y de la Internet

alrededor de todo el mundo haciendo que una computadora con información vital conectada a Internet sea inseguro, debido a que no existe demasiada información sobre medidas de seguridad por parte del usuario y el poco nivel de conocimiento acerca de medidas de seguridad de los administradores de sitios y servidores, así como el amplio conocimiento de los Hackers para actuar.

El Hacker utiliza agujeros en la seguridad de los protocolos para poder acceder y navegar en Internet, estos protocolos son conocidos como TCP/IP o protocolo de control de transmisión, que se divide en TCP o control de transición, haciendo que se reciba la información transmitiendo la dirección a donde deberá ser enviada según la solicitud del usuario y de mantener el orden de la información y el IP o protocolo de Internet, este último es una forma de identificación de equipos utilizados para la navegación, similar a un número telefónico que permite enviar y recibir información debido a que al dividir en bloques la información almacena la dirección de IP tanto del remitente como del destinatario.

A su vez éstos protocolos se dividen en otros dos que son: el protocolo encargado de la transmisión de datos de equipo a equipo y el protocolo que controlan la administración que permite ver parte de la información mientras ésta se transmite, de los protocolos útiles para conectarse, transferir datos, visitar páginas Web y de interés para un Hacker resaltan: ARP que es el protocolo de resolución de direcciones que convierte las direcciones de Internet en direcciones físicas descifrando las direcciones de IP de cada bloque de información y comprobar si ésta posee la dirección de IP del destinatario correcto según la petición hecha por el usuario evitando que llegue información no solicitada; ICMP o protocolo de mensaje de control de Internet encargado de monitorear el estado del mensaje, así como del estado de quien envía y recibe información; INETD este protocolo sirve para administrar los puertos en caso de que se necesiten realizar dos o más actividades al mismo tiempo y el HTTP utilizado para acceder a páginas Web, una vez siendo utilizados presentan espacios en la seguridad debido a errores en la programación de los programas legítimos, el mal uso de los protocolos o la navegación en Internet.

Otra forma que un Hacker pueda conocer estos protocolos es mediante los COOKIES, estos poseen una buena intención debido a que un usuario entra a una página y envía una solicitud para poder acceder a ella y ésta a su vez otorga o no autorización para el acceso y utiliza los Cookies para almacenar la información de los protocolos algo así como una tarjeta de datos para la transmisión de información de ambas partes con el fin de que en un futuro al ingresar de nuevo en la misma página no se tenga que hacer de nuevo todo el proceso de verificación y aceptación. El problema radica que muchos Hackers crean páginas señuelos con interés para el usuario el cual utilizan la excusa de los Cookies para obtener esta información o incluso más información confidencial sin que el usuario pueda darse cuenta con el fin de encontrar victimas para estudiar y encontrar brechas en la seguridad de los usuarios.

Una vez obtenida esta información el Hacker ingresa a la computadora investigando el tipo de software al que se enfrenta y el equipo en el que se encuentra, una vez adentro del sistema y conocer el software el Hacker puede entrar como si ya fuera un usuario legítimo o robando las claves de acceso al momento de entrar e intenta obtener los privilegios de un administrador autorizado con el fin de tener acceso a toda la información disponible en el equipo, con el fin de evitar sospechas de existencia de intrusos en el sistema, los Hackers intentan permanecer poco tiempo en ellos al día con lo que un ataque puede llevarse a cabo durante días o sólo tocar los archivos de interés sin acceder un número determinado de archivos que levante sospechas, al terminar para no ser detectado conforme a su dirección de correo electrónico o dirección IP utiliza editores dentro del sistema infiltrado para borrar o cambiar su mismo correo o dirección de IP.

En muchas ocasiones, personas normales se consideran Hackers, pero para entrar a éste selecto grupo de elite informático es necesario un nivel mínimo de conocimientos, aunque sí cualquier persona puede actuar como ellos, de los cuales surgen una sub-especie de Hackers bajo las siguientes denominaciones:

- Lamer: Son personas que no poseen el gran conocimiento de un Hacker aunque tiene un nivel básico para actuar, es un término usado de manera despectiva para este tipo de usuarios, no siguen la sed de conocimiento que un Hacker debe tener, por lo regular sus ataques son por diversión y presumir sus pocas habilidades.

- Wrackers: Son personas dedicadas a descargar programas nocivos como los Shareware o Freeware navegando por Internet, en muchos casos no poseen conocimientos amplios sobre informática y llegan a causar daño sin querer y en otros casos lo hacen sin saber. Se considera una práctica peligrosa debido a que al investigar y descargar programas dañinos para su beneficio muchas veces se encuentra en riesgo de ser atacado por virus o personas.

3.1.2. EL CRACKER.

Son los más peligrosos en el mundo de la informática, en muchos casos son Hackers al mismo tiempo, poseen gran capacidad de programación, amplios conocimientos en criptografías y criptoanálisis. Se dedican a acceder en lugares prohibidos tanto de empresas privadas como gubernamentales para robar, destruir y distribuir programas comerciales pirateados, crean todo tipo de virus para su beneficio e incluso para venderlos a terceros, más para violar derechos de autor que por curiosidad y búsqueda de conocimiento como el Hacker.

Al igual que los Hackers, existen diversos tipos de usuarios que sin ser Crackers son considerados de gran peligrosidad usando el nombre de Crakers y sus técnicas para lograr sus objetivos, entre los cuales están los siguientes:

- Phreaker: Son los usuarios que realizan actividades ilegales para enriquecerse, destruir o actos terroristas contra equipos informáticos, en unos inicios sólo atacan sistemas de telefonía fija o móvil celular, televisión de paga para obtener servicio gratuito mediante tecnología de avanzada comprada o creada por ellos mismos, después se enfocaron en ingresar a sitios bancarios para robar cuentas bancarias y números de tarjetas de crédito, o incluso de crear números de cuentas usando

programas

Originales de las empresas de tarjetas de crédito y siempre son auxiliados con grandes sistemas de cómputo armados por ellos mismos.

- Script-Kiddies: Son personas que se consideran Crackers, pero poseen menores conocimientos que los mismos, presumen de sus conocimientos utilizando programas de terceros para hacer daño que en la mayoría del caso son el reflejo de actos de vandalismo.

- Speaker: Considerado como el máximo espía de la informática; son usuarios con grandes conocimientos y capacidades, son relativamente indetectables debido a que no provocan daño, sólo cuando es realmente necesario, generalmente trabajan para organismos gubernamentales.

- Rider: Son todos los usuarios anteriores que han decidido dejar estas prácticas y trabajar para empresas de seguridad informática, gobiernos y empresas para emplear sus conocimientos y capacidades como especialistas en la seguridad, en el área de delitos informáticos con la policía, además del diseño de programas y protocolos de seguridad (Rodao, Jesús de Marcelo, 2001: 23-35).

2.2. CONDUCTAS DELICTIVAS Y PELIGROSAS EN MEDIOS INFORMÁTICOS.

Durante la creación de la Informática surgieron incidentes inesperados que han cambiado para siempre el rumbo del mundo en esta ciencia, la seguridad y el uso de las computadoras que en muchos casos se utilizaron para bien y en otras se ocuparon para realizar ilícitos y ataques tanto a gobiernos como a particulares. Los Bancos han sido algunas de esas instituciones afectadas que se dieron a conocer, las múltiples ocasiones en las que se han infiltrados en su sistema, lo han negado por obvias razones de imagen financiera.

Estos sujetos activos del los delito Informático, al tener otros conocimientos privilegiados podremos incluirlos en un grupo especial como en el caso de los llamados "delitos de cuello blanco" que son aquellas personas que tienen acceso a

instituciones financieras o gubernamentales y son personas que pueden manejar grandes inversiones. Son conocidos bajo esa terminología ya que son personajes de impecable presentación.

2.2.1. CONDUCTAS PELIGROSAS EN INTERNET.

La Internet como medio masivo de difusión de información ha presentado un sin número de beneficios en todos los campos de la vida humana en cualquier parte del mundo con el simple acceso a una computadora con Internet. de acuerdo a un informe de 2010 de la Unión Internacional de Telecomunicaciones (UIT), el organismo de la ONU encargado de regular las telecomunicaciones globales, Bolivia ocupa el ultimo puesto de de usuarios en América Latina y el Numero 135 a nivel global, con solo 9% de la población (938.354 habitantes), debido, principalmente, a las dificultades de acceso a la tecnología y a los altos costos del servicio que ofrecen los proveedores, aun con estas dificultades, el internet en nuestro país seguirá creciendo de gran manera lógicamente exponiéndose a todos los beneficios y por supuesto a los grandes peligros que ella supone.

Atentados en Internet: Con la extensión de las computadoras personales y la Internet alrededor del mundo, la existencia en los usuarios que interactúan entre sí es inmensa y la cantidad de usuarios continuará creciendo, pero por desgracia cantidad no significa calidad y muchos usuarios no son expertos en el uso de sistemas informáticos, con lo que ha llevado a un serio problema de seguridad, muchos usuarios actúan sin saber lo que se les espera.

En Internet las personas actúan de cierta manera que en sus vidas no lo harían normalmente, gracias al anonimato que otorga éste sistema, con lo que pueden iniciar ataques entre los usuarios, entre los más comunes encontramos los siguientes:

- Guerras en Internet: Estas se llevan a un nivel que el usuario promedio no

podría acceder, se da entre corporaciones, gobiernos y grupos de Hackers o Crackers en mayor escala donde los ataques, herramientas y conocimientos son más sofisticados para lograr el mayor daño posible.

- Ataques de correos: En muchas ocasiones los usuarios intercambian correos entre sí con información variada, pero en ocasiones ésta puede ser intervenida o borrada para no llegar a los destinatarios fijos, otro problema con los correos es el denominado "correo basura o Spam" el cual se dedica a invadir la bandeja de entrada de los usuarios sin que éste se desee, por lo regular de carácter comercial. Otro problema con el correo electrónico son las invasiones realizadas por usuarios mediante miles de correos a la vez mediante programas especializados que pueden saturar una bandeja de entrada.

- Ataques en el Chat: Durante esta actividad popular en Internet muchos usuarios fingen ser otra persona, o siendo ellos mismos agreden verbalmente a otros usuarios pero sin darse cuenta que pueden agredir a Hackers e incluso Crackers que pueden atacar a dicho usuario, e incluso en chats públicos se puede ser víctima de estos usuarios al aceptar archivos como las fotografías gracias a que se han ganando su confianza o incluso al almacenar los datos de usuario y estos al ser obtenidos se encuentran en un nivel de vulnerabilidad muy alto contraataques; incluso pueden contra atacar molestando a los usuarios llenando su computadora de archivos basura bloqueándolos por completo.

- Robo de contraseñas: Se considera un serio problema en el mundo de la Informática debido a que las cosas valiosas son guardadas bajo fuertes mecanismos de seguridad respaldado por contraseñas que las hacen accesibles a sus legítimos dueños, desde acceso a programas en computadoras personales y móviles, correos electrónicos, hasta cuentas bancarias, un Craker realiza ésta acción primero investigando cuál es el programa en el que se desea acceder, una vez encontrado el Craker busca una copia del programa para sí dentro de su equipo para poder trabajar con él, mediante programas especializados probará en él cientos de claves a la vez, si llega a encontrar reacción en una clave en especial la probara, si tiene éxito será usada en el programa legítimo para acceder a él tantas veces

como sea posible, tomando el papel de administrador teniendo libre control de la información

2.2.2. EL VIRUS INFORMÁTICO.

La palabra VIRUS fue utilizada por primera vez por David Gerrolden en su novela *"When Haerlie Was One"*, que en ella describía a una computadora que emulaba al cerebro humano que para conectarse a otras computadoras utilizaba un programa llamado *VIRUS*.

Durante mucho tiempo la palabra virus era usada al igual que en la Biología como con los ordenadores debido a muchas semejanzas entre los dos, que con la popularización de la Informática inició la controversia del uso de éste término, hasta que se generalizó el término V.I.R.U.S que significaba "Recurso de Información Vital Bajo Acoso" *(Vital Information Resources Under Siege)*.

Los virus informáticos son diseñados según las necesidades del usuario y la intención que se posea; muchos de los virus atacan diferentes partes de un equipo informático como: el sector de arranque, procesadores de órdenes, archivos en especial, memoria libre, instrucciones de uso y recursos de Internet (Revista de derecho, comunicaciones y nuevas tecnologías, 2006: 62-64).

Son programas capaces de reproducirse a sí mismos, para atacar sin ser detectado con buenas y malas intenciones, aunque en la actualidad ya existen muchas excepciones, ampliándose a diversos virus y técnicas víricas que a continuación se enlista una pequeña porción de ellos:

- Armouring: Son virus con mecanismos de seguridad para evitar ser detectados o crear dificultades para ser detectados y eliminados, utilizan básicamente técnicas de ocultación.

- Back Door: Es un programa creado por el mismo intruso para introducir gusanos y troyanos creando una brecha en la seguridad oculta tras los programas legítimos o víctimas para poder ser usada tantas veces sea necesario.

- Bomba de Tiempo: Son programas altamente destructivos, creados para ser ejecutados en determinado tiempo o incluso a cierta hora del día, son capaces de destruir e inutilizar equipos, redes y servidores tanto física como lógicamente.

- Bombas Lógicas: Similares a las bombas de tiempo pero para que estas entren en funcionamiento es necesario realizar determinada conducta, una palabra determinada o teclear cierta combinación de teclas, un nivel de espacio en el disco duro o ejecutar un programa en especial.

- Bug-Ware: Son errores provocados por el mal uso de programas legales, los cuales generan ligeros problemas en el que el usuario considera que está infectado por un virus informático al detectar errores en el sistema, que incluso pueden extenderse a otros programas.

- Caballo de Troya: Es la práctica más común en Internet, consiste en un engaño en la que el Hacker crea un programa maligno escondido en programas que a simple vista parecerían inofensivos, por lo regular en archivos de fotografía o música, pero al ingresar en el equipo de la víctima realizan su función incluso sin que éste se diera cuenta sino hasta que es demasiado tarde, por lo regular se encuentran en sitios pornográficos o en programas gratuitos, que al descargar entran en los equipos enviando de regreso información confidencial.

- Camaleón: Son los similares a los Troyanos, son programas malignos disfrazados como otros programas, que por lo general son enviados por correo electrónico.

- Cancelling: Técnica usada para eliminar información de una lista de correos o de noticias.

- Comadronas: Programas encargados de enviar virus de manera automática a equipos informáticos, redes o correos electrónicos.

- Companion: Son virus como troyanos que utilizan los tiempos de inicio de programas, para poder infiltrarse en la información y actuar, ya sea actuando antes de arrancar otro programa, durante la secuencia lógica, durante el uso

o al cierre del sistema.

- Conejos o Pestes: Son programas creados para auto replicarse de manera rápida, capaces de llenar los discos duros y los últimos rincones de memoria, inutilizando redes y saturando bandejas de entrada de correos electrónicos con correo basura.

- Gusanos: Son programas que requieren de un alto nivel de conocimiento para ser creados, no son muy comunes por esta situación, éstos pueden auto replicarse y viajar entre los archivos e incluso entre redes, su funcionamiento requieren en muchos casos que la víctima inicie el gusano, por lo regular son inofensivos, son empleados en muchos casos para difundir mensajes, pero existen los malignos que su función es infiltrarse en redes, derrumbar y colapsar equipos con sus replicas. Entre los gusanos más famosos se encuentran: HYBRIS, I LOVE YOU, LITLEDAVINI y SANTA.

- Joke-Programs: No son considerados propiamente como virus, ya que son unas bromas creadas por los programadores, Hacker y personas comunes, que pueden ser presentadas de tantas formas y sin aviso, son totalmente inofensivos para las víctimas, un ejemplo muy popular son los mensajes que anuncian la destrucción de equipos e información y errores graves en el sistema de los equipos, en muchas ocasiones estos ocultan Gusanos, Troyanos y Bombas.

- Killer: Son virus dedicados a destruir antivirus o vacunas especializadas, desde simplemente borrar el programa, inutilizarlo, borrar la lista de virus a atacar y proteger o eliminar por completo el antivirus, muchos casos son para futuros ataques de otro tipo de virus.

- Leapfrog: Es un programa usando a los gusanos para leer las listas de correo de las víctimas, enviándolo a los programadores.

- Máscaras: Éste requiere de un alto nivel de conocimiento técnico debido que con esta técnica el intruso engaña al sistema adoptando la personalidad de un usuario autorizado aprovechando huecos o fallas en el sistema y protocolos de seguridad robando información o alterando el sistema.

- Macrovirus: Son virus que atacan programas que poseen algún lenguaje de interpretación donde para realizar ciertas funciones, necesitan de instrucciones pre-programadas llamados macros, estos virus alteran estas instrucciones, como las de grabado, apertura e impresión de documentos en procesadores de textos.

- Mockinbird: Son virus inofensivos e inactivos, su función es esperar a que las víctimas ingresen sus claves y contraseñas para copiarlas y enviarlas, aprovecha huecos en la seguridad o en la entrada para actuar pero nunca hacen daño para no ser descubiertos.

- Rebundante: Son virus que cuando se encuentran con otros virus con los mismos objetivos no ataca, pero existen otros que al encontrar otro con las mismas intenciones decide atacar a otros sistemas como el de arranque, pero si uno borra alguno de ellos quedara otro que retomara sus objetivo, siendo de gran peligrosidad.

- Sniffer: Esta técnica es comúnmente utilizada para robar claves de acceso y otros datos de interés que generalmente no causan daño y pasan inadvertidas, pero otros según el intruso pueden ser destructivos.

- Spare: Son virus acompañados de bombas que son detonados con determinada secuencia lógica, capaces de permanecer en los sistemas por meses, pero mientras más permanezca en la computadora inactivo más fácil será detectarlo.

- Spamming: Son programas muy comunes para propaganda comercial y política el cual envía de forma masiva correos a diferentes direcciones de correo electrónico.

- Spiderning: Estos programas son diseñados para viajar por Internet buscando información de un tema determinado.

- Stealth: Es una técnica utilizada por los virus para ocultar todo rastro de operaciones, siendo virus inefectivos debido a que se arriesga a ser detectado por el antivirus al actuar en la memoria, estos funcionan copiando el programa a

atacar y plasmando dicha copia ante el escaneo del antivirus para que éste pase como archivo seguro, mientras el virus ataca el verdadero programa.

- Spare: Son virus acompañados de bombas que son detonados con determinada secuencia lógica, capaces de permanecer en los sistemas por meses, pero mientras más permanezca en la computadora inactivo más fácil será detectarlo.

- Spamming: Son programas muy comunes para propaganda comercial y política el cual envía de forma masiva correos a diferentes direcciones de correo electrónico.

- Spiderning: Estos programas son diseñados para viajar por Internet buscando información de un tema determinado.

- Stealth: Es una técnica utilizada por los virus para ocultar todo rastro de operaciones, siendo virus inefectivos debido a que se arriesga a ser detectado por el antivirus al actuar en la memoria, estos funcionan copiando el programa a atacar y plasmando dicha copia ante el escaneo del antivirus para que éste pase como archivo seguro, mientras el virus ataca el verdadero programa.

- Tunnelling: Es una técnica usada por los virus para evitar los antivirus aprovechándose al colocar falsos puntos para que sean detectados, el antivirus busca en puntos donde se supone debería estar el virus, el cual pasa por donde el antivirus considera seguro.

- Poliformismo: Estos tipos de virus intenta escapar de los antivirus mutando al momento de ser detectado logrando evitar al antivirus, llegaron a ser peligrosos debido a que podían existir miles de mutaciones de un solo virus.

- Xploit: Son programas especializados en escanear programas comerciales aprovechando errores en la programación creando puertas traseras para ser usadas tantas veces como sean necesitadas.

- Variante: Es una técnica usada por el usuario para modificar virus antiguos en su estructura o en pequeños detalles para aparentar un nuevo virus y evitar así su detección.

2.2.3. CONTENIDO PELIGROSO EN INTERNET.

Con los inicios comerciales de la Internet y su expansión en todo el mundo éste se ha convertido en un monumental medio de información y en especial de comunicación, en el que cualquier persona puede publicar todo tipo de contenido, expresar sus ideas y relatar hechos acontecidos, pero no siempre existe veracidad y la calidad en su contenido que se publica ni en lo que se puede llegar a encontrar y leer, ya que otro de los problemas que presenta la Internet es el escaso control en la información que se presenta publicada, ni tampoco del responsable de quien lo hace gracias una vez mas al anonimato, que ofrece este valioso medio, otro problema es el contenido nocivo que se muestra de diversas formas, tanto imagen sonido y video, que sin ser delito atentan contra la privacidad y la moral.

Los contenidos peligrosos en Internet dependen esencialmente de elementos subjetivos inherentes a cada persona, tanto de quien publica como de quien la observa y consulta como ser:

- Drogadicción
- Tabaquismo
- Sexo
- Homicidio
- Violencia
- Alcoholismo.
- Desordenes alimenticios.
- Conspiraciones
- Satanismo y culto a la muerte
- Religión y opiniones de todas las religiones del mundo.
- Suicidio y desensibilización a la muerte.
- Chismes y espectáculos.
- Noticias nacionales e internacionales.

2.2.4. CONDUCTAS DELICTIVAS EN INTERNET.

Con la aparición del Internet, han surgido nuevos delitos y nuevas formas de comisión del delito tradicional tienen que ver determinados aspectos.

2.2.4.1. FRAUDES EN INTERNET.

Con los inicios comerciales de la Internet muchas empresas han visto una oportunidad de éxito, mejorando sus ventas y crecimiento a proporciones inimaginables que sin la Internet hubiera sido difícil de lograr, creando que éste sea un mercado mundial de bienes y servicios accesibles al consumidor, pero este mundo también trae una gran desventaja debido a que muchas empresas con representantes mal intencionados o incluso usuarios aprovechen esta pequeña confianza de la Internet en el ámbito comercial para cometer fraudes, los más usados en este sistema me encontré con las siguientes características:

- Fraudes cometidos en compra-venta y subastas por Internet: Consiste en muchos casos en recibir productos de menor calidad o señalamientos que no fueron expresados al momento de la transacción.

- Engaños cometidos por empresas proveedoras del servicio de Internet: En muchas ocasiones las empresas limitan el uso de la Internet o alteran las velocidades del mismo para pagar más o igual precio al que lo hacían en otras velocidades de descarga sin previo aviso al cliente o limitan las posibilidades de uso al cliente para que éste busque el soporte del proveedor y la misma empresa pueda cobrar más.

- Fraudes en Servicios de Internet: Muchas empresas ofrecen servicios en Internet que siempre son exclusivos a través de este medio, ya sea el uso exclusivo de programas en red, consulta de información y base de datos o el diseño de páginas Web, compra de productos, alquiler de servicios turísticos, médicos o laborales, pero en ocasiones al contratar estos servicios, se puede agregar o incluso

disminuir la calidad y cantidad en el mismo, servicios que no fueron solicitados pero sí son reflejados en el costo, pueden presentarse cargos extras causado por el robo de números de tarjetas de crédito al proporcionarlos al adquirir estos usos, e incluso se puede entrar en un serio riesgo al proporcionar datos personales. Otro caso puede presentarse cuando algunas páginas ofrecen determinado servicio a cambio del número de tarjetas pre-pagadas para Internet o telefonía móvil como medio de pago.

- Fraudes en las oportunidades de negocios: Existen usuarios que crean empresas fantasmas que únicamente existen en Internet y ofrecen oportunidades fáciles de ganar dinero con negocios aparentemente sin pérdidas, constituyéndose en esquemas de inversión exitosos.

- Fraudes telefónicos: En muchas páginas de Internet de gran interés gratuito es necesario que se descarguen programas que supuestamente se conectan mediante el "modem" con la línea telefónica a una red privada pero sin darse cuenta el usuario le da oportunidad de que mediante su línea telefónica realicen llamadas de larga distancia o servicios telefónicos a cargo en la cuenta telefónica.

- Engaño por páginas falsas de Internet: Últimamente con el conocimiento de los usuarios para crear páginas de Internet se ha presentado el engaño para los usuarios presentándole páginas comerciales falsas aprovechándose de la ignorancia de los clientes y el rápido cambio que presenta la Internet, logrando que los usuarios depositen números de cuentas bancarias, números de tarjetas de crédito e incluso datos personales.

- Casinos virtuales: Con el amplio mundo de los videojuegos en Internet existen muchas páginas dedicadas a la estafa de usuarios mediante los casinos virtuales que usando tarjetas de crédito para apostar en un mundo donde el programador tiene las reglas de modificar cada aspecto a su favor para siempre ganar, éstas páginas por lo regular dejan ganar por poco tiempo a los usuarios para ganar

su confianza o incitarlos a apostar grandes cantidades y hacerlos perder, e incluso se encuentra en el peligro del robo de números de tarjetas de crédito.

2.2.4.2. PORNOGRAFÍA INFANTIL.

La pornografía se ha convertido en un negocio lucrativo alrededor del mundo durante muchos años dejando millonarias ganancias tanto a productores, actores y distribuidores, que en muchos casos son negocios lícitos y aceptados en diferentes partes del mundo, son negocios lícitos que con la llegada de la Internet y la libre apertura para publicar cualquier contenido, la circulación y redes pornográficas han venido creciendo de manera desproporcionada, pero dentro de este mundo se presenta un problema mayor aún más serio de resolver que es la pornografía infantil.

La pornografía infantil gracias a la libertad de publicar cualquier contenido, la extraterritorialidad y el relativo anonimato que otorga la Internet se ha convertido en un serio problema en todo el mundo. Las redes de prostitución infantil constituye una industria muy bien organizada y estructurada en diferentes lugares del mundo, aprovechando en muchos casos de la violencia, pobreza, hambre y las permisivas conductas de gobiernos corruptos, pero con la llegada de la Internet este problema que tiene dificultades en ser resuelto se convirtió en un serio problema a nivel internacional y aún más difícil de combatir, ya que no sólo se convirtió en industria privada aislada sino de bandas delictivas bien organizadas entre algunas naciones que conocían la magnitud del problema sin la Internet, sino que cualquier persona con acceso a una computadora, cámara digital, escáner y con acceso a Internet lo ha convertido en un negocio casero al alcance de cualquier persona, apilándose a un ámbito a nivel familiar y pequeña comunidad.

2.2.4.3. CORRUPCIÓN DE MENORES.

Uno de los grandes problemas a superar en la Internet alrededor del mundo es poder limitar el flujo de información lo cual es virtualmente imposible para

cualquier gobierno, debido que en cualquier parte del mundo cualquier persona con una computadora, y acceso a Internet puede realizar cualquier publicación amparado en muchas ocasiones por la libertad de expresión de sus respectivos países, por lo cual ésta información llega a personas incorrectas o no preparadas a los contenidos que aparecen en la internet.

La Internet se ha convertido en un amplio foro de ideas y opiniones alrededor del mundo, así como una enorme biblioteca de información que siempre se encuentra accesible a cualquier hora, siempre que se tenga un acceso a Internet en cualquier parte del mundo, pero por desgracia en muchas ocasiones la información no puede ser verdadera en el mejor de los casos pero en otros el contenido puede ser negativo, gracias a la facilidad que ofrece el uso de una computadora, es asi que los menores e incapaces son un grupo de alta vulnerabilidad al contenido no apto para ellos poniendo en riesgo su desarrollo emocional, psicológico, moral y educativo.

Los menores de edad e incapaces se encuentran desprotegidos de tres tipos de ataques, el primero consiste mediante sitios de conversación o chats públicos en los cuales a falta de administradores responsables permiten que menores y personas con malas intenciones interactúen entre sí, intercambiando ideas y material nocivo, en la actualidad muchos servidores responsables mantiene separada las sala de chats por áreas de edad y se encuentran bajo la supervisión de administradores o incluso hackers experimentados contratados para salvaguardar a los menores, contraatacar y denunciar a personas que no actúen conforme a las reglas estrictas de conducta de determinada sala.

Otro modo de ataque contra los menores e incapaces se producen cuando reciben correos basura o son intervenidos por hackers que envían información con contenido nocivo que en muchas ocasiones son recibidos gracias a deficientes servidores de correo electrónico que no poseen filtros adecuados o antivirus no actualizados para evitar que lleguen mensajes

inapropiados. Por último, el tercer ataque consiste derivado de voluntad de los menores los cuales navegan por Internet y al estar investigando caen en páginas señuelos donde supuestamente poseen contenido de interés para ellos, pero al momento de acceder o durante la navegación de estos sitios encuentran con material nocivo o incluso al realizar la búsqueda de un tema se pueden exponer a grandes volúmenes de información no apropiados para ellos debido que se encuentra ligada una o dos palabras de su búsqueda original, dentro de los temas que se pueden encontrar en Internet resaltan:

- Drogadicción: Sitios en los que señalan técnicas de cultivo de marihuana, como cortar la cocaína o producción de drogas sintéticas; sitios en los que incitan a la drogadicción minimizando daños y riesgos, y sitios en los que enseñan como ocultar los síntomas ante la autoridad, familiares y amigos.

- Comisión de delitos: Sitios en los que incitan a los menores a cometer una amplia gama de delitos por diversión, que indican cómo cometer delitos sin ser supuestamente detenidos o sorprendidos o en los que publican de diversas formas experiencias delictivas por diversión para motivar a otros a realizarlos y estos a su vez los vuelvan a publicar.

- Incitación a la discriminación racial, étnica y económica: Sitios que difunden la discriminación, de sectas religiosas, y grupo sociales que incitan a la discriminación o ataques contra grupos de población.

- Alto contenido violento: Mediante sitios en los que muestran la violencia de guerras o acontecimientos, videos caseros contenidos extremadamente violentos y sangriento.

- Desórdenes alimenticios: Sitios en Internet que fomenta la anorexia o bulimia, mostrando técnicas de cómo inducirse el vomito, cómo conseguir laxantes y medicamentos controlados para el control de peso, dietas y recetas perjudiciales, consejos de cómo evitar a las autoridades, padres, amigos y profesores, proporcionan tablas de peso y medida falsas, proporcionados por falsos médicos

o nutriólogos.

2.2.5. EL TERRORISMO CIBERNÉTICO.

No existe una definición universal de terrorismos internacional, en un sentido general el terrorismo es todo acto encaminado a inducir terror en una población definiendo al Terrorismo como:

> *Actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines político.* (Diccionario de la Lengua Española, 2003)

Sobre el Ciberterrorismo, no existe una definición clara, pero se puede definir como: "*El ciberterrorismo es la acción violenta que infunde terror realizada por una o más personas en internet o a través del uso indebido de tecnologías de comunicaciones"* (Wilson Clay, 2005: 11).

La Internet y las computadoras han demostrado ser una herramienta con inimaginables beneficios pero también de lamentables hechos, lo cual ha traído dos nuevas clases de terrorismo nunca antes vistos en el mundo: el primero es el terrorismo usando como herramienta al Internet y la informática.

2.2.5.1. ATAQUES EN CONTRA DEL ESTADO.

Como ya se ha mencionado todo ataque terrorista tiene por objeto generar terror en una determinada población o hacer que gobiernos, órganos u organismos internacionales cambien sus políticas, alguna característica:

Objetivos.

- Redes del Gobierno y FFAA.
- Servidores de nodos de comunicación.

- Servidores DNS locales.
- Centrales telefónicas locales.
- Estaciones de Radio y televisión.
- Centros satelitales.
- Represas, centrales eléctricas, y centrales nucleares

Tipos de ataques.

- Siembra de virus y gusanos.
- DNS (Cambio de las direcciones de dominio)
- Intrusiones no autorizadas.
- Saturación de correos.
- Bloquear los servicios públicos.
- Interferencia electrónica de comunicaciones.

2.2.5.2. ATAQUES A ENTIDADES FINANCIERAS.

Como ya se pudo apreciar anteriormente un ataque cibernético contra Estados es un problema serio que puede causar parálisis y grandes pérdidas en el funcionamiento del Estado, incluso ser vulnerables a posibles ataques bélicos, y con la expansión de las computadoras e Internet en los sistemas financieros para controlar grandes operaciones y transacciones de negocios que se han convertido en posibles ataques cibernéticos, lo que causaría grandes perdidas económicas a empresas y particulares como causar crisis económicas de escala global.

Los sistemas financieros al igual que un ciber-ataque convencional se puede encontrar bajo diversos tipos de ataques que pueden causar los mismos daños, dentro de los cuales se pueden encontrar:

- Ataque físico y eléctrico de los sistemas financieros: Este al igual

que cualquier ataque convencional se pueden ver afectados sistemas de cómputo tanto en su estructura física como eléctrica, que tenían por objeto almacenar, controlar o administrar información esencial, invaluable y única del sistema financiero; durante los ataques a las torres gemelas cientos de computadoras que almacenaban este tipo de información fueron completamente destruidas con lo que se perdieron millones de dólares en información vital de empresas y particulares.

- Ataques personales a sistemas financieros: Este tipo de ataques son comunes de realizar ya que cualquier empleado o experto en computación con el sistema financiero de la empresa o dependencia en la que trabaje, en sus manos tiene acceso a información vital de las mismas, que puede manipular, alterar, desaparecer o eliminar esta información o mover grandes cantidades de dinero en su propio beneficio o de terceros, que con la transferencia electrónica se realizan todos estos movimientos de manera inmediata lo que facilita la desaparición de grandes sumas o de operaciones en cuestión de segundos.

- Ataques vía Internet a sistemas financieros: Estos ataques son más peligrosos que los anteriores referidos ya que la Internet otorga anonimato para los expertos y facilidad de movilidad desde cualquier parte del mundo, ya que en los anteriores se podría encontrar con relativa facilidad al responsable, la Internet dificulta la forma de localizar al perpetrador y el tipo de ataque causado, pueden ser llevados en segundos sin necesidad de estar físicamente en el lugar donde se encuentren dichos sistemas, simplemente con los conocimientos necesarios, una computadora y acceso a Internet desde la comodidad del hogar pueden cometer este tipo de ataques.

Estas agresiones cibernéticas son realmente peligrosos ya que se controlan grandes cantidades de dinero e información financiera vital que puede cambiar el rumbo de los mercados de cada nación aun cuando éstas no estén controladas por sistemas avanzados de cómputo, ya que con los movimientos adecuados nadie podría darse cuenta de un ligero cambio en las cifras que en el mejor de los casos podría causar pérdidas económicas a particulares o empresas,

pérdida parcial o total de cuentas bancarias, robo en números de tarjetas de crédito en cuestión de segundos, en otros el cambio de información crucial sobre el precio de determinado producto o servicio cotizado en las bolsas de valores de cualquier nación, o incluso causar crisis económicas, devaluaciones, pérdidas de empleo, y duros golpes a cualquier economía emergente alrededor del mundo de la que difícilmente se podrían superar simplemente con presionar un botón del ratón en menos de unos cuantos segundos.

2.2.5.3. ATAQUES A SERVICIOS.

En un mundo cada vez más dependiente de las computadoras y la Internet, el hombre le ha dado cada vez más responsabilidades a las máquinas para mejorar y facilitar su vida diaria, desde éste sistema se ha facilitado el control y la consulta de información para una tarea en la primaria, el control de semáforos, los sistemas de emergencia y suministro de gas, agua y luz, hasta el control de tráfico aéreo, comunicaciones, sistemas de alerta y defensa militar. Con lo que este tipo de computadoras se han convertido en el blanco perfecto de ciber-ataques, al igual que un ataque convencional estas se encuentran vulnerables a un ataque físico, eléctrico, personal y vía Internet. En la que en cuestión de segundos puede generar caos y pánico en una población, paralizando los transportes públicos, aéreos y marítimos, apagando o alterando los sistemas de tránsito como semáforos y vigilancia, inutilizando sistemas de emergencia, o incluso inhabilitando el sistema de flujo de corriente eléctrica de una importante Capital.

No sólo con retrasos y ataques a estos sistemas se han paralizado el transporte, puede poner en riesgo a poblaciones enteras con el cambio en la calidad del agua potable al público, control en la fabricación de productos y en la calidad en los alimentos en sus procesos de producción y procesamiento, incluso causar pérdidas humanas al inutilizar sistemas de emergencia, tanto de comunicación como sistemas de los hospitales. Hasta llegar a la vulnerabilidad total contra ataques militares por otras naciones al dejar

inservibles sistemas de defensa y comunicación militar(Masana, Sebastián. 2002: 12-13).

2.2.5.4. LA SEGURIDAD INFORMÁTICA.

Este concepto abarca todos aquellos pasos y métodos para la protección de datos personales, equipos informáticos, claves personales, protocolos de seguridad, ya que para un usuario le afecta tanto perder información como el propio equipo donde se encuentra la misma o incluso la protección de otros bienes dentro de su patrimonio. Durante los años se ha venido perfeccionando todo lo relacionado a los sistemas de computación, adecuándose máquinas con mayor capacidad, con mayores funciones, más rápidas, más pequeñas, con mayor duración, etc. sin olvidar las diversas formas para recibir, procesar y transmitir la información, creándose para todo ello diversos sistemas de seguridad.

Ahora existen diversos sistemas de cómputo que guardan la información en altos índices de seguridad a lo que se le ha llamado "*encriptar la información*" desgraciadamente los diversos delincuentes informáticos a los que hemos hecho referencia se han encontrado pasos adelante para poder cometer sus conductas delictivas.

CAPITULO III
LA REGULACIÓN INTERNACIONAL Y NACIONAL DEL DELITO INFORMÁTICO

En el presente Capitulo desarrollaremos como los Organismos Internacionales mas importantes, los Estados nacionales y por supuesto el nuestro han creado legislaciones especiales para poder combatir y perseguir estos ilícitos, así como la importancia que cobra la Criminalística y Policía para una adecuada investigación de estos delitos.

3.1. ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU).

La Organización de las Naciones Unidas se ha preocupado por la problemática de los Delitos Informáticos alrededor del mundo y tras minuciosos análisis sociales y jurídicos ha llegado regular algunas conductas al respecto como reconocer algunos ilícitos Informáticos cometidos de manera frecuente dentro de los cuales encontramos los siguientes:

1. FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS

- Manipulación de datos de entrada: Es el delito informático más común, consiste en la sustracción de datos durante el suministro de datos a los sistemas informáticos, requiere niveles mínimos de conocimiento para realizarse.

- Manipulación de programas: Consiste en la alteración de programas genuinos o agregar programas adjuntos que generalmente son virus, ésta técnica requiere de altos niveles en el lenguaje de programación y se presenta en páginas

donde regalan programas que generalmente tienen un costo por su uso.

- Manipulación de datos de salida: Consiste en manipular el sistema para obtener un resultado diferente en el comportamiento del mismo, éste se presenta en la sustracción de dinero de los cajeros automáticos mediante computadoras y decodificadores.

- Fraudes efectuados por manipulación Informática: consiste en manipulación de información, esta técnica se da con frecuencia en la sustracción de dinero de las instituciones financieras, alterando los datos de las cuentas

2. FALSIFICACIONES INFORMÁTICAS.

- Como objeto: Es la alteración de datos en documentos computarizados.

- Como instrumento: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

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. Las técnicas que permiten cometer sabotajes informáticos son:

- Virus: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
- Gusanos: Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.
En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.
- Bombas lógicas o cronológicas: Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

4. FALSIFICACIONES INFORMÁTICAS.

- Acceso no autorizado a servicios y sistemas informáticos: Por motivos

diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

- Piratas Informáticos o Hackers: El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

- 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.

3.2. EL G8. (GRUPO DE LOS OCHO).

Conocido como el grupo de los ocho países más industrializados en el mundo, preocupados por este problema actual, el 11 de mayo de 2004 en Washintong, se realizó la cumbre "sea Island" meeting of G8 Justice and Home Affaire Ministres, reunión de los ministros de asuntos de Justicia y Estado, en el que asistieron Canadá, Francia, Alemania, Italia, Japón y Reino Unido, junto con comisionados de la Unión Europea sobre asuntos de Justicia y Estado en la que sus principales temas a tratar fueron:

1. La Prevención del terrorismo y actos criminales serios.
2. Seguridad fronteriza y de transporte.

3. Combate al ciber-crimen y redoblando esfuerzos en las ciber- investigaciones.
4. Lucha contra la corrupción oficial extranjera y recaptura de activos nacionales robados.

3.3. LA COMISIÓN DE LA COMUNIDADES EUROPEAS.

En el problema de los Delitos Informáticos, la Unión Europea se ha mostrado más unida y a la vanguardia, que se ve reflejado con diversos tratados referentes a esta actual problemática, de los que destacan convenios hechos por el Consejo Europeo (Council of Europe), de los cuales resaltan: El Convenio para la Protección de las Personas Referente al Tratamiento Automático de los Datos de Carácter Personal en 1991 y el Convenio sobre Ciber-criminalidad de 2001, en el cual hay que mencionar.

3.3.1. EL CONVENIO SOBRE LA CIBER-CRIMINALIDAD.

Firmado en Budapest el 23 de Noviembre de 2001, por los países integrantes de la Unión Europea y Estados participantes, en la que emite sus recomendaciones sobre el trato que deberá llevarse frente a los Delitos Informáticos, en el cual sus principales objetivos son:

- Reafirmar la estrecha unión entre las naciones de la Unión Europea y países firmantes para enfrentar la Cibercriminalidad.
- Intensificar la cooperación con los estados miembros.
- Prioridad en unificar una política penal para prevenir la criminalidad en el ciberespacio con una legislación apropiada y mejorar la cooperación internacional.
- Concientizar a los Estados miembros de los cambios suscitados por la convergencia y globalización de las redes.
- Concientizar sobre la preocupación del riesgo de las redes informáticas y

la informática electrónica de ser utilizadas para cometer infracciones penales, ser almacenados y exhibidos.

- Fomentar la cooperación entre los Estados e industrias privadas en la lucha contra la Cibercriminalidad y la necesidad de protección del uso de la Informática para fines legítimos al desarrollo de la tecnología.
- Concientizar que la lucha contra la Criminalidad requiere la cooperación internacional en materia penal asertiva, rápida y eficaz.
- Persuadir sobra la necesidad de un equilibrio entre los intereses de la acción represiva y el respeto de los Derechos del Hombre garantizado en el convenio para la protección de éstos derechos y libertades fundamentales y reafirmar el derecho de no ser perseguido por la opinión pública, la libertad de expresión, libertad de búsqueda y el respeto a la vida privada.
- Complementar los convenios anteriores, relacionados con la materia o que otorguen soporte, con el fin de hacer más efectiva la investigación, procedimientos penales y recolección de pruebas electrónicas.
- Persuadir sobre la necesidad de mantener y proteger la confiabilidad, integridad y disponibilidad de los sistemas de cómputo, bases de datos, computadoras y redes.

De lo convenido dentro de este documento destaca la descripción hecha de las conductas delictivas llevadas por medios informáticos, de aplicación para los Estados miembros de los cuales cabe resaltar los siguientes artículos:

Artículo 1 – **Definiciones**

A los efectos del presente Convenio, la expresión:

a).**"Sistema informático"** designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;

b). **"Datos informáticos"** designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento

informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;

c). **"Prestador de servicio"** designa:

I. Toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático;

II. Cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios;

d). "Datos de tráfico" designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Artículo 2 – Acceso ilícito

Cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para prever *como infracción penal*, conforme a su derecho interno, *el acceso doloso y sin autorización a todo o parte de un sistema informático***.** Las partes podrán exigir que la infracción *sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva*, o también podrán requerir que la infracción *se perpetre en un sistema informático conectado a otro sistema informático.*

Artículo 3 – Interceptación ilícita

Cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para prever *como infracción penal,* conforme a su derecho interno, la *interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos – en transmisiones no públicas– en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos.* Las partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción *se perpetre en un sistema informático conectado a otro sistema informático.*

Artículo 4 – Ataques a la integridad de los datos

1. Cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para prever como *infracción penal,* conforme a su derecho interno, la

conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero *ocasione daños que puedan calificarse de graves.*

Artículo 5 – Ataques a la integridad del sistema

Cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para prever *como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.*

Artículo 6 – Abuso de los dispositivos

1. Cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para prever *como infracción penal,* conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a).La *producción, venta, obtención para su utilización, importación, difusión* u otras formas de puesta a disposición:

I. *De un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados;*

II. De una *palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5* ; y

b). *La posesión de alguno de los elementos descritos* en los parágrafos (a) (1) o (2) *con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5* . Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal.

2. Lo dispuesto en el presente artículo *no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5* del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho de no aplicar el párrafo 1, a condición

de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el parágrafo 1 (a) (2).

Artículo 7 – Falsificación informática.

Cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para prever como *infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos* , con independencia de que sean directamente legibles e inteligibles. Las Partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.

Artículo 8 – Burla informática.

Cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para prever como *infracción penal,* conforme a su derecho interno, *la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:*

a). *La introducción, alteración, borrado o supresión de datos informáticos,*

b). *Cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.*

Artículo 9 – Delitos relacionados con la pornografía infantil.

1. Cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para prever como *infracción penal*, conforme a su derecho interno, las siguientes *conductas* cuando éstas sean cometidas *dolosamente y sin autorización:*

a). *La producción de pornografía infantil con la intención de difundirla a través de un sistema informático;*

b). *El ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático*;

c). *La difusión o la transmisión de pornografía infantil a través de un sistema informático;*

d). *El hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático*;

e). *La posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.*

2. A los efectos del párrafo 1 arriba descrito, la **«***pornografía infantil» comprende cualquier material pornográfico que represente de manera visual:*

a). *Un menor adoptando un comportamiento sexualmente explícito;*

b). *Una persona que aparece como un menor adoptando un comportamiento sexualmente explícito;*

c). *Unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito.*

3. A los efectos del párrafo 2 arriba descrito, el término *«menor» designa cualquier persona menor de 18 años*. Las Partes podrán exigir un límite de edad inferior, que debe *ser como mínimo de 16 años.*

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).

Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para prever como *infracción penal*, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, *conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor* , a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, *a escala comercial y a través de un sistema informático.*

2. Cada parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para prever como *infracción penal***,** conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, *conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.*

3. Las partes podrán, de concurrir determinadas circunstancias, reservarse el derecho de *no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.*

Cabe señalar que esta convención hace referencia a otros temas de gran relevancia para los Delitos informáticos, de los cuales destacan:

Artículo 11–Tentativa y complicidad.

Artículo 12–Responsabilidad de las personas jurídicas.

Artículo 13–Sanciones y medidas.

Artículo 14–Ámbito de aplicación de las medidas de derecho procesal.

Artículo 15–Condiciones y garantías.

Artículo 16–Conservación inmediata de los datos informáticos almacenados.

Artículo 17–Conservación y divulgación inmediata de los datos de tráfico.

Artículo 18–Mandato de comunicación.

Artículo 19–Registro y decomiso de datos informáticos almacenados.

Artículo 20–Recogida en tiempo real de datos informáticos.

Artículo 21–Interceptacion de datos relativos al contenido.

Artículo 22–Competencia.

Artículo 23–Principios generales relativos a la cooperación internacional.

Artículo 24–Extradición.

Artículo 25–Principios generales relativos a la colaboración.

Artículo 26–Información espontánea

Artículo 27–Procedimiento relativo las demandas de colaboración en ausencia de acuerdo internacional aplicable

Artículo 28–Confidencialidad y restricciones de uso.

Artículo 29–Conservación inmediata datos informáticos almacenados.

Artículo 30-Comunicación inmediata de los delitos conservados.

Artículo 31–Asistencia concerniente al acceso a datos informáticos almacenados

Artículo 32–Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso

Artículo 33–Asistencia para la recogida en tiempo real de datos de tráfico.

Artículo 34–Asistencia en materia de interceptación de datos relativos al contenido.

Artículo 35–Red 24/7 (Punto de contacto localizable las 24 horas del día, y los siete días de la semana, para asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal).

Artículo 36–Firma y entrada en vigor.

Artículo 37–Adhesion al Convenio.

Artículo 38–Aplicación territorial.

Artículo 39–Efectos del Convenio.

Artículo 40–Declaraciones.

Artículo 41–Cláusula federal.

Artículo 42–Reservas.

Artículo 43–Mantenimiento y retirada de las reservas.

Artículo 44–Enmiendas.

Artículo 45–Reglamento de controversia.

Artículo 46–Reuniones de los Estados.

Artículo 47–Denuncia.

Artículo 48–Notificación.

En este convenio se encuentran 39 países que han firmado de los 47 Estados miembros, de los cuales 21 ya ratificaron, y dentro de los 6 Estados no miembros del Consejo Europeo y participantes en esta convención sólo 4 han firmado y de entre los cuales únicamente Estados Unidos de América ratificó dicha Convención.

CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS SEGÚN EL CONVENIO DE CIBERDELINCUENCIA

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos:

- *Acceso ilícito*: El acceso deliberado e ilegitimo a la totalidad o a una parte de un sistema informático, ya sea infringiendo medidas de seguridad, con la intención de obtener datos informáticos

- *Interceptación ilícita:* Interceptación deliberada e ilegitima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos.

- *Interferencia en los Datos*: Comisión deliberada e ilegitima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

- *Interferencia en el sistema:* Obstaculización grave, deliberada e ilegitima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

- *Abuso de los dispositivos:* Comisión deliberada e ilegitima de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático.

Delitos informáticos:

- *Falsificación informática:* Cometer de forma deliberada e ilegitima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.

- *Fraude Informático:* Actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o supresión de datos informáticos, cualquier interferencia en el funcionamiento de un sistema informático.

Delitos relacionados con el contenido:

- ***Delitos relacionados con la pornografía infantil:*** Comisión deliberada e ilegitima de producción de pornografía infantil con vistas a su difusión por medio de un sistema informático, la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático, la difusión o transmisión de pornografía infantil por medio de un sistema informático, la adquirió de pornografía infantil por medio de un sistema informática para uno mismo o para otra persona, la posesión de pornografía infantil por medio de un sistema informático o en un medio de almacenamiento de datos informáticos.

Se entiende como pornografía infantil, todo material pornográfico que contenga representación visual de un menor comportándose de una forma sexualmente explicita, una persona que parezca un menor comportándose de una forma sexualmente explicita, imágenes realistas que representen a un menor comportándose de una forma sexualmente explicita.

Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines:

- Infracciones de la propiedad intelectual, de conformidad con las obligaciones asumidas por el Convenio de Berna para la protección de las obras literarias y artísticas, Tratado de la OMPI sobre propiedad intelectual, Convenio de Roma

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en Enero de 2008 se promulgó el "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa" que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

- Difusión de material xenófobo o racista.
- Insultos o amenazas con motivación racista o xenófoba.
- Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

3.4. REFORMAS Y LEGISLACIÓN COMPARADA EN LATINOAMÉRICA.

PAÍS	ACTO NORMATIVO	CONTENIDO	TÉCNICA

Argentina	Ley 26388 26/6/08 Reforma del Código penal Argentino	Contenido: Pornografía infantil por Internet u otros medios electrónicos (Art. 128 CP); • Violación, apoderamiento y desvío de comunicación electrónica (Art. 153, párrafo 1º CP); • Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (Art. 153, párrafo ºCP); • Acceso a un sistema o dato informático (artículo 153 bis CP); • Publicación de una comunicación electrónica (artículo 155 CP); • Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP); • Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP); • Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data); • Fraude informático (artículo 173, inciso 16 CP); • Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP)	Reforma código penal (La Ley 26.388 no es una ley especial, que regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias y especificas, sino una ley que modifica sustituye e incorpora figuras típicas a diversos artículos al CP actualmente en vigencia)
Brasil	Ley 8137 (27/12/90), sobre "Crímenes contra el orden económico y las relaciones de consumo" Ley 7646/1987 Ley 9100, Art. 67 inc. VII.	Uso ilícito del ordenador, que sería la acción de utilizar o divulgar programas de procesamiento de datos que permita al contribuyente poseer información contable diversa que es, por ley, proporcionada a la Hacienda Pública. Violación de derechos de autor de programas de ordenador. Acceso a bancos de datos. Tipo penal para punir con reclusión de uno a dos años y multa la obtención indebida de acceso, o su intento, a un sistema de tratamiento automatizado de datos utilizado por el servicio electoral, con el fin de alterar el cómputo o cálculo de votos	Ley especial Ley especial Ley especial
Colombia	Ley 679 de 2001 sobre pornografía infantil en redes globales	Medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio.	Ley especial (El Código Penal Colombiano expedido con la Ley 599 de 2000, no hace referencia expresa a los delitos informáticos como tales)
		Figuras previstas: 1.- acceso indebido a información contenida en un sistema de tratamiento de la misma; 2.- destrucción de un sistema informático o alteración del	

Chile	Ley 19.223/1993 sobre delitos informáticos	funcionamiento del mismo; 3.- daño, alteración y divulgación indebida de datos informáticos. Nuevo proyecto de ley (mensaje del Ejecutivo boletín Nº 3083-07) que introduce nuevos delitos informáticos, no especialmente incriminados en la legislación anterior; a saber: 1.- falsificación de documentos electrónicos y tarjetas de crédito 2.- fraude informático; y 3.- obtención indebida de servicios de telecomunicaciones.	Ley especial
Cuba	Reglamento de Seguridad Informática en vigor desde Noviembre de 1996	Estipula que en todos los Órganos y Organismos de la Administración Central del Estado se deberán analizar, confeccionar y aplicar el "Plan de Seguridad Informática y de Contingencia"; y el Reglamento sobre la protección y seguridad técnica de los sistemas informáticos, emitido por el Ministerio de la Industria Sideromecánica y la Electrónica, también en vigor desde Noviembre de 1996.	Reglamento
México	El código penal mexicano fue reformado con Ley el 17 mayo 1999. El título Décimo del Código Penal, en la sección sobre "Delitos contra el patrimonio", prevé en el artículo 217 del referido texto legal al delito informático.	Comete delito informático: “la persona que dolosamente y sin derecho intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red, se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días de multa”. El código no contempla todos los tipos más comunes de ataques informáticos. El capítulo II (como reformado en 1999) se refiere a los "accesos ilícitos", poniendo de hecho un límite a su aplicación, ya que no todos los ataques informáticos se perpetran necesariamente con acceso directo a un sistema. Ejemplo es el caso de "*denial of service*" que, según el código penal federal, tiene como objetivo el de modificar, destruir o provocar la pérdida de información. La conducta de aquel que simplemente imposibilita o inhabilita temporalmente un servidor no vendría entonces a caer en el marco de la norma citada.	Código Penal
	Art 184 del CP		

Paraguay	(1997) en función de la Ley 1328/1998 “De Derecho de Autor y Derechos Conexos	Violación del derecho de autor o inventor	Reforma código penal
Perú	ley 26612/1996 Ley 27309, Ley de incorporación de los delitos informáticos al código penal Proyecto de ley No. 2825-2000/CR, sobre pornografía infantil en Internet	Espionaje industrial Figuras: ingreso o interferencia en bases de datos, sistema o red de computadores El proyecto trata de tipificar e incorporar en el Código Penal el tipo penal de pornografía infantil que contemple tanto la conducta de procurar y facilitar que los menores de dieciocho años realicen actos de exhibicionismo corporal, lascivos y sexuales con el objeto y fin de fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, como la de fijar, grabar, imprimir, actos de exhibicionismo corporal lascivos y sexuales con menores de dieciocho años y la de elaborar, reproducir, vender, arrendar, exponer, publicitar o trasmitir el material pornográfico.	Ley especial de incorporación de los delitos informáticos en el código penal
Uruguay	Ley de Protección del Derecho de Autor y Derechos Conexos Nº 17.616 (13 de enero de 2003)	Normas que tutelan solamente la propiedad intelectual (software)	Ley especial (Se trata de buscar un aplicación amplia de las figuras clásicas introducidas por el código penal: hurto, estafa, daño)
Venezuela (República Bolivariana de)	Decreto 48/2001(Ley Especial Contra los Delitos Informáticos)	Hasta entonces se extendían las tipologías penales del código penal de 1964.nuevas figuras contempladas: sabotaje, daño de sistemas, falsificación documentos, acceso indebido, espionaje informático, violación de privacidad o de datos personales, relevación indebida de información personal, difusión o exhibición de material pornográfico adulto o de niños/adolescentes, apropiación de propiedad intelectual	Ley especial

(Fuente: elaboración propia datos de Gamba, Jacopo: 24 -26)

En América Latina se considera que no existe una cantidad suficiente de leyes en materia de Delitos Informáticos para las diferentes tipologías de crímenes. Se

nota una gran diversidad de delitos y al mismo tiempo una gran cantidad de bienes jurídicos que estas normas quieren proteger. Hay casos de delitos contra el patrimonio, delitos contra la propiedad (física o intelectual), delitos contra las personas (contra la Intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio), delitos contra la hacienda pública nacional que han sido tratados por normativas diferentes, a veces con reformas de los códigos penales, a veces con leyes ad hoc, en última instancia hasta con leyes de comercio electrónico.

3.5. LA CRIMINALÍSTICA INFORMÁTICA.

En los delitos informáticos estudiados en la presente investigación definitivamente, dentro de la especialización requerida para descubrir el *modus operandi* de los delincuentes o sujetos activos son la Informática y la Cibernética desde todos los enfoques analizados en el Capítulo Primero; es decir, podemos asistirnos desde la Informática en general, así como a la propia informática Jurídica, y de otras ciencias auxiliares; como ejemplo sería la contabilidad, para el caso de que se sustraiga información contable contenida en medios informáticos, o bien en aquellos delitos financieros cometidos a través de medios informáticos. Cabe recordar que el Derecho se encuentra inmerso en un mundo interdisciplinario en donde puede asistirse de inimaginables medios con el fin de llegar a la verdad histórica.

Surge así la "Informática Forense" la cual va a tratar sobre la aplicación de las diversas técnicas científicas y analíticas sobre la infraestructura de sistemas computacionales, para identificar, preservar, analizar y presentar las evidencias para encontrar el *modus operandi* del delincuente informático.

Problemática a la que se han enfrentado las investigaciones de los delitos informáticos:

a) Uniformar disposiciones sobre los delitos informáticos
b) Facultad de especialización en los órganos de investigación y administración de justicia para el tratamiento de los delitos

informáticos.

c) La ausencia en la creación de órganos auxiliares en la procuración de justicia para la adecuada investigación de los delitos informáticos, tales como una policía especializada, así como un cuerpo de expertos en la materia.

d) El carácter transnacional de las múltiples operaciones realizadas a través de los sistemas computacionales.

e) Ausencia de tratados internacionales para resolver múltiples problemas relacionados con los delitos informáticos, que van desde la celebración de convenios internacionales de colaboración, así como de extradición o de intercambio de reos por estos delitos.

La Informática Forense puede también ser utilizada como un efectivo proceso de aclaración interno de incidentes computacionales de riego antisocial, de errores o negligencias al interior de organizaciones, realizando un reporte discrecional hacia las autoridades públicas ya que puede haber razones de peso estratégico que afectarían la continuidad operativa, viabilidad o imagen de una organización en particular si se revelase información sensible sobre sistemas o aplicaciones vulnerables.

3.5.1. LA POLICÍA INFORMÁTICA.

De gran función en la Criminalística resultan los cuerpos policiacos que son los que acuden al lugar en donde se cometieron los hechos realizando lo que se conoce como trabajo de campo y su labor principal es recabar los indicios que le servirán al órgano de justicia para integrar adecuadamente su averiguación previa.

En otros países sobre todo de origen anglosajón como los Estados Unidos de América se encuentran cuerpos de policía especializados como el Federal Boreal Investigación (FBI) que concentra la información recabada en el lugar de los hechos

y dentro de ella la concentran en oficinas especializadas que realizan funciones de Inteligencia Criminal a efecto de depurar los datos recabados y solamente analizar lo que realmente importen para una investigación, apareciendo oficinas para el análisis de los vestigios que requieren de la especialización de cada delito, como sería el caso de los informáticos, originándose la creación de la llamada "Policía nformatica".

Definitivamente que la policía debe tener un grado de especialización para la investigación de los delitos existiendo academias en todo el mundo en donde surge una disciplina conocida como "La Policía Científica".

En la *Criminalística Forense* es indispensable comprender que identificar y seguir la pista a la evidencia digital y protegerla, es la parte trascendental de una adecuada investigación; la Policía Cibernética debe saber enfocar su atención a los hechos del delito en donde aparece tanto al delincuente informático como el sistema de cómputo que ha utilizado y en dónde lo ha usado, ya que como sabemos puede utilizar una computadora de escritorio, una lap top, propia o ajena, o inclusive otro sistema de cómputo aún más compacto como las conocidas "palm o pocket pc", en un país o en el extranjero o inclusive en varios países; la evidencia digital puede estar contenida en la computadora de la víctima o en un dispositivo de almacenamiento como un disquete, en los archivos de una empresa de servicios de Internet, en la computadora del sujeto pasivo o en sus disquete o discos o "usb" o bien, en otras ubicaciones de la red; una gran labor para el Policía Cibernético.

Una de las principales labores de toda policía es saber conservar el lugar de los hechos con todos los conocimientos especializados para ello, ya que desgraciadamente sabemos en la práctica de campo muchas unidades policiacas creen que cumplen con ello solamente con recabar toda información sin saber que hay técnicas especializadas para ello. Ejemplo sería en un robo a casa habitación en donde la policía solamente se concreta a tomar declaraciones de los testigos e introducir en bolsas algunos objetos que pudieron haber servido como instrumentos del delito sin tener el cuidado de que cada objeto debe ser

preservado con su técnica especial ya que podemos encontrar algunos que con el tiempo se puedan destruir, o bien, sin tener la precaución de tomar las posibles huellas digitales que pudieran haber dejado los sujetos activos.

3.5.2. LA INVESTIGACIÓN DE DELITOS INFORMÁTICOS.

En la región:

- En Perú: Existe la Dirección de Investigación Criminal y de Apoyo a la Justicia, con su División de Delitos de Alta Tecnología; que es parte de la Policía Nacional del Perú (PNP). Cuentan con tres departamentos: i) Departamento de Delitos Informáticos, Patrullaje Virtual, ii) Departamento de Investigación Especial (Hurto de Fondos, Pornografía Infantil, Piratería de Software, Investigaciones Especiales) y iii) Departamento de Coordinación, Coordinación Búsqueda de Información.

- En Colombia: Existe el grupo de delitos informáticos de la SIJIN (Policía Nacional) quien tiene varios laboratorios de computación forense, y el DAS (Departamento Administrativo de Seguridad) que tiene una unidad específica de delitos informáticos, además de varias entidades investigativas privadas que colaboran con los agentes nacionales.

- En Uruguay: Está presente la sección Delitos Informáticos del Departamento de Delitos Complejos, de la Dirección de Investigaciones de la Jefatura de Policía.

- En Ecuador: Existe la DIDAT, Departamento de Investigación de Alta Tecnología de la Policía Judicial del Ecuador, además en la Fiscalía General del Estado existe el Departamento de Investigación y Análisis Forense.

- En México: La Policía Cibernética de la Secretaría de Seguridad Pública Federal, trabaja en temas de delitos informáticos, llevando a cabo campañas de prevención del delito informático a través de la radio y cursos en instituciones públicas y privadas. También está el equipo UNAM-CERT que, sin tener la misión de perseguir los delitos cibernéticos, igual realiza acciones contra sitios de phishing y análisis

forense.

- En Chile: Desde el año 2000, existe la "Brigada Investigadora del Ciber Crimen", dependiente de la Jefatura Nacional de Delitos Económicos. Esta Brigada se principales: el Grupo de Investigación de Pornografía Infantil, el de Delitos Financieros e Investigaciones Especiales y el de Análisis Forense Informático (Jacopo Gamba, 2010: 23).

En el mundo:

- Organización Internacional de Policía (INTERPOL): Actualmente, la "Comisión Criminal Internacional del Policía" conocida también como: "La Organización Criminal Internacional de la Policía - INTERPOL - es la organización internacional más grande de la policía del mundo ya que a ella se han afiliado más de 186 países miembros incluido el nuestro. Fue creado en 1923, con el objetivo de facilitar la cooperación fronteriza del policía, así como apoyar y asistir a todas las organizaciones, autoridades y servicios. Su misión más importante es prevenir o combatir el crimen internacional.

Cada país miembro de la Interpol mantiene una Oficina Central Nacional (NCB) provista de personal constituido por oficiales del Estado Miembros. El NCB es el punto de contacto señalado por la Secretaría General; las oficinas regionales son utilizadas como el punto de contacto entre el Estado Miembros de la Interpol cuando éstos requieren ayuda respecto a investigaciones de ultramar, así como la localización y aprehensión de fugitivos.

- Oficina Europea de Policía (EUROPOL): El establecimiento de la Europol fue convenido en el tratado de *Maastricht* en la Unión Europea del 7 de febrero de 1992 en La Haya, Países Bajos, En la Europol comenzaron operaciones limitadas el 3 de enero de 1994 bajo la forma de unidad de las drogas de Europol (EDU). La Europol comenzó sus actividades el 1º de julio de 1999, y el día 1o. de enero de 2002, el mandato de Europol fue extendido al reparto con todas las formas

serias de crimen internacional, una de las principales prioridades para la Europol incluyen el combate a los crímenes contra personas, los de índole financiero y los del *cybercrime* (Delitos Informáticos). Esto se aplica donde está implicada una estructura criminal organizada y que afectan dos o más Estados Miembros.

- El Buró Federal de Investigaciones (FBI): El Servicio de Seguridad del Estado, *Federal Bureau of Investigation*, por sus siglas en inglés (FBI), es una división del Departamento de Justicia de los Estados Unidos, en una de las más poderosas e influyentes organizaciones en el mundo. Con más de 8,000 agentes especiales en el país tanto en grandes ciudades como en pueblos pequeños o fijos, tiene su sede en la ciudad de Washington, D.C.

El FBI cuenta con un Sistema Informático denominado Carnívoro (*Carnivore*) que se dio a conocer públicamente en Junio del 2000 a un selecto grupo de expertos de las industrias de la telecomunicación para demostrar la habilidad del FBI para interferir teléfonos a solicitud de la Comisión Federal de Comunicaciones.

Utilizando personal externo para que instale en las computadoras servidores ISP, Carnívoro opera en un sistema de "olfateo" que puede analizar grandes pedazos de datos electrónicos mientras viajan por la Internet.

3.6. EL DELITO INFORMATICO EN BOLIVIA.

La tipificación de los delitos informáticos en el CAPITULO XI del Código Penal Boliviano, toma en cuenta que los sistemas informáticos procesan y transfieren información valiosa, o que esta información no solo es valiosa en si misma sino que puede contener información representativa personal del patrimonio de las personas, la comisión de estos delitos son mediante el sistema informático, es decir que requiere el uso de las computadoras o sistemas informáticos, y contra el sistema debido a que la conducta delictiva es contra la información misma.

3.6.1.- ANÁLISIS DEL ART. 363 bis Y ter CÓDIGO PENAL BOLIVIANO

A continuación, procederemos al análisis de la tipificación de los delitos

informáticos que han sido introducidos al Código Penal Bolivia mediante Ley Nº 1768 del 11 de marzo de 1997 "Ley de Modificaciones del Código Penal" en el Gobierno de Gonzalo Sánchez de Lozada.

CAPITULO XI DELITOS INFORMÁTICOS CODIGO PENAL BOLIVIANO

Artículo 363 bis.- (MANIPULACION INFORMATICA)

> El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Este tipo penal prevé aquella conducta por la cual se modifica información ya sea en el momento de su procesamiento o de su transmisión, es decir en el momento en la que esta información esta siendo procesada por un sistema informático o cuando después de haber sido procesada, es transmitida. Para que esta conducta constituya delito, debe producirse una transferencia patrimonial en perjuicio de un tercero y así generar un beneficio indebido

Es importante resalta que este tipo penal no toma en cuenta el hecho de la manipulación del procesamiento o transferencia de datos sea realizada mediante un acceso no autorizado a la información, es decir que en este tipo penal no se toma en cuenta la posibilidad de la violación de los sistemas de seguridad o del acceso sin autorización a los sistemas informáticos, sino que se toma como presupuesto del tipo penal al resultado mismo.

Artículo 363 ter.- (ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS)

> El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de

trabajo hasta un año o multa hasta doscientos días.

Al igual que la tipificación establecida en el artículo 363 bis del Código Penal, que constituye un delito de resultado, es decir que la tipicidad requiere de un resultado (la transferencia patrimonial en perjuicio de un tercero y generando un beneficio indebido).

En el caso del articulo 363 ter. Se observa que el tipo penal exige que la acción realizadora del tipo (el acceso no autorizado a un sistema informático, para apoderarse, utilizar y modificar información) deba de derivar a un resultado típico (ocasionar un perjuicio a un tercero).

En este tipo penal se está protegiendo la integridad del sistema mismo y de la información procesada o contenida en el, los denominados virus informáticos son precisamente un ejemplo de destrucción o supresión de la información.

En cuanto al contenido general de los artículos son amplios y vagos, pero cubre, de cierta manera, la laguna legal existente hasta ese momento. En todo delito de los llamados informáticos, hay que distinguir el medio y el fin. Para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad informática y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito, una finalidad deseada que causa un perjuicio a otro, o a un tercero

EL REGLAMENTO DEL SOPORTE LÓGICO O SOFTWARE Nº 24582 25 DE ABRIL DE 1997.

> Datos informáticos o banco de datos informáticos como el conjunto organizado de información accesible por computadora. Soporte informático. Es todo dispositivo o medio físico (memoria, disquetes, discos duros, cintas, etc.) o medio magnético, óptico, químico o papel y otros, empleados para propósitos de comunicación entre

humanos y máquinas y fines de almacenamiento.

Si bien algunos de estos verbos y sustantivos pueden agruparse para identificar una figura delictiva - como alterar, modificar, suprimir o inutilizar que equivalen relativamente al sabotaje o el acceso y uso son equivalentes al acceso no autorizado -. Se omiten algunos detalles característicos de cada figura; por ejemplo, en el caso de acceso no se establece la diferencia entre acceso doloso y acceso culposo. ¿Qué sucede entonces cuando los datos son revelados a terceras personas? o ¿cuándo no afectan tan sólo al titular de la información? Así es como se crea un universo grande para la aplicación del artículo: o todas las conductas ingresan o no hace ninguna, lo cual perjudica la labor de interpretación. Introducirnos al análisis de los delitos informáticos en su interrelación con el derecho penal implica cotejar ambos en virtud de las nuevas corrientes científicas.

3.6.2.- LA INVESTIGACION DEL DELITO INFORMATICO EN BOLIVIA.

En Bolivia existía la División Delitos Informáticos (2007 -2009) que fue cerrada por no presentar los resultados esperados, ahora es La Fuerza Especial de Lucha Contra el Crimen (FELCC) que es la unidad encargada de la investigación de estos nuevos delitos así como también los ilícitos traiciónales cometidos atreves de nuevas tecnologías teniendo que recurrir a veces a peritos especializados independientes para realizar las investigaciones respectivas, veamos algunas estadísticas disponibles de estos ilícitos reportados a la (FELCC).

Entre 2003 y 2007 la fuerza anticrimen recibió 185 denuncias de manipulación informática y alteración, acceso y uso indebido de datos en toda Bolivia, pero se desconoce si alguna de ellas fue resuelta. Los datos de La Fuerza Especial de Lucha Contra el Crimen (FELCC) revelan que 177 corresponden a manipulación informática y 8 a alteración, acceso y uso indebido de información. De la primera figura legal, 91 casos hubo en Santa Cruz, 46 en Cochabamba, 30 en La Paz, 4 en Potosí, 3 en Oruro, 2 en Beni y 1 en Tarija. Sobre alteración informática, 3 ocurrieron en La Paz, 2 en Cochabamba, 2 en Beni y 1 en Santa Cruz.

El 2008 la Fuerza Especial de Lucha Contra el Crimen (FELCC) recibió al menos 50 denuncias de Delitos Informáticos, en el país de las cuales solo 36 fueron investigadas pero ninguna fue resuelta.

A ello se suma la falta de fiscales especializados en la materia para conducir las investigaciones.

De enero a agosto del presente año hubo 50 denuncias de manipulación electrónica, 27 en Santa Cruz, 12 en La Paz, 9 en Cochabamba, 2 en Chuquisaca y ninguna acerca de alteración.

Podemos decir que la Policía Boliviana no cuenta con los medios y conocimientos especializados para poder llevar a cabo una investigación adecuada respectos a estos Delitos Informáticos además de no contar también de herramientas necesarias a si como un disprosio legal claro y detallado que facilitaría su trabajo.

Nuestro ordenamiento jurídico pase haber legislado en el Código Penal los delitos informáticos no contempla claramente la descripción de estas conductas delictivas detalladas anteriormente, en consecuencia la atipicidad de las mismas en nuestro ordenamiento jurídico imposibilita una calificación jurídico legal que individualice a las mismas, llegando lógicamente a existir una alta cifra de criminalidad e impunidad, haciendo de esta manera casi imposible sancionar como delitos hecho no escritos en nuestra legislación penal, es por lo cual se necesita de manera imperiosa una modificación de nuestro código penal referente a los delitos informáticos acorde a esta nueva realidad que se presenta.

CAPITULO IV

CONCLUSIONES Y PROPUESTAS

CONCLUSIONES.

Primera.- La tecnología presentara siempre nuevos y dinámicos beneficios en cada aspecto de la sociedad y por supuesto en la vida humana pero así como beneficios,

también trae serios inconvenientes como ser los Delitos Informáticos, nuevos tipos penales que se presentan a partir del avance tecnológico, estos nuevos ilícitos diversos que tienen variedad de definiciones así como también características diferentes a los delitos tradicionales que conocemos por que cambian, evolucionan y surgen en días, siendo mas difíciles de combatir, causando de esta manera grandes perdidas en empresas como en particulares.

Segunda.- La información se ha convertido en esta época como uno de los bienes mas preciados y es también blanco principal de los delincuentes informáticos, apropiándose, modificándola o divulgando en beneficio propio, además que por su carácter transnacional, es difícil de perseguir y sancionar por que estos ilícitos pueden cometerse desde cualquier rincón del mundo.

Tercera.- La problemática de la delincuencia informática radica en su variedad pero sobre todo en las características especiales que tienen estos delincuentes por que se tratan de especialistas en informática, por ello borrar las pruebas les resulta relativamente fácil así como ejecutar su labor en el anonimato mas profundo y es por ello que se debería crear convenios con los demás estados para combatir a estos delincuentes y la unificación de la ley penal *referentes a estos delitos.*

Cuarta.- El internet ha venido a mejorar la historia del hombre en actividades tales como la comunicación, mensajería, y información entre otras mas convirtiéndose en una herramienta en beneficio del hombre, pero lamentablemente la facilidad que lleva su uso y las malas intenciones de las personas la hace fácil utilizarla para cometer delitos de gran variedad en perjuicio de personas, empresas e incluso estados ocasionando perdidas de gran consideración.

Quinta.- Los Delitos Informáticos por tratarse de una problemática mundial ha sido regulada jurídicamente por los organismos mas importantes entre los cuales destacamos La Organización de Naciones Unidas (O.N.U.) el llamado Grupo de los 8 o (G8) y la comisión de comunidades Europeas, siendo esta ultima la que ha tenido los mas importantes logros en esta lucha, creando convenios como el de la Ciber-criminalidad del 23 de octubre de 2001, que precisa un marco jurídico avanzado. Que serviría como modelo para adoptar en caso de una legislación especial en nuestro medio y ha nivel mundial.

Sexta.- Uno de los grandes problemas de toda clase de delincuencia es el detectar el modus vivendi y operando del delincuente para así poderlo detener, por lo que una de las ciencias auxiliarles del Derecho Penal para llevar a cabo esa finalidad es la Criminalística que enfocada a Los Delitos Informáticos va a ser indispensable para lograr la aprehensión del delincuente informático que utiliza los grandes avances tecnológicos para sus fines delictivos y que se oculta y huye a través de las líneas alambicas e inalámbricas de esos sistemas computacionales.

Séptima.- Las investigaciones de los Delitos Informáticos han enfrentado grandes problemas de origen técnico, así como de conocimiento de las personas de los diversos sectores en donde se comete esta clase de ilícitos, así como de quienes se encargan de la investigación y administración de justicia.

Octava.- La Policía es de gran importancia para la investigación de los delitos, y los informáticos no son la excepción, por lo que surge a nivel internacional en diferentes países la "Policía Cibernética", que deberá utilizar todos los conocimientos en Informática para localizar y detener al delincuente informático. En Bolivia existía una División de Delitos Informáticos (2007 – 2009), ahora estos ilícitos los investigan la Fuerza Especial de Lucha Contra el Crimen (FELCC) con especialistas propios y a veces recurriendo a peritos independientes.

Novena.- En Bolivia se tuvo la preocupación de regular los Delitos Informáticos el año 1997 siendo una de las primeras en el continente en incluir estos delitos en el Código Penal, con lo cual se pretendía esencialmente proteger la información que se tenía en un sistema informático de manera general, amplia e imprecisa, pero cubriendo de cierta manera la laguna legal existente en nuestra legislación hasta ese momento.

Decima.- Nuestro ordenamiento jurídico pese haber legislado en el Código Penal capitulo XI los Delitos Informáticos no contempla claramente la descripción de estas conductas delictivas detalladas anteriormente, en consecuencia la atipicidad de las mismas en nuestro ordenamiento jurídico imposibilita una calificación jurídico legal que individualice a las mismas, llegando lógicamente a existir una alta cifra de criminalidad e impunidad, haciendo de esta manera casi imposible sancionar como delitos, estos ilícitos nuevos, hay que tomar también en cuenta que la legislación elaborada data de aproximadamente ya de 14 años y en ese tiempo la tecnología informática no tenia el avance que tiene en la actualidad.

PROPUESTAS.

1.- Mi primera propuesta, se centra en la creación de nuevos tipos y normas legales, ya que no se cuenta con las disposiciones penales necesarias de fondo y forma que sirvan para describir y sancionar la enorme variedad de conductas ilícitas producidas por estos nuevos Delitos Informáticos, y que por tal razón permanecen impunes.

2.- Se debería sancionar con penas mas duras a quienes utilicen sus conocimientos para traspasar mecanismos informáticos de seguridad de una base de datos, por que estos delitos a diferencia de los tradicionales causan gigantes pedidas económicas. Así también creo que en cuanto a las sanciones estas deberían plasmarse de acuerdo al sujeto pasivo al que es victima de estos delincuentes por que podría tratarse del Estado y esto agravaría la sanción.

3.- El Legislador debe contar con toda la educación que le pueda aportar el derecho informático y conjuntamente con esos conocimientos y la realidad social que pretende regular pueda formular una adecuada legislación, dentro de esa legislación penal a definir debe hacerse una clara distinción de los ilícitos informáticos conforme a los bienes jurídicos que se pretende tutelar, ya sea cuando se hace mención a la confidencialidad de la información contenida en medios informáticos, en relación a la protección de éstos medios informáticos, o bien cuando se refieren a los delitos tradicionales cometidos por medios informáticos nuevos.

4.- Además propongo la creación de unidades de investigación especializada en la Policía Nacional que se dediquen al rastreo, identificación y detención de los delincuentes informáticos, es necesario para que estas unidades de policía sean realmente eficaces, tienen que contar con herramientas jurídicas para poder así hacer frente a estos nuevos ilícitos.

5.- No cabe duda que uno de los factores mas importantes para prevenir y combatir a los delitos informáticos es la educación a particulares, escuelas, empresas, entidades financieras incluso al propio Estado en si a todo aquel que utilice esta tecnología.

6.- Es necesario la actualización de juristas, personal judicial, abogados e interesados mediante una enseñanza integrada y multidisciplinaria capaz de proveer la base técnica indispensablemente para entender el fenómeno de esta nueva era a través de seminarios y cursos participativos.

7.- En cuanto al carácter transnacional de los Delitos Informáticos, es preciso crear un ambiente de cooperación y coordinación entre los Estados vecinos mas adelantados sobre el tema así mismo que Bolivia pertenezca a organismos internacionales especializados para llevar a cabo una adecuada lucha contra este flagelo global manteniendo claro siempre los principios constitucionales y jurídicos de nuestro país.

8.- también propongo una activa cooperación y participación entre instituciones que conforman en El Gobierno y Estado Nacional tales como la Ministerio Publico, Procuraduría General del Estado, Gobernaciones Departamentales, etc. y no solo adopten un papel de observadores.

9.- Se deben establecer políticas especializadas para combatir las diversas conductas antisociales realizadas por medios informáticos que pueden incurrir en infracciones o inclusive delitos, por lo que su atención debe ser en los cuatro Órganos que conforman del Estado tanto el legislativo, ejecutivo, judicial y electoral.

10.- Propongo también que para detener la comisión de los Delitos Informáticos es la de trabajar juntos la sociedad en general, juristas, policía, investigadores etc. y compartir nuestros conocimientos por mas pequeños que estos sean para lograr construir un frente en contra a esta problemática.

BIBLOGRAFIA:

1.- Arce Jofré, José Alfredo. (2003). *"Informática y Derecho".* Ediciones Instituto Boliviano de Informaciones Jurídicas. La Paz.

2.- Davara Rodríguez, M.A. (2008). *"Manual de Derecho Informático"*. Editorial Aranzadi, 5ta. Edición, Madrid.

3.- Gamba, Jacopo. (2010). *"Panorama del derecho informático en América Latina y el Caribe".* Publicaciones CEPAL. Santiago de Chile.

4.- Masana, Sebastian. (2002). *"El Ciberterrorismo".* Publicaciones FLACSO. Buenos Aires.

5.- Mata Y Martín, Ricardo M. (2001), "*Delincuencia Informática y Derecho Penal".* Editorial Rama. España.

6.- Rodao, Jesús de Marcelo. (2001). *"Piratas Cibernéticos, Cyberwars, Seguridad Informática e Internet".* Editorial Rama. España.

7.- Téllez Valdés, Julio. (2004). *"Derecho Informático".* Editorial Mc Graw Hill, 3ra Edición. México.

8.- Wilson, Clay. (2005). *"Ataque de equipo y Ciberterrorismo".* EEUU.

LEGISLACIÓN:

1.- Bolivia. (1997). *Código Penal Boliviano. Ley Nº1768. Gaceta Oficial del Estado Plurinacional de Bolivia. La Paz – Bolivia*.

2.- Bolivia. (1997). *Reglamento de Software. Decreto Supremo 24582. Gaceta Oficial del Estado Plurinacional de Bolivia. La Paz – Bolivia.*

3.- Consejo de Europa. (2001). "*Convenio sobre cibercriminalidad"* Unión Europea, Budapest.

REVISTAS:

1.- Palazzi, Pablo A. (2006). *"Análisis legal del accionar de un virus informático en el derecho penal argentino y comparado",* en Revista de derecho, comunicaciones y nuevas tecnologías. Ediciones UniAndes. Bogotá.

DICCIONARIOS:

1.- Diccionario de la Lengua Española, Edición 2003

REFERENCIA ELECTRÓNICA:

1.- *"Ranking TIC-Internet: Bolivia a la cola de América Latina".* [En línea]: http://www.bolpress.com/art.php?Cod=2011060313 [Consulta: 2/09/2011]

2.- *Griselda Cousirat, Viviana. "Informática y Derecho en Internet".* [En línea]: http://www.robertexto.com/archivo13/derecho_internet.htm [Consulta: 28/08/2011]

3*.- "Pericias Informáticas".* [En línea]: http://www.peritajeinformatica.com.ar [Consulta: 28/09/2011]

4**.-** Tinajeros Arce, Erika Patricia*. "Criminalidad informática en Bolivia".* [En línea]:http://www.informatica-juridica.com/trabajos/Criminalidad_informatica_en_Bolivia.asp [Consulta: 25/08/2011]

5.- Rota, Pablo Cristóbal. *"Seguridad Informática".* [En línea]: http://es.scribd.com/doc/38695176/23618536-Seguridad-a-Trabajo-Practico [Consulta: 1/09/2011]