UNIVERSIDAD MAYOR DE SAN ANDRÉS
Facultad de Derecho y Ciencias Políticas
Carrera Derecho

TRABAJO DIRIGIDO

"EL FENÓMENO DEL DELITO FRENTE AL DESARROLLO INFORMATICO, Y LA NECESIDAD DE QUE SUS CONDUCTAS SE ENCUENTREN CLARAMENTE TIPIFICADAS"

Postulante: William Condori Arizaya
Tutor: **Dr. Jorge Ocampo Castelu**

La Paz – Bolivia
2002

Agradezco imperecederamente a docentes que contribuyeron en mi formación profesional durante los años de estudio en la Carrera de Derecho de la U.M.S.A., a mis padres por su apoyo incondicional y al tutor Dr. Jorge Ocampo Castelu, por su supervisión continua en su juiciosa orientación.

RESUMEN

En los últimas décadas hemos sido testigos de una elevada escala de tecnología informática. el desarrollo de los sistemas informáticos produce, a su vez, el desarrollo de nuevas formas de comunicación entre los individuos, producto de todo el avance tecnológico, el Derecho también se ve inmerso en nuevas formas de actividades de diverso tipo, en las cuales la intervención de los sistemas informáticos para su realización es cada vez más común, estas conductas no siempre son lícitas, por lo que es necesario su debida regulación en el Código Penal para garantizar de esta manera una aplicación y una tipificación correcta. Es indudable, pues, que la informática produce cada día una intensa evolución en las distintas ramas, en nuestro caso, del Derecho Penal porque constituye también parte esencial del desarrollo tecnológico y comercial del mundo entero. Como es sabido, el uso de sistemas informáticos forma desde hace mucho tiempo una pieza clave en la vida de cada individuo, el cual se ve sujeto a la necesidad de tener una computadora, una base de datos, la red, etc., como medio para realizar diversas conductas en su vida diaria.

Mucho se habla de los grandes beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual, sin embargo, el desarrollo tan amplio de la tecnología informática ofrece también un aspecto negativo, ya que se han generado nuevas conductas antisociales y delictivas que se manifiestan en formas que no era posible imaginar en el siglo pasado.

Los sistemas de computadoras ofrecen oportunidades nuevas y muy complejas de infringir la ley y han creado la posibilidad de cometer delitos en formas no tan tradicionales. Así tenemos que en nuestra legislación no tipifica el sabotaje informático, con lo cual las conductas ilícitas que se realizan quedarían impunes, pues la necesidad de regular esta conducta ilícita ha llevado a las grandes potencias al contemplar en sus legislaciones al respecto. El Derecho Comparado así como las Naciones Unidas, nos permite hacer una lista de los delitos que no están contemplados en nuestro Código Penal vigente. Es así que debido a estos procesos de aceleración en la informática, surgen también nuevas formas de conductas delictuales.

PRIMERA PARTE

(CONCEPTUALIZACION Y DIAGNOSTICO)

CAPITULO I

Capitulo II

ALGUNAS PRECISIONES ACERCA DE LA CRIMINALIDAD INFORMÁTICA COMO NUEVA FORMA DE CRIMINALIDAD

2.5 El Salame, Redondeo de Cuentas o "*Rounding Down*".

2.6 Uso Indebido de Programas o "*Superzapping*".

2.7 Puertas falsas o "*Traps Doors*".

2.8 Bombas Lógicas o "*Logic Bombs*".

2.9 Ataques Asincrónicos o "*Asynchronic Attacks*".

2.10 Recojo de Información Residual o "*Scavenging*".

2.11 Divulgación No Autorizada de Datos o "*Data Leakcage*".

2.12 Acceso a Áreas No Autorizadas o "*Piggyn Baking*".

2.13 Suplantación de la Personalidad o "*Impersonation*".

2.14 Simulación e Imitación de Modelos o "*Simulation and Modeling*"

Segunda Parte

DE LOS DELITOS INFORMÁTICOS:

MARCO LEGAL

Capítulo III

Delimitación conceptual del delito informático

3.1 El Concepto de Delito Informático

- 3.1.1 La Función de Tutela de Bienes Jurídicos
- 3.1.2. El contenido del bien jurídico protegido en los Delitos Informáticos
- 3.1.3 La Intimidad como bien jurídico protegido
- 3.1.4 El Patrimonio como Bien Jurídico Protegido
- 3.1.5 El Honor como Bien Jurídico Protegido

3.2. La libertad Informática

3.3 La Seguridad Informática

3.4 Presupuestos para la Tipificación de los Delitos.

- 3.4.1. Acción.
- 3.4.2. Tipicidad.
- 3.4.3 Antijuricidad.
- 3.4.4 Culpabilidad.
- 3.4.5 Imputabilidad.

3.5 La Informática y el Derecho.

INTRODUCCIÓN

La informática es un fenómeno multifacético de realidad contemporánea, constituye una opción metodológica para el desarrollo, la misma nos acercará a la propia actuación de las personas y sus conflictos generados en la red. Asimismo, podremos observar como el desarrollo de los sistemas informáticos ha producido grandes cambios en nuestra sociedad. Hoy en día, nadie duda de la importancia que han adquirido en la actualidad la utilización de sistemas informáticos para el buen desarrollo de la vida en sociedad.

Ya desde algunos años atrás el avance tecnológico de las comunicaciones y la enorme trascendencia del uso de la mayor autopista mundial de información Internet, que es la red de redes más extendida del planeta, la forma de conectar distintas computadoras, y posibilitar todo tipo de transmisión de datos entre ella, ha causado infinidad de problemas en el uso ilícito de las herramientas informáticas por personas que por distintos motivos, han causado perjuicios en sistemas y bancos de datos.

Es el objetivo del presente trabajo, analizar cuales son algunas de las principales conductas antijurídicas desarrolladas con el uso de la computadora por personas generalmente con conocimiento en informática y cual el marco normativo represivo aplicable a la misma.

Para explicar la importancia de estos sistemas en la vida diaria de cada individuo, empezaremos este capítulo por la explicación de la incidencia social que ha originado el uso de las computadoras en la colectividad. Seguidamente, explicaremos en qué consiste el ciberespacio y el anonimato, así como los sujetos que intervienen en la red.

Así mismo, señalaremos algunas precisiones acerca de la criminalidad informática, y conductas nocivas que se cometen a través de los sistemas informáticos. En cuanto al marco legal estableceremos la tutela de los bienes jurídicos, de esta manera ingresamos a los elementos del delito y la necesidad de incorporar nuevos tipos penales en nuestra

economía jurídica bajo el principio "Nullum crimen, nulla poena, sine lege", No hay delito ni pena sin una ley previa.

Se destacara las principales manifestaciones de los delincuentes informáticos, y establecer cual es el perfil del delincuente informático. Por último conoceremos nuestra legislación en comparación al sistema comparado de otras legislaciones en el ámbito internacional, y que teniendo en cuenta esta situación es necesario resaltar que los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada.

PRIMERA PARTE

(CONCEPTUALIZACION Y DIAGNOSTICO)

CAPITULO I

1.1 La Informática y Proceso de Comunicación de las Personas en la Red

1.2. Breve Reseña

Los pueblos primitivos en la antigüedad buscaron un medio para registrar el lenguaje, para ello utilizaron signos que designaban a una tribu o pertenencia, ya que no habían desarrollado otras formas de comunicación. Posteriormente, alrededor del año 700 A.C, surge el alfabeto en Grecia, el cual determinó la infraestructura mental necesaria para una comunicación de tipo acumulativa basada en el conocimiento. Este nuevo orden permitió dentro del discurso racional, separar la comunicación escrita del sistema audiovisual de símbolos y percepciones.

A partir del desarrollo de la civilización y de las lenguas escritas, surgió también la necesidad de comunicarse a distancia de forma regular. Así es como se fueron desarrollando múltiples formas de comunicación: los servicios postales, el telégrafo, el teléfono, la telefonía celular, el fax, etc.

Las comunicaciones ocupan un lugar central y preponderante en el desarrollo de los individuos. Desde la comunicación oral hasta la virtual el hombre ha modificado su conducta y su manera de percibir la realidad. En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación fundado en la informática, tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos. La informática está hoy en casi todos los campos de la vida moderna, este es el panorama, de este nuevo fenómeno científico – tecnológico en las sociedades modernas, por ello ha llegado a sostenerse que la informática es hoy una forma de poder social.

1.2.1 El Internet

El inicio del Internet, se remonta a 1969, cuando la Agencia de Proyectos de Investigación Avanzado en estados Unidos, conocido como por sus siglas "ARPA", desarrolló ARPANET, una especie de red que unía redes de computo del ejercicio y de laboratorios Universitarios que hacían investigaciones sobre la defensa. Esta red, permitió primero a los investigadores de Estado Unidos acceder y usar directamente supercomputadoras localizadas en algunas Universidades y laboratorios clave, después compartir archivos y enviar correspondencia electrónica. En 1980, las redes más coordinadas, como CSNET (red de ciencias de computo), empezaron a proporcionar redes de alcance nacional a las comunidades académicas y de investigación en Estados Unidos. En 1986, se creo la NSFNET (Red de la Fundación Nacional de Ciencias), de este modo esta red se expandió con gran rapidez. Actualmente cualquier persona puede ofrecer su propia página, un lugar virtual en WWW (World Wide Web), o abrir su propio foro de discusión y que abordan desde temas muy interesantes hasta conductas criminales.

Esta red se diseño para una serie descentralizada y autónoma de uniones de redes de computo, con la capacidad de transmitir comunicaciones rápidamente sin el control de persona o empresa comercial alguna y con la habilidad automática de renrutar datos si una o más uniones individuales se dañan, o están por alguna razón inaccesibles, se diseño para permitir la continuación de investigación vitales y comunicación cuando algunas partes de esta red se dañaran por cualquier causa.

El Internet una red mundial formada por millones de ordenadores de todo tipo y plataforma, conectados entre si por diversos medios y equipos de comunicación, cuya función principal es la de localizar, seleccionar, e intercambiar información desde el lugar en donde se encuentra hasta aquella donde haya sido solicitada o enviada, mediante el uso de diversas modalidades de comunicación en línea (listas de correo, grupos de discusión de Usenet, WWW, chats, etc.).

Internet se muestra como un medio universal de comunicación y búsqueda de información a muy bajo costo. "Se compone por un conjunto de redes interconectadas que permiten la comunicación entre millones de usuarios de todo el mundo, generando un inmenso grupo de recursos de información, en forma de imágenes, texto, gráficos y sonido". Sin duda, Internet ha sido creada para el libre acceso a la información global.

Internet es identificada por la mayor parte de usuarios como la gran autopista de la información. Así, la eficaz intermediación de Internet posibilita reconducir los incontenibles flujos de información y contribuye a que la "sociedad de la información" pueda efectivamente transformarse en "sociedad del conocimiento", como consecuencia de la posibilidad de extraer conocimientos útiles de la sobreabundancia de información.

Sin embargo, a partir de 1990, por la afluencia comercial de Internet, comienza la preocupación principal por la seguridad y es que hay que recordar que ninguna entidad académica, empresarial, gubernamental o de cualquier otro tipo administra Internet.

1.2.2 Crecimiento demográfico latinoamericano respecto del uso de Internet.

Se considera un análisis global a nivel latinoamericano como base de este estudio, considerando que el Internet es una red sin fronteras, que interconecta a todos los países a nivel mundial.

América Latina, donde los idiomas predominantes son el español y el portugués comprende infinidad de conexiones que se extienden desde la frontera de Estados Unidos hasta el extremo sur de Tierra sin Fuego, en Argentina.

1.2.3 El crecimiento de uso de Internet

Según estudio reciente de Nazca S&S, la red Latinoamericana de Satchi&Satchi World Wide, el uso regional aumento en 788% desde 1995. El estudio pronostica que para el año 2005, unos

34 millones de Latinoamericanos tendrán acceso a la Web, lo que significará un aumento del 4250 % desde 1995.

Estudios en Latinoamérica, realizados sugieren que el número de usuarios de Internet en la región está aumentando casi en un 20% al mes.

1.2.4 Incursión de Internet en Bolivia.

En Bolivia la expansión y uso de la Red de Telecomunicaciones digitales "Internet", está enmarcado por un crecimiento exponencial a nivel nacional de un número cada vez mayor de usuarios. La autopista de la información, red de redes o más conocida como Internet aparece en Bolivia en el año 1993, mediante un convenio realizado con UNICEF y las Naciones Unidas.

Distribución de usuarios de Internet en Bolivia

15 % Cochabamba
30 % La Paz
45 % Santa Cruz
10 % Otros
Datos: WWW.Bolnet.com.bo

1.3. Incidencia Social de las Computadoras

Han pasado más de cincuenta años desde que Howard Aiken presentó en la Universidad de Harvard la primera computadora. Décadas más tarde, la evolución tecnológica ha dejado atrás los antiguos tubos electrónicos y válvulas para reemplazarlos, en la actualidad, por diminutos circuitos integrados que procesan millones de operaciones por segundo.

De un tiempo a esta parte, las computadoras han evolucionado de una manera muy rápida, tan rápida que apenas la sociedad puede asimilar estos nuevos cambios. Los efectos de Internet tienen una importante incidencia sobre la estructura familiar y social. Gran parte de individuos que observaban a las computadoras como medios muy sofisticados en cuanto a su utilización, se han visto obligados al uso de las computadoras en su vida diaria. El hombre digital no necesita estas funciones para desenvolverse y crecer, dado que puede almacenar y recuperar

información con facilidad y rapidez. El *bit* [1] y la velocidad en su transmisión han adquirido el máximo protagonismo, hasta el punto de definir y caracterizar la era digital.

La realidad informática presenta, en ocasiones cada vez más numerosas, la utilización de sistemas informáticos en la sociedad actual. Hoy en día nadie duda de la incidencia que han tenido las computadoras en la sociedad. Cada día más son las familias que poseen una computadora en su casa y ya nadie se puede imaginar una empresa que no posea una computadora. En la actual configuración social es necesario una complejidad de relaciones interpersonales, esta complejidad lleva implícito muchas veces el sistema de servicios informáticos para consolidar relaciones sociales. El hombre organiza su vida según sus conocimientos y según sus experiencias, por tanto, a mayor conocimiento de la informática, mayor hará uso de ésta.

Ahora bien, esta interiorización de los sistemas informáticos en las formas de comunicación de los sujetos se ve influenciado por los procesos de internacionalización de las economías, los mercados y por el fenómeno de la globalización. En efecto, "la globalización como salto cualitativo de la internacionalización es una de las características definitorias de los modelos sociales postindustriales, cuya principal expresión es ser un fenómeno económico orientado a la eliminación de las restricciones a las transacciones y la ampliación de los mercados." Como consecuencia de ello se ha de agregar, sin lugar a dudas, otro fenómeno: la globalización de las comunicaciones, generado por las innovaciones técnicas. Si bien es cierto que nuestro país no está considerado como un país postindustrial, el avance tecnológico modifica altamente el desarrollo social de Bolivia. Un indicador importante para evaluar la capacidad de respuesta de las sociedades a los desafíos de la nueva sociedad en despegue, es su capacidad para incorporarse a las redes que crecientemente enlazan al mundo.

En el mes abril del año 1999, la cantidad de internautas ascendía a 100,000 y se multiplicó por cuatro en los diez meses siguientes. Según datos del Instituto Nacional de Estadística (INE), a fines del mes de mayo del año 2000, la cantidad volvió a duplicarse llegando a 820,000

[1] El bit es considerado como la unidad mínima de información digital que puedeser tratada por un ordenador. proviene de la contracción de la expresión binary digit (dígito binario).

personas que utilizaban Internet como medio de comunicación o para la adquisición de algún producto. Sin duda, podríamos llegar a decir que se trata de una de las tasas de crecimiento más elevadas.

De las cantidades anteriormente descritas, el 26% de usuarios de Internet accede al servicio desde su centro de trabajo. Otro 50% lo hace desde cabinas públicas. El resto de porcentaje, suponemos que comprendería el acceso al servicio de Internet desde cada uno los hogares de las personas que ingresan a este sistema. Por otro lado, se espera que para este año en nuestro país las inversiones publicitarias en Internet alcancen un crecimiento aproximado de 300 por ciento.

Como se puede observar la incidencia que tiene el desarrollo tecnológico en Bolivia es elevada, por lo que es innegable argumentar que nuestra sociedad se encuentra también inmersa dentro de todo el desarrollo tecnológico evidenciado en países altamente industrializados. Sin embargo, no debemos olvidar las consecuencias negativas que el propio avance trae consigo, como, por ejemplo, la aparición de nuevos riesgos para los usuarios de sistemas informáticos en la medida que deberán adoptar nuevas formas de conductas para solventarlos.

1.3.1 Nuevas Formas de Comunicación

1.3.2. Internet Relay Chat

La comunicación mediada por computadoras ha generado nuevas formas de comunicación entre las personas como por ejemplo el fenómeno del IRC [2] .IRC es el acrónimo de *Internet Relay Cha*t, y es un protocolo que permite intercambiar mensajes en forma directa a un gran número de usuarios conectados simultáneamente a la red por medio de servidores de IRC diseminados por todo el mundo. Con frecuencia se lo utiliza para charlas simples o juegos intranscendentes, aunque otras veces se lo ha empleado para cosas más serias; por ejemplo, durante la Guerra del Golfo y en otras situaciones catastróficas, sirvió para obtener noticias en

[2] En http://www.guias.se/~oscar/adiccion/comunicacion.html. Fecha de acceso: 20 de enero del año 2002.

directo. Dicha comunicación es en tiempo real y sus implicancias y sus efectos sobre los sujetos que participan en dichas conversaciones podría llegar a ser adictivo.

1.3.3 El Correo Electrónico

Otra forma de comunicación virtual entre las personas es el uso del correo electrónico (e-mail) sin lugar a dudas, el servicio más utilizado de Internet. Este servicio permite el intercambio de mensajes entre usuarios de todo el mundo a través de este medio. Años atrás, los individuos debían de conformarse con el uso del correo postal, en donde una carta podía demorar meses en ser leída por su destinatario, sin embargo, hoy en día el uso del correo electrónico ha favorecido muchísimo no sólo las relaciones personales, sino también los negocios, la economía y la industria. [3] En tanto la realidad social ofrece un sin número de posibilidades de formas de comunicación, estas posibilidades proveen que a través de la red un individuo pueda optar por la personalidad que quiera. "La máscara que facilita la red, la facultad de simulación, permite a algunos de sus navegantes ganarse el respeto de otros usuarios, a los que no podrían acercarse en la sociedad real.

Podríamos atrevernos a decir que la comunicación social no podría conseguirse de una manera eficiente sin el empleo del uso del correo electrónico, cámaras virtuales, etc., ya que hoy en día el ser humano no puede desarrollarse de forma óptima (en tiempo y espacio) sólo con el uso de medios de comunicación tradicionales, tales como el correo postal o los videos comunes. Por estas razones, cada vez más los contactos sociales son producto de nuevas formas de avanzada tecnología. Como es sabido, el desarrollo de esta tecnología no sólo se encuadra en los cambios sociales que produce el uso de los sistemas informáticos. La industria, la economía, la educación, la administración pública, los sistemas financieros etc., son testigos de los cambios que se han producido en estos últimos cincuenta años. El Derecho no es la excepción.

Si bien es cierto que el presente trabajo no pretende enunciar de manera amplia todos los cambios que se han originado desde la creación de los medios informáticos, ya que de esto, se ocupa el Derecho Informático, nos parece necesario destacar la relación existente entre la

[3] En http://delitosinformáticos.com-/noticias/98370553075358.htm Fecha de acceso: 10 de enero del año 2002.

informática y las diversas ramas del Derecho, las mismas que han tenido en muchos casos que cambiar su normativa vigente y/o adaptar su derecho positivo a las necesidades que la informática obliga.

De igual manera, en cuanto al Derecho Comercial, mediante el uso del Internet es posible adquirir todo tipo de productos en la red, tales como libros, medicamentos etc.

En efecto, si bien es cierto que todos estos avances tecnológicos son bien recibidos por la sociedad; este desarrollo sumado a los fenómenos económicos de la globalización y de la integración económica dan lugar a la conformación de nuevas modalidades de delitos clásicos, así como a la aparición de nuevas formas delictivas así tenemos por ejemplo: sabotaje informático, etc.

1.4 Principales Características en la Red

1.4.1. El Ciberespacio

"El desarrollo alcanzado por los elementos electrónicos, unión con las redes de telecomunicaciones determinan la creación de una zona donde las personas pueden interactuar sin estar físicamente presentes" . Esta zona, es denominada "ciberespacio".

Por ciberespacio se puede entender el lugar en el cual ocurren determinadas conductas, desde conversaciones telefónicas, comunicación por chat, envió de mensajes electrónicos, compra de artículos de diversas clases, etc.

"El concepto de ciberespacio, expresa la directa incidencia de la nueva tecnología sobre la efectividad de los límites territoriales de los Estados y sobre las políticas que, sin integrar este concepto operativo puedan diseñar y pretendan hacer valer". Así, el ciberespacio origina una nueva cultura, la denominada "cultura tecnológica". El desarrollo del ciberespacio es cada vez tan exorbitante, que Internet cuenta ya con más de 150 millones de usuarios en el planeta.

Cada hora aparecen 6,500 nuevas páginas en la Red, cada día se conectan 15,000 nuevos usuarios y para el presente año 2002 se espera que superen los 350 millones.

Por último, "podemos inferir que el ciberespacio es una realidad nueva que va adquiriendo día a día mayor importancia estratégica desde el punto de vista: empresarial, cultural, político y social; que para su funcionamiento necesita de un medio físico adecuado, el mismo que se encuentra en Internet".

1.4.2. El Anonimato

Ahora bien, "las nuevas formas de comunicación electrónica ahora dan el ámbito de la subjetividad. El anonimato de la red promueve igualmente actitudes críticas abiertas, puntos de vista excéntricos e impopulares, estimulando la promiscuidad del yo. El género, la orientación sexual, la edad, todo puede cambiar al instante y a voluntad, en la creación de una nueva y efímera identidad". Por tanto, las personas en la red pueden poseer cualquier nacionalidad, cualquier inclinación religiosa, cualquier tipo de vida y ser identificados bajo una personalidad virtualmente construida. No en vano se dice que Internet es la reina del anonimato. Este hecho es de enorme importancia, toda vez que la sociedad está construida sobre las bases de una comunicación personalizada, en la cual los contactos directos e individualizados son su característica principal; sin embargo, se expande hoy en día en la sociedad la idea del anonimato en las relaciones sociales, es decir, la despersonalización de los contactos como, por ejemplo, cada vez sabemos menos quien es nuestra contraparte en una operación bancaria debido a los cajeros automáticos. En la comunicación que se origina por medio del chateo en Internet, la mayoría de personas no se conocen físicamente sino sólo a través del medio de comunicación virtual.

Así, aparecen hoy día nuevas formas de criminalidad que son difíciles de comprobar. "En primer lugar, porque las nuevas técnicas han supuesto la incorporación al mundo jurídico de un nuevo ámbito de regulación (los derechos u obligaciones consecuentes a la creación, distribución, uso del hardware y el software, a las bases de datos, a la contratación de servicios informáticos o a la transferencia electrónica de datos); y porque tales aparatos y tales técnicas

han supuesto cambios revolucionarios en la manera de entender las relaciones jurídicas tradicionales".

1.5 Los Sujetos en la Red

1.5.1 Cinco Categorías

Concordamos con De Miguel, cuando establece cinco categorías para diferenciar a los sujetos en la Red, las mismas que se detallan a continuación.

1. Los Operadores de telecomunicaciones: Quienes disponen de la infraestructura que permite la transmisión de datos.
2. Los proveedores de acceso a Internet: Quienes proporcionan el servicio de conexión a la Red.
3. Los proveedores de servicios de Internet: Servicios que son ofrecidos como el buzón de correo electrónico, elaboración de páginas web, etc.
4. Los suministradores de servicios en línea y suministradores de contenido: Los primeros proporcionan información a los abonados a sus sistemas, mientras que los segundos son los titulares de la información y los datos que constituyen los contenidos, normalmente de las páginas web.
5. Los usuarios: Que en un primer momento consistían en un grupo de personas homogéneas personas que poseían alto cocimiento informático sin embargo, la heterogeneidad es la principal característica hoy en día entre los usuarios.

Como se puede apreciar de la clasificación descrita, existe una relación de dependencia entre los sujetos que intervienen en la red, los mismos que forman parte de un gran engranaje que hace posible la comunicación y la obtención de información entre los usuarios. Afirmamos esto debido a que la falta de alguno de los sujetos descritos haría imposible la configuración de la red.

Podemos advertir que en estas cinco categorías se ha configurado el mercado en la red, sin embargo, debemos señalar que no se trata de un número cerrado, ya que la constante y vertiginosa evolución de los sistemas informáticos harán que en un breve plazo sean integrados nuevos sujetos en la red.

Por otra parte, la precisión de los sujetos en la red no sólo es una cuestión de identificación, porque, además, permite atribuir determinadas competencias a los autores en la red y así atribuir responsabilidades, inclusive penales.

1.6 Necesidad de Regulación del Internet.

1.6.1 Contenidos Ilegales en Internet

Los contenidos ilegales en la Red son el problema más difícil de atacar por parte de los países. El acceso libre a contenidos ilícitos en Internet se ha convertido en uno de los problemas fundamentales de los Estados a la hora de regular su uso. Todos los países coinciden con la necesidad de fomentar el desarrollo de Internet y las nuevas tecnologías, y generalizar su uso para el comercio y las comunicaciones. Pero una de las primeras alarmas que surgen en este proceso es cómo hacer compatible ese desarrollo con el aumento exorbitante de los contenidos de pornografía, armas, racismo o drogas ilegales terminando en el espionaje. [4] No es tan cierto que Internet sea un territorio no regulado. Por un lado, "existen normas sencillas de carácter formalista, expresas para un uso más rápido y eficaz en la red."

Se tratan de normas de cortesía, relativas, por ejemplo, a cómo debe emplearse el lenguaje en la red, a la extensión y número que deben tener los mensajes de correo electrónico, etc. Sin querer abordar con profundidad el ámbito de las normas de cortesía conocidas también como las "*nettiquettes*", se considera que éstas, devienen en pautas de comportamiento eficaces y generalmente respetadas, tales como no usaras un ordenador para dañar a otros, no entraras en colisión ni interferirás con el trabajo digital ajeno, no violarás los archivos ajenos, no usarás un ordenador para robar, no usarás un ordenador para mentir, no usarás o copiarás software por el

[4] Página Web del Boletín de Noticias de Delitos Informáticos. Sección: Articulos. Fecha de acceso. 19 de enero del año 2002.

que no has pagado, no usarás los recursos de un ordenador ajeno sin autorización, no te apropiarás del trabajo intelectual ajeno, habrás de considerar las consecuencias sociales del programa que "escribes" y usarás un ordenador de manera tal que muestres consideración y respeto.

Sin embargo, la otra cara de la moneda nos muestra que son muy pocas las personas que consideran este tipo de normas, máxime cuando en la red como hemos visto prevalece el anonimato de los individuos, por lo que se podría llegar a decir que la educación cibernética aún se encuentra en forma incipiente; se cuestiona, precisamente, que dadas las características de Internet, estas normas ejerzan una real y verdadera coerción entre los usuarios en la Red.

Los usos asociados a Internet requieren de instituciones jurídicas tradicionales que se adecuen para dar solución a aquellas conductas antisociales que se producen en la red, así como la creación de nuevas instituciones jurídicas que tutelen estos casos. Sin embargo, para este planteamiento es necesario considerar el principio de "universalidad" que rige en Internet, considerando así una regulación internacional. Ahora bien, el explosivo crecimiento de Internet como medio comercial impone nuevos desafíos en el Derecho Penal, por ello resulta necesaria la determinación de las conductas atentatorias a la red que puedan y deban ser comprendidas en una regulación jurídico penal.

En nuestra opinión, respecto de si se deben controlar o no los contenidos que proporciona Internet, pensamos que desde el momento en que se comprueba que se están cometiendo conductas antisociales a través de la red, es innegable la necesidad de una debida regulación. Sin embargo, esta regulación no debe perder de vista el objetivo por el que se creó Internet, compartir información, conocimientos, ideas, etc.

Así, somos de la opinión que se debe crear una instancia previa a la penal, en donde se regule las actividades ilícitas en la red y en los sistemas informáticos y se establezca qué conductas están permitidas y cuáles constituyen un daño tanto para los individuos como para los sistemas informáticos, como por ejemplo, el envío de publicidad no deseada, más conocido como el spamming y aquellas conductas atentatorias a la red, pero que no llegan a constituir la

comisión de un delito. De esta manera, se crearía una Institución con leyes y normas propias que regulen las actividades en la red, todo ello con la finalidad de poder distinguir cuantitativa y cualitativamente las actividades ilícitas con significación jurídico penal de aquellas que seguirán sólo una regulación administrativa.

1.6.2 **La *Free Net***

A pesar de lo señalado en los apartados precedentes, pareciera ser que cualquier intento de regulación y limitación de determinadas actividades antisociales en la red se verá en un futuro truncado, ya que se encuentra en proyecto la *"Free Net"*.

La aplicación *"Free Net"* ha sido diseñada precisamente con la intención de impedir cualquier control para los mensajes o informaciones que se expiden desde cualquier punto que aplique tal tecnología.

El uso de la multipolaridad de Internet consigue que los mensajes se copien y multipliquen instantáneamente al salir del servidor, de modo que quedan automáticamente a disposición de todos los ordenadores conectados a la red. Mediante este proyecto, se puede acceder a una red muy similar a Internet, sin embargo, los puntos que diferencian a *"Free Net"* constituyen una bomba de tiempo para el Derecho Penal. Mediante este sistema, la información es almacenada en los ordenadores de las personas conectadas.

Así, no sólo se estaría compartiendo información como en el modelo tradicional, sino que sería imposible el censurar o eliminar publicaciones, ya que se desconocería dónde está almacenada dicha información debido a que las conexiones se harían de forma anónima siendo mucho más sencillo acceder a la información más demandada, ya que ésta se duplica a medida que se va desplegando por la red. [5]

Esperamos que el mencionado proyecto no llegue a su realización, ya que de lo contrario, podría existir una red privada internacional de delincuentes de todos los niveles, delincuentes

[5] En http://www.delitosinformaticos.com/articulos/freenet.htm. Fechade acceso: 12 de diciembre del año 2001

que serían inubicables como autores de diversos delitos informáticos, los mismos que gozarían de impunidad bajo la protección de la red privada *"Free Net"*.

1.6.3 Amenazas en Internet

Mientras uno navega por Internet, existen todo tipo de amenazas que se pueden originar por malos usurarios. Las amenazas en Internet están latentes para el individuo que ingresa diariamente a este amplio mundo de información como es Internet.

En el lenguaje informático se denomina "amenaza" a la violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo) que podría efectuar una persona, máquina, suceso o idea, dada una oportunidad. Un ataque no es más que la realización de una amenaza. Y las categorías de amenaza o ataques que pueden producirse cuando una persona utiliza el Internet, son las siguientes:

a. Interrupción: Es un ataque contra un recurso del sistema que es destruido o deshabilitado temporalmente.
b. Interceptación: Este es un ataque de una entidad que consigue acceso a un recurso no autorizado. Dicha entidad podría ser una persona, un programa o una computadora.
c. Modificación: Este es un ataque de una entidad no autorizada que consigue acceder a un recurso y es capaz de modificarlo.
d. Fabricación: Este es un ataque de una entidad no autorizada que añade mensajes, archivos u otros objetos extraños en el sistema.

Asimismo, existe diferencias entre ataques pasivos y ataques activos en Internet. En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la observa, con el fin de obtener la información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación puede consistir en:

a. Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los mensajes interceptados.
b. Control del volumen de tráfico intercambiado entre las entidades interceptadas, obteniendo así información acerca de actividad o la inactividad inusuales.
c. Control de las horas habituales de intercambio de datos entre las entidades de comunicación, para extraer información acerca de los períodos de actividad.

Cabe señalar, que al igual que los sujetos en la red, los ataques tanto activos como pasivos, no constituyen de ninguna manera números cerrados para la configuración de las amenazas, ya que cada día se originan nuevos tipos de ataques y/o amenazas para los sujetos que ingresan a Internet. Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos de seguridad de la información.

Los ataques activos implican algún tipo de modificación en el proceso de transmisión de información a través de la red o a creación de un falso proceso de transmisión, pudiendo subdividirse en cuatro categorías:

a) Suplantación de identidad, el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo.
b) Reactuación, uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado.
c) Modificación de mensajes, una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.
d) Degradación fraudulenta del servicio, impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones.

Pareciera ser, como se ha podido apreciar de las conductas descritas, que Internet no ha sido diseñado para ser seguro, la inexistencia de fronteras presenta ciertos riesgos tanto para los usuarios como para los servidores.

"La pretendida sustitución de los límites territoriales por nuevas fronteras propias de Internet, junto con la independencia atribuida a las redes en su funcionamiento y su supuesta transformación en comunidades con poder para imponer sus propias reglas, son elementos que se encuentran en el origen de uno de los planteamientos básicos en lo que respecta al régimen jurídico en Internet".

Por lo expuesto, concluimos el presente punto señalando que la necesidad de una regulación de Internet es urgente no sólo por el hecho que las normas de cortesía no producen un efecto coercitivo o por las amenazas latentes tanto pasivas como activas que se pueden generar en la red, sino especialmente por el hecho que es necesaria la creación de una institución que regule las conductas que no están permitidas en la red para que de esta manera, se lleve a cabo un buen funcionamiento entre los sujetos que utilizan este amplio campo de la información.

Sólo a través de la regulación de la red en una instancia previa a la penal, podrá orientarse a los usuarios sobre el correcto uso y funcionamiento de la misma, podrá delimitarse las conductas que son permitidas de aquellas que son prohibidas y, luego, definirse aquellas que requieren de una regulación jurídico penal.

Por último, debemos advertir que para la definición de las formas de intervención sobre aquellas conductas nocivas en la red, resulta necesario la previa determinación del objeto jurídico de protección, de ello nos ocuparemos en el primer capítulo de la segunda parte de la presente investigación.

Capitulo II

ALGUNAS PRECISIONES ACERCA DE LA CRIMINALIDAD INFORMÁTICA COMO NUEVA FORMA DE CRIMINALIDAD

2.1 Aspectos generales de la criminalidad informática

Las líneas de este subcapítulo obedecen a la preocupación constante por las recientes formas de criminalidad que han sido tratadas por la dogmática penal tanto en artículos, revistas, como en diversos congresos sobre la novedosa forma de criminalidad, denominada "criminalidad informática".

Mucho se habla de los grandes beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual, sin embargo, el desarrollo tan amplio de la tecnología informática ofrece también un aspecto negativo, ya que se han generado nuevas conductas antisociales que se manifiestan en formas que no era posible imaginar en el siglo pasado. Los sistemas de computadoras ofrecen oportunidades nuevas y muy complicadas de infringir la ley y han creado la posibilidad de cometer delitos tradicionales en formas no tan tradicionales.

El comercio en la Red es un lugar muy apetecible para que personas sin escrúpulos o criminales con acceso a nuevas tecnologías, puedan acceder a sistemas remotos y cometer robos electrónicos al detectar puertas traseras en los sistemas de las Empresas. Por este motivo es importante que las naciones tomen medidas más concretas en esta materia para evitar llegar a un caos en esta materia.

La enorme evolución de la informática ha transformado al mundo en una gran tecnología, la cual nos facilita el que hacer diario y la eficacia de nuestro trabajo, sin embargo, así como ha transformado al mundo, la tecnología también ha transformado las antiguas conductas delictuales en los ahora llamados "delitos informáticos", las empresas que sufrieron de ataques cibernéticos (últimamente) fueron, entre otras, el portal de Internet Yahoo, la tienda minorista

Amazon.com, el lugar de subastas Ebay, la tienda de descuentos Buy.com, la cadena CNN interactive [6] y ZDNet, la progresiva implantación de las nuevas tecnologías en todos los ámbitos de la denominada sociedad de la información ha disparado el uso ilegal de aplicaciones de software en todo el mundo, en 1999 se hicieron famosos los virus Melissa, Chernovyl, Explore Zip, Babylonia y Bubleboy; en el año 2000 el virus I LOVE YOU conmovió al mundo entero causando daños, en algunos casos, irreparables, los fraudes en Internet aumentaron significativamente en el año 2000 y representaron dos tercios del total de casos presentados en el Servicio de Crímenes Comerciales de la Cámara de Comercio Internacional (ICC). Según el informe, 2 mil 776 de los 4 mil 139 casos referidos por sus miembros estuvieron directamente relacionados al crimen, fraude y falsificación a través de sitios web que ofrecen mercancía o servicios falsos, dicha encuesta mostró que en el año 2000, esta oficina salvó a sus miembros de pérdidas de alrededor de 2 millones 300 mil dólares, advirtiéndoles acerca de las negociaciones con esta nueva generación de criminales que habían sido previamente investigados". Noticias como éstas son temas tratados todos los días en los medios de comunicación.

Es innegable, que el uso de las nuevas tecnologías conduce a la ampliación y creación de nuevos delitos en todas las partes del mundo. Es por conductas que son producto del desarrollo tecnológico que se dice que el moderno Derecho Penal necesita asumir y afrontar los nuevos conceptos y estrategias de la criminalidad, sobre todo en conexión con nuevos fenómenos o formas delictivas.

Por "criminalidad informática" se pueden señalar conductas tales como la burla a los sistemas de dispositivos de seguridad, tanto en cajeros automáticos, como en máquinas tragamonedas, manipulaciones técnicas en el sistema de televisión pagado, invasiones a computadoras, correos o sistemas mediante una clave de acceso, revelación de secretos por parte del personal de la institución bancaria, fraudes en la telefonía celular móvil, conductas antisociales de personas que ingresan a sistemas no autorizados, sustracción de información, envío de mensajes falsos, hasta la alteración de datos que provocan cada vez más pérdidas de miles de

[6] Según las informaciones procedentes de Atlanta sobre el ataque de "bloqueo de servicio", los *hackers* saturaron un sitio en la red con mensajes inútiles que atoraron sus computadoras lo que produjo la alteración en las operaciones del sitios noticioso durante varias horas.

millones de dólares cada año. Como se puede desprender de lo anteriormente establecido, la utilización de computadoras en la economía, industria y, sobre todo, en el sector de bancos y seguros, genera también la aparición de nuevas formas de conductas delictivas que pronostican desde ya, el origen de una criminalidad informática transnacional. En consecuencia, la interconexión global posibilitada por el Internet trae consigo, una nueva calidad de criminalidad que afecta numerosos ámbitos de la vida y la economía.

Es preciso señalar que el concepto de "criminalidad informática transnacional" no se deberá de confundir con el término "criminalidad organizada." Como hemos explicado, la criminalidad informática será transnacional cuando las conductas delictuales traspasen las fronteras de los países.

Por "criminalidad organizada", establece la UNION EUROPEA que la define según 11 requisitos, de los cuales como mínimo han de concurrir 6, en los siguientes términos:

1. Más de dos personas.
2. Distribución entre más de dos personas.
3. Permanencia.
4. Control interno.
5. Sospechosas de la comisión de un delito grave.
6. Actividad internacional.
7. Uso de estructuras comerciales o de negocios.
8. Blanqueo de dinero.
9. Presión sobre el poder público.
10. Ánimo de lucro.

Por este motivo, el crecimiento del comercio en la Red introduce dos retos para tratar el crimen cibernético:

A. Determinar exactamente en qué lugar se está realizando el delito.
B. El problema de localizar al sospechoso.

Actualmente hay escasos acuerdos internacionales que permiten a las diferentes policías y diferentes países compartir información, más allá de los tratados, para criminales detenidos en terceros países. Ahora bien, así como vemos la necesidad de regulación de las conductas que se originan por el avance tecnológico, no debemos perder de vista que al ser reguladas, también debemos de recordar el principio de ultima ratio que le asiste al Derecho Penal.

2.2 Conductas nocivas que se cometen a través de sistemas informáticos y de Internet.

Existen dos posiciones respecto de las conductas que originan el "delito informático". La primera comprende conductas cuya única característica especial radica en el empleo de una computadora. La segunda posición consiste en toda conducta ilegal que requiere del conocimiento de la tecnología informática para su perpetración, investigación y prosecución, de tal forma que el empleo mismo del medio informático le permita su diferenciación respecto de un delito común que utilice como medio de comisión la computadora. Sin embargo, ha de tenerse en cuenta que las nuevas técnicas informáticas no son simplemente el instrumento para la comisión de un delito, sino que en muchas ocasiones son el mismo objeto de la conducta delictiva. Nos parece necesario señalar algunas de las conductas más comunes que se cometen a través de los sistemas informáticos y de Internet, sin embargo esta clasificación es una simple enumeración de las conductas cometidas por los delincuentes informáticos en los últimos años, por lo que no se deberá pensar que constituyen la totalidad de conductas nocivas e ilícitas existentes.

2.3 Introducción de datos falsos o "Data Diddling"

Consiste en manipular las transacciones de entrada al computador con el fin de ingresar movimientos falsos total o parcialmente, o eliminar transacciones verdaderas que deberían haberse introducido. Es un método al alcance de muchas personas que desarrollan tareas en los servicios informáticos para lo cual no es necesario poseer conocimientos técnicos especiales sino tan sólo haber percibido las deficiencias de control que muestre un determinado Sistema. Se trata de una manipulación de los sistemas o programas informáticos, cuya alteración genera

información distorsionada que puede tener incidencia económica y causar un perjuicio patrimonial, de ahí que pueda ser considerada como una conducta fraudulenta.

2.4 El Caballo de Troya o "Trojan Horse"

Atendiendo a su denominación, podemos precisar que este método consiste en la inclusión de instrucciones dentro del programa de uso habitual de una rutina para que realice un conjunto de funciones, desde luego no autorizadas, para que dicho programa ejecute en ciertos casos de una forma distinta a como estaba previsto. Puede tratarse en determinados casos de la ejecución de cálculos erróneos, por ejemplo, aumentando el importe de la lista de un empleado, desviando ingresos hacia cuentas ficticias, etc. También puede presentarse cuando se imprimen documentos no autorizados o inclusive no imprimir documentos reales, por ejemplo, emitir cheques a proveedores reales cuando previamente se les ha cancelado su deuda, ya que se ha alterado la forma de pago transfiriendo los fondos a una cuenta que pertenece al defraudador.

Por sus características es necesario que el agente posea una capacidad técnica suficiente, al menos saber programar y, además, tener acceso al programa para poder manipularlo. Es importante agregar que en todo este tipo de ilícitos el programa manipulado ha estado en funcionamiento habitual desde hace un buen tiempo y casi nunca se trataba de un programa de nueva creación. El motivo es muy simple, los programas nuevos suelen ser sometidos a procesos de revisión y chequeo para detectar cualquier anomalía que puedan afectarlos.

Sin embargo, un programa que ha estado en funcionamiento correctamente durante un prolongado tiempo no es cuestionado, y salvo casos absolutamente excepcionales, jamás sus resultados son sometidos a comprobación. Debido a ello la modalidad del Caballo de Troya es una de las más peligrosas formas delictivas y al mismo tiempo difícil de detectar.

Al igual que la conducta anterior, se trata de una manipulación fraudulenta de los sistemas o programas informáticos generalmente practicados con fines económicos.

2.5 El Salame, Redondeo de Cuentas o "Rounding Down"

Es tal vez la técnica más sencilla de realizar y la que menos probabilidades tiene de ser descubierta. La modalidad consiste en introducir o modificar unas pocas instrucciones de los programas para reducir sistemáticamente una cantidad de dinero transfiriéndola a una cuenta distinta o proveedor ficticio que se abre con nombre supuesto y que obviamente la controla el defraudador. Por ejemplo, puede darse el caso de disminuir constantemente en unos céntimos las cuentas corrientes de un cliente bancario, pequeños saldos de proveedores, reducir los talones de impresión para el pago a acreedores, transfiriendo luego estas pequeñas cantidades a la cuenta particular del autor.

También se suele aplicar esta modalidad cuando se calculan los intereses de cuentas corrientes bancarias, de libretas de ahorro, de depósitos a plazo o bien cuando se elabora el cálculo de la planilla de los trabajadores de una empresa, procediéndose a eliminar el criterio generalizado de redondeo de céntimos a la alza o a la baja de dinero en montos exactos y a cambiarlo por la eliminación total de dichos céntimos que son transferidos a una determinada cuenta o a nombre de un empleado real o ficticio.

La razón principal por la que es tan difícil descubrir este tipo de hechos es porque las cuentas o el importe total del listado, siguen estando "cuadrados" o contablemente equilibrados en el arqueo de caja por lo que no se deduce ninguna señal de alarma que pueda indicar lo que está sucediendo. Por ejemplo, se da el caso al redondear cuentas bancarias y acreditar los montos resultantes a una cuenta determinada repitiendo automáticamente la operación sin intervención posterior del autor. La finalidad económica de la conducta fraudulenta se torna evidente en el presente caso, de ahí que se trate de otra de las formas de manipulación informática con incidencia patrimonial.

2.6 Uso Indebido de Programas o "Superzapping"

Es el uso no autorizado de un programa de utilidad para alterar, borrar, copiar, insertar o utilizar cualquier forma no permitida, los datos almacenados en el computador o en los

soportes magnéticos. El nombre proviene de un programa llamado "*Superzap*" y es una especie de llave que permite abrir cualquier rincón de una computadora por más protegida que pueda estar. Estos programas pertenecen al grupo de los llamados "Programas de Acceso Universal" de uso imprescindible en cualquier instalación de ciertas dimensiones cuando fallan los procedimientos normales para recuperar o reiniciar "el sistema". Efectivamente, cuando un sistema informático almacena gran cantidad de información se hace necesario disponer de un mecanismo de emergencia que permita entrar a cualquier punto del sistema en caso que se produzca alguna avería o lo que normalmente se ha denominado "caída del sistema".

Es por esta razón que se justifica la existencia de los llamados "Programas de Acceso Universal" (PAU); herramientas imprescindibles en cualquier instalación de ciertas proporciones cuando fallan los procedimientos normales para "recuperar" o "reiniciar" el sistema.

Los programas de utilidad son una herramienta valiosa y muchas veces imprescindible en los casos de caída del sistema pero igualmente un arma peligrosísima cuando se encuentra al alcance de personas que lo utilizarán con otras intenciones. No obstante, suelen estar archivados en las librerías de producción junto con el resto de programas de uso común y generalizado, con lo cual cualquier técnica podría tener la posibilidad de utilizarlo indebidamente. Con la modalidad de "*superzaping*" es posible alterar los registros de un fichero sin que quede constancia de tal modificación, lo cual hace sumamente difícil descubrir y detectar al autor de tales eventos. Aparentemente se suelen registrar los ingresos a un sistema y las transacciones que se han procesado en una determinada operación actualizando los registros con un dato específico como, por ejemplo, la hora de ingreso.

Sin embargo, los programas de acceso universal permiten modificar directamente la información sin activar los programas de actualización ni introducir ninguna operación al computador. Aún más, sin dejar rastro si la persona que lo está usando sabe como realizarlo. Bastaría con hacer coincidir el monto de la modificación no autorizada con el comienzo o el final de la ejecución del programa verdadero de actualización y algún error intencionado en el sistema que requiera la utilización del programa de acceso universal. En ese preciso momento

tendremos cargado en el sistema el fichero que queremos modificar y el programa que nos permite modificar, no registrándose por lo tanto su utilización no justificada ni del fichero, ni del programa de utilidad. Cuando se descubran las alteraciones de los datos se pensará que ha sido un funcionamiento erróneo del programa de actualización, un funcionamiento inadecuado del computador o una transacción errónea y en esas direcciones se encaminará la investigación, las cuales seguramente no abordarán a ningún puerto. En el mejor de los casos, si se descubre como se realizó la alteración de datos, será muy difícil probarlo. *(Un conocido caso con el método del superzaping ocurrió New Jersey en donde el autor comenzó a desviar fondos desde las cuentas de diferentes clientes hacia la de unos amigos sin que quedara en el sistema ninguna evidencia de las modificaciones efectuadas en los saldos de cuenta corriente. El delito se descubrió por los reclamos efectuados por uno de los afectados, lo cual motivó una investigación que culminó con la detención del sujeto).*

En definitiva, la técnica del "superzapping" representa una forma de acceso a sistemas o programas informáticos que puede o no estar autorizado por un titular, lo cual incide en la licitud o no de la conducta, dicho acceso puede orientarse a cuestiones económicas o al conocimiento de información o datos reservados, por lo que puede tener una incidencia patrimonial como también para la intimidad.

2.7 Puertas falsas o "Traps Doors"

Es una costumbre en el desarrollo de aplicaciones complejas que los programas permitan introducir interrupciones en la lógica de los desarrollos del mismo, con el objeto de chequear por medio de los procesos informáticos si los resultados intermedios son correctos, producir salidas de emergencia y de control a fin de guardar resultados parciales en ciertas áreas del sistema para comprobarlos después. Inclusive algunas veces este procedimiento se enlaza con rutinas del sistema operativo para facilitar una "puerta entrada al programa" que no estaba prevista, pero de esta manera facilitan la labor de desarrollo y prueba de programas.

El problema radica en tener la seguridad de que cuando los programas entran en proceso de producción normal, todas esas "puertas falsas" hayan desaparecido.

Y aunque parezca mentira, las puertas creadas no se eliminan, permitiendo a su paso puertas de acceso al programa con el agravante que por ser elementos temporales creados por la computadora no constan en la documentación del sistema.

Es de uso frecuente para posibles recuperaciones en caso de "caída del sistema" a mitad de un proceso, ir grabando en cinta resultados intermedios o copia de las transacciones procesadas, o incluso ciertas áreas de memoria para la recuperación más rápida y sencilla. Las puertas falsas son: por personas que no las crearon, pero que una vez descubiertas se aprovechan de ella sin necesidad de poseer una formación informática profunda. *(Tal es el caso de unos ingenieros en una fábrica de automóviles en Detroit que descubrieron una puerta falsa en una red de servicios público de time-sharing de Florida. Después de una serie de intentos consiguieron ingresar con una llave de ingreso de alto nivel, según parece la del propio presidente ejecutivo de la compañía y utilizándola pudieron apoderarse de diferentes programas clasificados de carácter reservado y archivados en el computador bajo la denominación de secreto comercial, al mismo tiempo que utilizaban la red sin cargo económico alguno).*

Estas técnicas inciden en la forma de acceso a los sistemas o programas informáticos, por lo que tendrá relación en cuanto se trata de un ingreso no autorizado. En tal virtud, es una conducta antesala a aquellas vinculadas a fraudes o sabotajes informáticos.

2.8 Bombas Lógicas o "Logic Bombs"

Previamente debe señalarse que este tipo de delito se ejecuta para producir daños sin otro beneficio que el placer de perjudicar.

El método consiste en introducir en un programa un conjunto de instrucciones no autorizadas para que en una fecha o circunstancia predeterminada se ejecuten automáticamente desencadenando el borrado o la destrucción de información almacenada en el computador, distorsionando el funcionamiento del sistema o produciendo paralizaciones intermitentes.

(Un conocido caso de bomba lógica se presentó en Septiembre de 1981 y tuvo como protagonista un programador de computadoras de 26 años de edad que trabajaba para el departamento de defensa en Washington D.C. en los Estados Unidos de Norteamérica. Resulta que el programador se sintió frustrado y discriminado al no recibir una promoción que supuestamente le correspondía, por lo que decidió vengarse. El trabajo de este empleado consistía en el mantenimiento de las nóminas del sistema de personal lo que le permitía tener acceso a todos los programas y a la información contenida en la base de datos de dicho sistema. Decidido a vengarse escribió unas rutinas para incluir en los programas que a cierta señal se borren y destruyan gran parte de la información que él procesaba en los sistemas. Posteriormente comenzó a buscar otro trabajo para lo cual solicitó vacaciones en su empleo siendo así que consiguió un nuevo trabajo. Unos días después que recibió la confirmación de su nuevo empleo, y en ese mismo momento aprovechando la hora del almuerzo, introdujo la rutina que tenía programada, incluyendo un control que se activaría seis meses desde la fecha de su salida de su anterior empleo. En efecto, seis meses después de haber abandonado a su anterior trabajo cuando se estaban procesando las nóminas de personal la rutina introducida por él funcionó como había previsto su autor, borrando la mayor parte de información de los registros de personas. Dado que el programa había estado funcionando largo tiempo y nadie dudaba de su funcionamiento se volvieron a probar con las copias de seguridad las que también resultaron dañadas. El descubrir el motivo de los daños al sistema y recomponer la información requirió gran esfuerzo de personal y de tiempo, lo que puede dar una idea del costo que se supuso, pero no fue posible probar la autoría del hecho, aunque las sospechas recayeron sobre su verdadero autor, el que nunca fue acusado formalmente, ni juzgado ni castigado).

Esta modalidad es una forma bastante extendida, utilizada por muchos fabricantes de paquetes de software con el fin de asegurar el importe de los mismos.

Consiste en programar una instrucción que revisa la fecha del día, lo que permite una fecha de caducidad oculta que ha introducido el fabricante del software al instalarlo en el computador del cliente y que no será eliminada o prorrogada hasta que el cliente pague los nuevos derechos.

Esto constituye una verdadera forma de coacción ilegal, pero que es utilizada por una falta de protección adecuada de los derechos de autor y los derechos del consumidor o usuario. Esta conducta es denominada comúnmente como daños o sabotaje informático.

2.9 Ataques Asincrónicos o "Asynchronic Attacks"

Los sistemas informáticos en la mayoría de los casos funcionan ejecutando más de dos comandos u órdenes a la vez o en otras circunstancias una instrucción sucesiva de la otra en forma secuencial. Cabe recordar que el sistema operativo es el conjunto de programas que controlan el funcionamiento del computador y todos sus dispositivos periféricos (discos, cintas, impresoras), la entrada de los datos procesados por el programa, la ejecución de los programas de las diferentes aplicaciones y la salida de la información elaborada hacia los dispositivos exteriores.

El sistema operativo es imprescindible para el funcionamiento del equipo y su desarrollo es responsabilidad del fabricante. Una de las principales funciones del sistema operativo de las computadoras es controlar la ejecución simultánea de varios programas a la vez. Otra función fundamental del sistema operativo es optimizar la ocupación de memoria central reasignando áreas en función de las necesidades de cada uno en los programas que están ejecutando en cada momento. De otro lado el sistema operativo asigna a los programas otras funciones de clasificación, intercambio, etc. Por lo tanto, el sistema operativo es quien controla y maneja todos los errores que pueden producirse tanto en la computadora como en los programas que se están ejecutando, avisando al operador por medio de mensajes de cualquier situación anormal que se produzca.

Pues bien, los programas funcionan en forma sincrónica, es decir, ejecutando sus instrucciones en un orden fijo predeterminado de nivel en nivel, en tanto que el sistema operativo funciona en forma asincrónica, es decir, ejecutando sus órdenes de manera independiente, en función de una gran cantidad de factores ajenos a él. Como consecuencia, se produce rigurosidad en los programas en ejecución conformando las llamadas "colas de espera" que se van a ir

desbloqueando en función de la disponibilidad de los datos o comandos que estaban esperando. Uno de los típicos casos es el que puede producirse en los llamados puntos de recuperación del sistema. Cuando se procesan programas complejos y de larga duración se establecen puntos de recuperación cada cinco o diez minutos, por ejemplo, gravando en soporte magnético externo (diskettes) el estado del programa, lo que implica que si el sistema "se cae", es decir, que se interrumpa el proceso por una situación de error no recuperable, por ejemplo, falta de energía eléctrica, no es necesario retroceder desde el principio del programa sino bastará hacerlo desde el último punto de recuperación ya que todo se encuentra gravado, reiniciando de esta manera el proceso. Pues bien, si entre dos puntos de recuperación se provoca voluntariamente una "caída del sistema" y en el intermedio se manipula los parámetros en que se va a apoyar el sistema operativo, para reiniciar resulta obvio que las condiciones en que se ejecuten serán distintas a las originales por lo que sus resultados serán por lo menos diferentes, fraudulentos o erróneos. Se trata de una conducta de sabotaje informático que puede orientarse hacia la obtención de un provecho económico para el agente o un tercero, o hacia la causación de daños de los sistemas o programas informáticos.

2.10 Recojo de Información Residual o *"Scavenging"*

Este procedimiento se basa en aprovechar los descuidos de los usuarios ya que la información ha sido abandonada sin ninguna protección como residuo de un trabajo real efectuado con la debida autorización.

La denominación proviene del anglicismo *"to scavenge"* que significa recoger la basura. Simplemente se va aprovechando las finalizaciones de los trabajos reales en el computador para obtener la información residual que ha quedado en la memoria.

La modalidad más frecuente es la "impresión diferida", la cual prepara la unidad para que posteriormente imprima sin ningún tipo de protección siendo fácilmente recuperable sin necesidad de utilizar ninguna clave de acceso.

Tiene dos formas bien definidas: *scavenging* físico y *scavenging* electrónico.

a. El *Scavenging* Físico: Consiste en recoger el material de desecho que se abandona en las papeleras, encima de las mesa, en le suelo, etc., y que frecuentemente incluye listados de pruebas de programas, documentos conteniendo información de entrada a un programa a la computador, a copias de apoyo que no han sido repartidas, etc.

b. El *Scavenging* Electrónico: Consiste en aprovechar las finalizaciones de las ejecuciones de los programas realizados en el computador para obtener la información residual que ha quedado en la memoria o en los soportes magnéticos.

Una de las formas más simples del *scavenging* electrónico es cuando se ordena la impresión diferida, ya que en la computadora queda preparada la información que posteriormente se imprimirá sin ningún tipo de protección, siendo sumamente fácil recuperar la información sin la necesidad de utilizar ningún tipo de clave o cualquier procedimiento de seguridad. (*El caso más célebre de scavenging ocurrió en Los Ángeles por un estudiante de ingeniería eléctrica. El estudiante simultáneamente trabajaba como vendedor de equipos de comunicaciones lo cual le permitió adquirir un conocimiento bastante profundo de cómo operaban los sistemas mecanizados de la empresa. Al haber recogido cada mañana los papeles que depositaban en el exterior del centro de procesamiento de datos de la compañía. El estudiante simulando ser un publicista convenció a los directivos de la empresa para lanzar un boletín que reforzaría considerablemente la imagen de la compañía. Esto le permitió recopilar información, añadida a al compra de una camioneta en una subasta de la propia compañía. El estudiante pidió telefónicamente mercadería para una empresa que había seleccionado previamente. Para ser despachada por la noche por la cantidad de 30mil dólares, lo que hizo fue recoger la mercadería y distribuirla a diferentes compradores. El estudiante fue descubierto al ser denunciado por su ayudante a quien se negó a aumentar el dinero que le pagaba por sus servicios especiales. El estudiante fue acusado de varios delitos y el 5 de julio de 1972 fue condenado por el Juez M. Deal a dos meses en una correccional, 500 dólares de multa y tres años de libertad vigilada).*

Se trata de una técnica para obtener información sin autorización. Por tanto, lo importante en estos casos será el contenido de la información.

2.11 Divulgación no Autorizada de Datos o *"Data Leakcage"*

Consiste en sustraer información confidencial almacenada en un computador central desde un punto remoto, accediendo a ella, recuperándola y finalmente enviándola a una unidad de computador personal, copiándola simultáneamente. La sustracción de información confidencial es quizás uno de los cánceres que con mayor peligro acechan a los grandes sistemas informáticos. Se ha empleado también bajo la denominación de espionaje industrial, pues sería particularmente débiles al sustraerse aspectos claves de su actividad empresarial, como, por ejemplo, estrategias de mercado, nuevos productos, fórmulas de producción, inclusive hay cierto tipo de empresas que dependen de la privacidad de su información como las empresas de publicidad directa en donde tiene ficheros completos de su público objetivo.

2.12 Acceso a Áreas No Autorizadas o *"Piggyn Baking"*

Pese a no tener una traducción específica consiste en acceder a áreas restringidas dentro de la computadora o de sus dispositivos periféricos como consecuencias de puertas abiertas o dispositivos desconectados. Se da también cuando el usuario que está trabajando en una terminal en un nivel autorizado que le permite realizar ciertas funciones reservadas deja el terminal conectado, con lo que cualquier otra persona puede continuar trabajando sin necesidad de identificarse pudiendo efectuar operaciones que en condiciones normales no le estarían permitidas.

2.13 Suplantación de la Personalidad o *"Impersonation"*

Puede ser entendida como la suplantación de personalidad, fingiendo ser una persona que no es imitándola e inclusive remedándola. Algunos sistemas requieren la identificación con una clave para acceder al sistema. Más adelante se ha requerido la posesión de algo pudiendo ser una llave o tarjeta magnética. Y aún podríamos complicarlo más si adicionamos dispositivos de

reconocimiento biométrico como identificación con la palma de la mano o dactilográfica, scanners de retina o del iris, reconocimiento de voz, etc.

Un caso muy frecuente de *impersonation* o suplantación de personalidad se da en el robo de las tarjetas de crédito y de cajeros automáticos. Los autores del delito se hacen pasar por empleados de la central de tarjetas de crédito, llamando telefónicamente al titular para solicitarle que con el objeto de anular la posibilidad de utilización fraudulenta de la tarjeta robada le revele su clave secreta o personal. Como es fácil advertir, una vez descubierta la clave a la persona desconocida que las ha llamado utilizan la tarjeta para sacar el dinero de los cajeros automáticos hasta su límite máximo de crédito. (*Otro caso célebre es el que hicieron los estudiantes de una universidad norteamericana al mandar una carta en papel oficial a todos los usuarios de computadoras de la universidad advirtiéndoles que el número de conexión al sistema había sido cambiado, solicitándoles su número anterior. Posteriormente y debido a que lo primero que solicita el sistema al conectarse era la clave de identificación, los estudiantes recogieron la clave e indicaron que hasta nueva orden volvieran a usar su número antiguo, obteniendo así el número clave de todos los usuarios del sistema, descubriendo todos los secretos de los estudiantes de la universidad. Una vez descubierto el procedimiento todas las claves fueron cambiadas).*

2.14 Simulación e Imitación de Modelos o *"Simulation and Modeling"*

Se trata del uso de la computadora para simular y planificar la comisión de un delito antes de realizarlo. La utilización de la computadora se realiza de forma mediata para conseguir un fin ilícito, como ejemplos podemos señalar desde la simulación del robo de una bóveda de un banco hasta el contador que contrató los servicios contables de una empresa para estudiar detenidamente las repercusiones de los asientos fraudulentos que pensaba realizar para sustraer una cantidad importante de dinero. Aquí se difiere de los anteriores tipos de infracciones informáticas, pues el computador que puede ser usado para simular situaciones previsible o efectuar modelos que representen el comportamiento previsible de una empresa, una fábrica, una inversión, es utilizado equivocadamente con fines delictivos.

Segunda Parte

LOS DELITOS INFORMÁTICOS: MARCO LEGAL

Capítulo II
Delimitación conceptual del delito informático

3.1 El Concepto de Delito Informático

Se debe partir de la idea que todos los programas de informática pueden ser vulnerados; asimismo, de que todos los sistemas de seguridad basados en el software son vulnerables. De esta manera, las conductas delincuenciales respecto a sistemas informáticos son inimaginables, es por esto, que es necesario una delimitación terminológica y conceptual de los llamados delitos informáticos.

Sin embargo, esta delimitación no es nada sencilla y, por el contrario, como señala Romeo Casbona, las nuevas tecnologías informáticas deben ser reducidas a sus justos términos. En efecto, no se debe entender que por el mero hecho de que en una conducta intervenga un elemento del ámbito de atención de la informática ésta sea un delito informático. De mantenerse esta postura acabaría por considerarse a cualquier conducta delictiva en la que se vea implicada una computadora, como delito informático.

En primer lugar, debemos entender qué conductas están referidas a los llamados "delitos informáticos". Creemos que la falta de una definición general sobre las conductas que comprenden el llamado "delito informático" se debe a la inexistencia de una tipificación generalizada. Así, si existiera una definición sobre que es en realidad un "delito informático" para todos los países, sería mucho más fácil comprender el concepto de esta conducta. Así, encontramos términos como delitos informáticos, delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadoras, crímenes informáticos, delincuencia

relacionada con los sistemas informáticos, etc.; son denominaciones que se han creado a fin de señalar conductas ilícitas en las que se emplean sistemas informáticos. Muchos han sido los esfuerzos de expertos, tanto de juristas como de ingenieros de sistemas, sobre una definición única de delito informático. Pese a tales esfuerzos, aún no se ha conseguido dar una definición unánime sobre que es un "delito informático".

Según el material revisado para el presente trabajo, podemos llegar a decir que no existe una definición propia, tanto a nivel nacional como internacional, sobre "delito informático", ni existe un concepto uniforme sobre su significado.

Para Davara Rodríguez, no parece adecuado hablar de delito informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito. Por ejemplo, el Código penal español de 1995 no introduce el delito informático, ni admite que exista como tal un delito informático, si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático.

La Organización para la Cooperación Económica del Desarrollo (OCDE) ha definido al delito informático como cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento de datos y/o la transmisión de datos.

Por su parte Jijena Leiva, define a los delitos informáticos como toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma. Como se puede apreciar de la mayoría de autores citados, el concepto de delito informático involucra en el medio comisivo de la conducta delictuosa un sistema informático o base de datos.

Cabe agregar que la ausencia de una identificación homogénea del delito informático es también consecuencia del hecho que la mayoría de empresas no sólo no denuncia estos hechos, sino que los niega rotundamente, dado el temor al desprestigio que pudiera provocar estas

denuncias. Por ejemplo, si A ha transferido sumas de dinero a una cuenta por medio de los sistemas de cómputo del Banco X, éste no denunciará el hecho, debido a que pudiera crear un pánico colectivo a distintos ahorristas que confían en el prestigio y seguridad del Banco X.

Ello también pone en evidencia la existencia de una gran dificultad en cuanto a la elaboración de estadísticas sobre los delitos informáticos. La *cifra negra* es muy alta, existen grandes dificultades para descubrir estas conductas ilícitas y más aún para sancionarlas. Así, las víctimas optan por sufrir las consecuencias e intentar prevenir estas conductas en un futuro, conciliar con los delincuentes informáticos y no iniciar un procedimiento judicial.

En definitiva, podemos advertir que la doctrina mayoritaria define al delito informático como aquella conducta en la cual el medio comisivo es la utilización propia de un sistema informático. Sin embargo, pensamos que esta idea es demasiado genérica, pues el empleo en sí mismo de un sistema informático no es determinante para poder hablar de la existencia de un "delito informático", toda vez que se ampliaría el concepto de éste y se incurriría en el error de definir como delito informático a todas aquellas conductas en donde intervenga un sistema informático, como pudiera ser el caso del médico que prescribe una medicina mediante correos electrónicos a un paciente y le altera la receta, cometería, entonces, un homicidio "informático". O, por ejemplo, el daño que se genere por un delito de lesiones en donde el objeto fue una computadora, también constituirían un delito informático o un delito de estafa a una empresa virtual que se pudiera cometer mediante un sistema informático. Así, todos los delitos, en un futuro no muy lejano, constituirían un delito informático por el creciente uso de la red o sistemas informáticos.

En síntesis, la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos que aumenta de modo creciente, conlleva también a la posibilidad creciente de estos delitos, por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargados de las investigaciones y los funcionarios judiciales.

Por lo anteriormente, tenemos la siguiente aproximación entendiéndose como delitos informáticos todas aquellas conductas ilícitas susceptibles de ser sancionados por el Derecho Penal, que hacen uso indebido de cualquier medio informático.

Por tanto, en nuestra opinión, creemos que para poder dar una definición propia sobre las conductas que configuran el "delito informático" es prioritario y necesario identificar qué bienes jurídicos se protege y si estos bienes jurídicos deben ser objeto de protección penal. Pues, entendemos que la creación de un delito atendiendo a los principios de lesividad y proporcionalidad, sólo está justificada cuando exista un objeto jurídico digno de protección penal. Desde esta perspectiva, la determinación del objeto de protección nos brindará, precisamente, los índices necesarios de tipificación o no de un delito informático con autonomía.

En tal virtud, antes de asumir una posición acerca de si las conductas nocivas que se cometen a través de sistemas informáticos y de Internet anteriormente descritas configuran un delito informático, resulta necesario revisar previamente el objeto de protección al que se pretende otorgar protección penal.

3.1.1 La Función de Tutela de Bienes Jurídicos

Podemos señalar que el término "bien jurídico" se atribuye a Birnbaum, a mediados del siglo XIX. El origen de este concepto es propio de la dogmática del objeto de protección elegido por la ley. Posteriormente, Von Liszt afirmó que el origen del bien jurídico era en realidad un interés de la vida previo al Derecho, que surgía de las relaciones sociales; sin embargo, admitió que el interés vital no se convierte en bien jurídico hasta que es protegido por el Derecho. La discusión se centra entre aquellas posiciones que formalizan los fines del ordenamiento jurídico recurriendo a la Constitución, ya sea identificando bienes jurídicos con derechos fundamentales o bien con los fines del Estado y la sociedad trazados en el texto constitucional, y las posiciones que van más allá y pretenden identificar los bienes jurídicos en la realidad social.

Dentro de las concepciones que vinculan la teoría del bien jurídico con la realidad social misma, se ha de destacar la obra de Bustos Ramírez, cuya posición acerca de la teoría del delito toma, precisamente, al bien jurídico como piedra angular del sistema.

"Por el término "bienes jurídicos" se entiende aquellos presupuestos que la persona necesita para su autorrealización y el desarrollo de su personalidad en la vida social." Así, la autorrealización humana necesita de unos presupuestos existenciales que, en tanto son de utilidad para el hombre, se denominan "bienes" y mientras sean objeto de protección por el Derecho, serán "bienes jurídicos".

3.1.2. El contenido del bien jurídico protegido en los delitos informáticos

Como se ha podido apreciar en la primera parte del presente trabajo, las diferentes conductas nocivas que se cometen a través de sistemas informáticos y en Internet pueden ocasionar diversas lesiones a diferentes bienes jurídicos protegidos, tales como la intimidad, el patrimonio y nuevos objetos jurídicos de protección que adquieren autonomía e identidad propias en la red, los cuales serán tratados en los apartados siguientes.

Es innegable que el bien jurídico protegido es un punto de referencia obligado para la determinación del tipo penal del delito informático, pues determina el marco dentro del cual pueden realizarse las conductas delictivas. Ahora bien, luego de haber optado por la tesis que recoge la función del Derecho Penal como la exclusiva protección de bienes jurídicos, nos dedicaremos a determinar el bien jurídico protegido en los delitos informáticos.

Al igual que sucede respecto del concepto de delito informático, sobre el cual, como hemos visto, no existe un consenso unánime en cuanto a su significado, creemos que ocurre lo mismo en cuanto al contenido del bien jurídico protegido. Algunos autores sostienen que en los delitos informáticos el bien jurídico protegido es el patrimonio y la intimidad de la persona.

Sin embargo, creemos que si bien estos bienes jurídicos pueden verse afectados mediante el uso de sistemas informáticos, principalmente debido a la expansión de la tecnología, no constituyen bienes jurídicos propios de los delitos informáticos, ya que se trata de objetos de protección penal que están más allá del uso de los sistemas informáticos y que, en consecuencia, no se han originado producto de la tecnología.

3.1.3 La Intimidad como bien jurídico protegido

Se puede decir que la elaboración doctrinal que sirve de precedente a la constitucionalidad del derecho a la intimidad, fue concebida como *"the right to be let alone"*, es decir, el derecho a ser dejado en paz o a ser dejado solo. Para empezar a desarrollar la intimidad como bien jurídico protegido por el Derecho penal, nos vemos en la obligación de señalar las diferencias entre el significado del vocablo intimidad y privacidad. El vocablo intimidad se alude tanto al carácter oculto o secreto de aquellas circunstancias que rodean la existencia de un individuo, como a las circunstancias internas, esenciales del hombre y que éste mantiene como núcleo de su personalidad". Sin embargo, Davara Rrodrigez define la privacidad como el "término al que le podemos hacer referencia bajo la óptica de la pertenencia de los datos a una persona su titular y que en ellos se puedan analizar aspectos que individualmente no tienen mayor trascendencia, pero que al unirlos a otros pueden configurar un perfil determinado sobre una o varias características del individuo que éste tiene derecho a exigir que permanezcan en su esfera interna, en su ámbito de privacidad."

En efecto, la defensa de la intimidad y los demás derechos fundamentales no es privativa de los individuos, sino que debe proyectarse a las formaciones sociales en las que los seres humanos desarrollan plenamente su personalidad. Ello se aprecia, fundamentalmente, en cuanto a la participación de las personas jurídicas en el sistema económico, dentro del cual adquiere el rol de agente económico y es socialmente individualizada en la unidad empresarial. De ahí que, las personas jurídicas ostentan una identidad y significación social propias y distintas de las personas naturales que la integran y/o representan.

En el plano internacional, el derecho a la intimidad ha sido reconocido en el artículo 12 de la Declaración Universal de Derechos Humanos de las Naciones Unidas de 1948, en el artículo 8.1 de la Convención Europea para la protección de los Derechos Humanos y de las Libertades Fundamentales de 1950 y en el artículo 17.1 del Pacto Internacional de Derecho Civiles y Políticos de 1966.

Es ya conocida la violación constante a los derechos de la intimidad de individuos por información que se encuentra latente en Internet. Todo parece ser que el derecho a la intimidad relacionado con el aspecto informático juega un papel importante en la red. Así, aparece el término "intimidad informática", el cual podemos entender como la información personal que puede ser manejada en la red y/o almacenada en el disco duro de una computadora. Si bien es cierto que la definición de intimidad informática ha sido producto del desarrollo de la tecnología, podemos argumentar que se trata de la misma intimidad y del mismo concepto que se ha venido desarrollando años atrás, variando, únicamente, la forma de almacenamiento de los datos de carácter personal.

De otro lado, cabe indicar que la página web es considerada como medio de difusión general, por lo tanto Internet es un espacio difícil para preservar derechos fundamentales como la intimidad. En efecto, Internet es un territorio incómodo para preservar derechos fundamentales, como, por ejemplo, el derecho a la intimidad, el dominio reservado de cada uno que no se desea abrir al conocimiento de los demás. Al parecer con la denominada sociedad de la información ha sido cuando más se ha invadido la intimidad de las personas, hasta el punto que en la actualidad el individuo reclama la adopción de instrumentos jurídicos de respuesta a las sucesivas y frecuentes intromisiones que debe padecer en su intimidad. El gran riesgo de la privacidad frente a la informática es inimaginable. "El empleo de computadoras hace factible recopilar una amplia información sobre cada persona, reuniendo un conjunto de datos que aisladamente nada dicen, pero que al ser presentados en forma sistematizada, pueden dar lugar a una información que el afectado no se imagina ni le agradaría ver en poder de otros. Tengamos presente que un computador puede clasificar y relacionar rápidamente, por ejemplo, nuestros datos económicos, legales, laborales y de salud, construyendo un detallado perfil de cada individuo.

La facilidad para hacer acopio, tratar, transmitir y almacenar información pone en riesgo uno de los bienes más preciados del ser humano: su derecho a la intimidad, a no permitir que los demás conozcan de uno aquello que no deseamos que se conozca y, en último caso, si esto llega a ocurrir que podamos saber quién tiene nuestros datos, qué datos tiene, cómo los ha obtenido y para qué los quiere. De la misma manera deben considerarse las conductas que ponen a disposición de menores de edad imágenes de contenido altamente sexual explícito y que ponen en riesgo su formación integral ocasionando trastornos en el normal desenvolvimiento de su personalidad. Se debería controlar esta situación mediante el acceso a estas páginas web con doble clave. De otra parte, los contenidos nocivos en Internet están amparados bajo la libertad de expresión, sin embargo, no debe olvidarse la preservación del derecho de las personas, en cuanto a que alguna información nociva existente en Internet pueda afectar a algún individuo.

La gravedad de estos comportamientos, las peculiares exigencias que impone la supervisión de los contenidos disponibles por Internet y la paulatina extensión de este medio a sectores de la población necesitados de especial protección, como los menores, justifican la importancia del debate que se ve condicionado por la existencia de estándares diferentes según los países al concretar los límites de lo tolerable. Pero creemos que es necesario regular el uso que se puede dar a los datos que tan fácilmente se obtienen de cualquiera que se asoma a la red, aunque sólo sea para curiosear lo que hay en ella. Pareciera ser entonces que las cuestiones a decidir son las limitaciones al desarrollo de la libre comunicación en la red y cómo puede preservarse la intimidad y los datos personales frente a su utilización abusiva o no consentida; y para esto la libre comunicación en la red y la preservación de la intimidad y los datos personales tienen que ser normas universales.

Asimismo, el Habeas Data, no legislado, constituye una de las garantías constitucionales más modernas, a través de la cual todo individuo tiene derecho a accionar contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos. Para proteger la privacidad de las personas contra el abuso de la informática cuando se almacenan datos sin autorización o estando con el consentimiento del interesado se

tergiversan datos personales o íntimos, como ser la salud, la vida sexual, la economía personal, cuentas corrientes, solvencia económica y otros, surge una nueva institución, destinado a proteger la privacidad de las personas, situación en que se puede recurrir, para que la autoridad judicial ordene se cancelen o borren esos datos o se los corrija en su caso. En Bolivia aun no se encuentra legislado lo que algunos denominan " Datos Informáticos Privados".

Por último, del análisis expuesto, podemos concluir que los delitos contra la intimidad en donde los medios de ejecución sean sistemas informáticos, el bien jurídico protegido seguirá siendo la intimidad y, por lo tanto, no podemos hablar de delitos informáticos, ya que somos de la opinión que el derecho a la intimidad no es característica exclusiva de los sistemas informáticos, ya que sólo está en relación a ellos en cuanto al tipo de información almacenada, lo cual nos permite sostener que la intimidad constituye un valor a ser preservado en la red y sistemas informáticos, sin llegar a sostener que constituye el bien jurídico protegido en los delitos informáticos.

3.1.4 El Patrimonio como Bien Jurídico Protegido

Existen principalmente cuatro tesis planteadas en torno al concepto de "patrimonio". La concepción jurídica del patrimonio, la concepción económica estricta del patrimonio, la concepción patrimonial personal y, por último, la concepción mixta o jurídico-económica del patrimonio. No siendo nuestra intención explicar las referidas teorías, nos limitaremos a comentar brevemente la posición que actualmente asume la doctrina mayoritaria.

Desde esta concepción el patrimonio está constituido por la suma de los valores económicos puestos a disposición de una persona, bajo la protección del ordenamiento jurídico. Ahora, debido al desarrollo que ha tenido el comercio electrónico, el patrimonio se ha convertido en un derecho importante para todo individuo que ingresa a la red. "El traslado creciente de las decisiones a sistemas informáticos presenta sobre todo el problema penal de cuando y por qué la protección del patrimonio, la cual es clásicamente otorgada sólo contra las formas de ataque de engaño (astucia), amenaza y violencia, como también de abuso de confianza, es ampliada a la burla de los dispositivos de seguridad que ofrece o puede ofrecer el sistema informático."

El patrimonio se evidencia como uno de los principales objetos de protección en la red debido a la expansión del comercio electrónico como nueva forma de contratación, de allí que su protección adquiere enorme relevancia dentro de la criminalidad informática. En definitiva, si bien el patrimonio se erige como un valor a ser preservado y salvaguardado en la red, no constituye el bien jurídico protegido en los delitos informáticos, ya que no responde a la propia naturaleza de la red que está en función del acceso y transmisión de información.

Por tanto, concluimos que aquellas conductas que sean realizadas mediante sistemas informáticos o redes, en donde el bien jurídico afectado sea el patrimonio, no se les deberá dar la definición de delitos informáticos, ya que en un futuro caeríamos en el error de comprender a todos los delitos contra el patrimonio como delitos informáticos.

3.1.5 El Honor como Bien Jurídico Protegido

"Jurídicamente, el derecho al honor constituye el derecho que cada ser humano tiene al reconocimiento y respeto, ante él mismo y ante las demás personas, de su dignidad humana y de los méritos y cualidades que ha ido adquiriendo como fruto de su desarrollo personal y social".

El honor como objeto de protección penal ha sido concebido desde muy diversas perspectivas, sin embargo, para una concepción estrictamente jurídica, la dignidad de la persona, como sujeto de derecho, constituye la esencia misma del honor y determina su contenido. "Los servicios y aplicaciones de Internet pueden ser instrumentos para la realización de actividades que suponen intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

Al igual que otros bienes jurídicos tutelados por el Derecho Penal, el derecho al honor puede verse afectado; ya sea por algún envío masivo a un determinado grupo de personas de mensajes difamatorios, como publicaciones en páginas web con información que atente contra el honor de una determinada persona. "jurídicamente el honor y la intimidad representan diferentes

bienes de la persona, lo cual no significa que mediante una misma acción no puedan ser lesionados ambos, ya que el derecho a la intimidad se caracteriza por el derecho del individuo a preservar su vida privada de cualquier injerencia ajena, mientras que el derecho al honor se define por el derecho al respeto que merece toda persona en su dignidad humana".

Desde este orden de ideas, partimos por reconocer que tanto el honor como la intimidad pueden verse afectados, conjunta o indistintamente, a través del empleo de medios informáticos.

Sin duda, el debate se ha desarrollado debido a las numerosas reclamaciones interpuestas por usuarios contra proveedores de servicios de Internet, típicamente operadores de foros de discusión, por mensajes difamatorios publicados en esos foros. Entre la inicial jurisprudencia de EE.UU. dos decisiones se han convertido en referencia obligada. En el asunto *Cuvi vs Compuserver* no se consideró responsable por las afirmaciones difamatorias de terceros, a un proveedor de servicios en uno de cuyos foros de discusión habían aparecido esas afirmaciones, con base en que el proveedor de servicio actuaba como un mero distribuidor de información. Por su parte, en el asunto *Stratton Oakmont vs. Prodigy* el proveedor de servicios demandado fue considerado responsable por comentarios difamatorios de terceros aparecidos en un foro de discusión que ofrecía, con base en que decía ejercer un control efectivo sobre los contenidos públicos y había implantado ciertos mecanismos de control.

Ahora bien, el alcance del control que se ejerce varía significativamente según los instrumentos tecnológicos empleados. En concreto, la simple aplicación de programas de filtro que detectan el empleo de expresiones que pueden ser indicio de la existencia de contenidos ilícitos, no es un medio determinante del efectivo control de la presencia de contenidos difamatorios.

Por lo tanto, la mera contraposición entre la ausencia de todo control, de una parte, y el efectivo control de los contenidos en los términos tradicionales de la supervisión editorial de los medios de información tradicionales, de otra, es una simplificación que margina la realidad del alcance de las tecnologías de filtrado más difundidas.

Por último, es necesario advertir como ha sido explicado líneas arriba que sí debería ser considerado como medio de publicidad análogo la edición y publicación de una página web con información difamatoria, ya que no sólo resulta un medio idóneo para la realización de la conducta típica del delito de difamación, sino que, además, no se trata de una comunicación interpersonal, sino que está dirigida a la comunidad de la red y pueden acceder a ella todos los usuarios del sistema sin limitación alguna, resultando un medio de comunicación social masivo.

3.2. La libertad Informática

Según el diccionario, por el término "informática" se entiende el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

Hoy por hoy, debido al avance tecnológico y como respuesta a la necesidad de tutela de los derechos humanos, surge para ser frente a las necesidades de los individuos propias de la denominada "era tecnológica", la "Tercera Generación de Derechos".

Entre los derechos de la "Tercera Generación" destaca la libertad informática o autodeterminación informativa, en donde se pretende tutelar los derechos frente a la creciente utilización de la informática. la libertad informática, como bien jurídico objeto de consumo en las sociedades avanzadas, no puede concebirse sin el contrapunto de la salvaguarda o defensa de los datos personales que afecten la intimidad personal y familiar. Por tanto, por "libertad informática" se puede entender el derecho del individuo a controlar el uso de sus datos personales tratados o insertos en un programa informático.

La libertad informática ha sido denominada por la doctrina española como "un nuevo derecho fundamental que tiene por objeto garantizar la facultad de las personas para conocer y acceder a las informaciones que les conciernen archivadas en bancos de datos lo que se denomina habeas data por su función análoga en el ámbito de la libertad de información a cuanto supuso el tradicional habeas corpus en lo referente a la libertad personal, controlar su

calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados y disponer sobre su transmisión".

Ahora bien, creemos que el derecho a la autodeterminación informativa o libertad informática se encuentra estrechamente vinculado al concepto de intimidad, ya que se trata de ofrecer al individuo la seguridad de sus datos de carácter personal ante el posible uso mediante la informática u otro sistema automatizado; sin embargo, no es necesario que los datos utilizados sean íntimos o pertenezcan al núcleo esencial de la personalidad del individuo, sino, simplemente, que sean datos que puedan revelar sus hábitos y comportamientos. Así, el individuo tendría el derecho a decidir que información personal se podrá difundir y el destino sobre esta información dentro de la informática.

Después de un largo debate entre cada posición, la mayoría de autores estudiosos del tema, equiparan el término libertad informática con la autodeterminación informativa.

Por tanto, creemos que debido a la relación que existe entre la libertad informática y el derecho a la intimidad, ambos bienes jurídicos se encuentran vinculados en la medida en que el ejercicio de la capacidad de decidir sobre los datos protegidos por el derecho a la intimidad, constituye precisamente el ejercicio de la libertad informática cuando tales datos se encuentren almacenados en un sistema informático; por lo que no se debe considerar la libertad informática como un bien jurídico que requiere de protección penal en forma autónoma de la intimidad, ya que quien disponga de datos que se encuentren almacenados en sistemas informáticos y los utilice en perjuicio del titular, estará afectado el derecho a la intimidad o al honor, según sea el caso.

Por último, llegamos a la conclusión que la libertad informática si bien se erige como un valor a ser reconocido en la red, no podrá ser considerada como bien jurídico en los delitos informáticos, debido a que consiste en la facultad de decidir sobre los datos de carácter personal y, precisamente, el ejercicio de dicha libertad se verifica a través de los límites establecidos por el derecho a la intimidad y al honor, bienes jurídicos que cuentan con protección penal.

3.3 La Seguridad Informática

Según el Diccionario de la Real Academia de la Lengua Española, la seguridad se encuentra definida respecto a los temas tratados como el término que se aplica también a ciertos mecanismos que aseguran algún buen funcionamiento, precaviendo que éste falle, se frustre o se violente. La informática es "la ciencia que estudia y tiene como objeto el tratamiento automatizado o electrónico de la información".

Como se sabe, Internet es una red abierta donde la información es susceptible de ser inspeccionada, manipulada o intervenida por terceras personas. De hecho, el nacimiento de Internet se produce por la interconexión espontánea de redes y ordenadores a través de los cuales se formaliza la transmisión de información. Por lo tanto, la comunicación en Internet se produce de manera más sensible y menos segura, y la intrusión y alteración de cualquier comunicación es más frecuente.

Los riesgos más importantes derivados de un intercambio de información a través de redes abiertas son que el autor y fuente del mensaje hayan sido suplantados; que el mensaje se haya alterado, de forma accidental o de forma maliciosa, durante la transmisión; que el emisor del mensaje niegue haberlo transmitido o el destinatario niegue haberlo recibido; y que el contenido del mensaje sea leído por una persona no autorizada. A estas preocupaciones en materia de seguridad informática se corresponden los conceptos jurídicos de autenticación, integridad, no rechazo o no repudio y confidencialidad. Estos cuatro tipos de servicio de seguridad son ofrecidos por la técnica para conseguir una cierta certidumbre en los contenidos transmitidos por Internet. Así, la autenticación es el servicio que asegura la identidad del remitente del mensaje y que el mensaje procede de quien se dice que lo envía. La seguridad jurídica es un principio fundamental del derecho, y se expresa cuando el individuo como sujeto activo y pasivo de relaciones sociales, sabiendo y debiendo saber cuales son las normas jurídicas vigentes, tiene fundamentadas expectativas que ellas se cumplan. Este valor puede concebirse de dos maneras:

Seguridad jurídica propiamente tal, que es la seguridad del individuo frente a todo lo que atente contra sus derechos, que otros conciben como la certidumbre fundada y garantizada que la norma será cumplida. Certeza jurídica o certeza del derecho, que es la perceptibilidad cierta de la norma jurídica, la certidumbre de que se trata del contenido del Derecho vigente, situación que precave al ciudadano de las modificaciones arbitrarias de este derecho. Donde se requiere:

1. Que el Derecho sea positivo.
2. Que la norma preexista a la conducta regulada por ella.
3. Que la norma sea conocida, así como las consecuencias de su cumplimiento.
4. Que la norma sea inteligible, es decir carezca de ambigüedad que pueda dar lugar a equívocos.

Las condiciones o requisitos de la certeza hacen indispensable contar con herramientas e instrumentos que permitan al ciudadano acceder en forma oportuna y precisa a la información y alcanzar el conocimiento de las normas jurídicas del ordenamiento respectivo. La seguridad contra los delitos informáticos, hoy en día, muchos usuarios no confían en la seguridad del Internet. En 1996 IDC Research realizo una encuesta en Estados Unidos en donde el 90% de los usuarios expreso gran interés en la seguridad de Internet, pues temen que alguien pueda conseguir el número de su tarjeta de crédito mediante el uso de la Red.

Ellos temen que otros descubran su código de acceso de la cuenta del banco y entonces transferir fondos a la cuenta del hurtador. Las organizaciones, empresas se preocupan que sus competidores tengan conocimiento sobre información patentada que pueda dañarlos. Lo que se necesita es un plan de defensa, donde se requiere comunicar este plan a la gerencia y usuarios finales. Esto requiere educación y capacitación conjuntamente con la explicación, claramente detallada, de las consecuencias de las violaciones. Y es el primer paso para asegurar responsablemente la red. El desarrollo de una política de seguridad comprende la identificación de los activos organizativos, evaluación de amenazas potenciales, la evaluación del riesgo implementación de las herramientas y tecnologías disponibles para hacer frente a los riesgos, y el desarrollo de una política de uso. Debe crearse un procedimiento de auditoria que revise el uso de la red y servidores de forma periódica.

Identificación de los activos organizativos por ejemplo:

Hardware (ordenadores y equipos de telecomunicación)
Software (programas fuente, sistemas operativos, programas de comunicaciones)
Datos (copias de seguridad, registros de auditoria, base de datos).

Por otro lado definir los derechos y responsabilidades de los usuarios:

- Si los usuarios están restringidos y cuales son sus restricciones.
- Con que frecuencia deben cambiar sus contraseñas.
- Como deberían mantener sus contraseñas los usuarios.
- Si los usuarios pueden compartir cuentas o dejar que otros usuarios utilicen sus cuentas.

3.4 Presupuestos para la Tipificación de los Delitos.

Según Mezger, el "Delito es la acción típicamente antijurídica y culpable", de acuerdo a ella los elementos constitutivos del delito son la acción, tipicidad, antijuricidad y culpabilidad, para don Luis Jiménez de Asúa, el delito es "El acto típicamente antijurídico y culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una acción penal", de donde las características propias del delito son: actividad, adecuación típica, antijuricidad, imputabilidad, culpabilidad, penalidad y en ciertos casos, condición objetiva de punibilidad. El delito, es acto humano, es decir cualquier mal o daño que no tiene origen en la actividad humana, por graves que sean sus consecuencias no puede reputarse como delito si so se encuentran tipificados en nuestra legislación.

3.4.1. Acción.

La acción es el primer elemento de la definición del delito y, en el Derecho Penal se la define como la modificación del mundo externo por un movimiento corporal.

3.4.2. Tipicidad.

Según Jiménez de Asúa, que "el tipo legal es la abstracción concreta que ha trazado el legislador, descartando los detalles innecesarios para la definición del hecho que se cataloga en la ley como delito", vale decir, que el hecho que una conducta sea típica ya afirma un indicio de su antijuricidad, después de indicar la teoría de la tipicidad, podemos indicar que, la misma puede resumirse, de la siguiente manera.

3.4.3 Antijuricidad.

De la antijuricidad comenzaremos diciendo que es el elemento contrario al derecho. La antijuricidad tiene un concepto eminentemente antijurídico y se funda en la teoría de la norma y la ley, así tenemos que si se mata o se roba, se quebranta la norma y no la Ley. Binding dice: "La norma crea lo antijurídico, la ley crea la acción punible o, dicho de otra manera: La norma valoriza, la ley describe. Esto constituye la disposición penal que se compone del "precepto" en que se describe y define el acto o la omisión y la "sanción" en que se determina la pena con que el hecho esta conminado.

La conducta será antijurídica, cuando se opone al ordenamiento jurídico, debe lesionar o poner en peligro un interés jurídicamente protegido. No basta la contraposición de la conducta con la norma jurídica, sino también debe ser típica, es decir caer en un tipo o definición legal, en otras palabras debe corresponder a un tipo legal, que es la definición que da la ley de un delito.

3.4.4 Culpabilidad.

El acto debe ser culpable o sea que la conducta debe ser producto de la actividad, imputable a dolo o culpa. La acción es imputable cuando puede oponerse al cargo de una determinada persona, pero además de estos elementos se tiene la pena, es decir que la conducta típica, antijurídica y culpable debe estar sancionado con una pena. Son elementos esenciales que sin uno de ellos no hay delito, deben concurrir todos ninguno tiene preeminencia sobre los otros, estos elementos forman una unidad indivisible.

La culpabilidad, en el más amplio sentido, puede definirse como el nexo general de tipo intelectual y emocional que liga al sujeto con su acto. Es el conjunto de presupuestos que fundamenta la reprochabilidad personal de la conducta personal de la conducta antijurídica.

Si bien es preciso reconocer que la culpabilidad supone un contenido psicológico, éste no constituye de por si la culpabilidad. Es el objeto sobre el que recae el reproche sobre el autor. Es un juicio valorativo. En referencia a la culpabilidad de lo injusto esta se basa en que el concepto de la culpabilidad esta fundado en la culpabilidad del alto concreto injusto.

3.4.5 **Imputabilidad.**

El concepto de la imputabilidad puede dárselo indicando que imputar un hecho a una persona es atribuírselo para hacerle sufrir las consecuencias, es decir, para hacerle responsable de él, puesto que de tal hecho es culpable. La imputabilidad afirma la existencia de una relación de causalidad psíquica entre el delito y la persona, la responsabilidad resulta de la imputabilidad, puesto que es responsable el que tiene capacidad para sufrir las consecuencias del delito.

Por otro lado, el delito no se presenta al sujeto activo de improviso, de golpe, si no que obedece, a un proceso a un camino que recorre, al iter criminis. En efecto el delito recorre un camino cuyo punto de partida es un acto interno siguiendo otras fases hasta culminar en la ejecución. Este proceso constituido por varios actos que podemos dividirlo en dos fases: interna y externa. Generalmente el hombre delibera y después ejecuta. Muchas veces después de la deliberación se puede entrar en una fase intermedia, que Jiménez de Asúa llama intermedia y que son: la resolución manifiesta y el delito putativo.

La fase interna es subjetiva o psíquica, y la externa es objetiva o material. La fase interna solo existe mientras el delito queda encerrado en la mente del autor, no se manifiesta exteriormente. La externa ya se manifiesta, sale a la luz por actos incluso de preparación. La primera no es punible no se puede sancionar lo que queda como puro pensamiento.

En cuanto a la fase intermedia "la resolución manifestada y el delito putativo" En la primera no existe todavía la fase externa, no se tratan de actos materiales, más que de acción es de resolución como (proposición, conspiración, provocación). En el delito putativo hay una exteriorización del propósito de delinquir, pero el delito solo lo es en la mente del autor.

3.5 La Informática y el Derecho.

Podemos decir que la informática ha revolucionado la conducta humana y por ende las relaciones sociales, ha cambiado los patrones de producción, comunicación y otros, puesto que mediante este instrumento se logra un mayor rendimiento, utilidad y beneficio, siendo la información un medio del saber humano y de la comunicación, suscitadas por la aplicación de la información computarizada en todas las actividades de la sociedad actual.

Por tanto, el derecho, como producto de la organización social, surge la necesidad imprescindible de regulación del fenómeno informático en la actual sociedad moderna, lo que permite consecuentemente, una convivencia racional de normas sociales de conductas obligatorias surgidas de la realidad histórica, en la continua búsqueda de la justicia y el bien común.

3.5 **Delincuencia Informática y Delito Informático**

Es necesario hablar de delitos que atentan contra intereses jurídicamente protegidos, los cuales pueden presentarse de dos formas: delitos informáticos en si, (Aquellas acciones u omisiones que atenten en parte o en todo contra los Sistemas Informáticos, es decir, transmisión ilícita de datos e informaciones) – y delitos por si, conductas delictivas que emplean a los sistemas informáticos como medio comisivo, fraudes, falsificaciones, etc.

Vale decir que los actos delictivos cometido mediante manipulación dolosa en las computadoras abarcan una amplia gama de conductas, que van desde la violación de esos derechos, pasando por nuevas modalidades de sabotaje, transferencia ilícita de fondos y cuentas bancarias, invasión (atropello) de la privacidad.

Este fenómeno, en cuanto a su estudio, plantea una alta cifra negra de criminalidad, en vista de que las empresas y/o instituciones afectados, sobre todo los bancos, no presentan denuncias correspondientes, por temor a dañar su imagen. Aspecto este que ha tenido la oportunidad de corroborar con varias instituciones bancarias por ejemplo al recopilar datos.

3.7 Necesidad de Incorporar Nuevos Tipos Penales.

La informática es un fenómeno multifacético de realidad contemporánea, como consecuencia inmediata de estos avances, a través del tiempo el delito fue mutando, alternando su estructura, modificando y adquiriendo distintos perfiles, es cierto que el crimen existe desde que existe el hombre. Sin embargo, el progreso tecnológico hace más dificultoso su control y penalización, esa dificultad radica, en las sofisticadas formas que adquiere el delito con ayuda de la tecnología. En este sentido, los sistemas informáticos logran potencializar las posibilidades de las distintas modalidades delictivas denominadas tradicionales. Las inimaginables posibilidades que estos sistemas aportan al desenvolvimiento del hombre en todas sus esferas de actuación exteriorizan su faceta indeseable en el nacimiento de nuevas modalidades delictivas que radica su particularidad en su vinculación con los sistemas informáticos y en la potencialidad dañosa que esta herramienta posee en su uso ilícito. Podemos decir entonces que con el desarrollo de la informática, hace aparición un nuevo tipo de delincuencia, sofisticada, suficientemente capaz en si misma, de aparejar nuevos problemas al Derecho Penal y a la Administración de Justicia.

Frente a esta problemática, es evidente que como punto inicial se presenta, el comprender que es necesario generar nuevos marcos legales intentando conjugar la experiencia extranjera con la situación local, no hay que perder de vista que en un mundo globalizado no es posible tomar decisiones aisladas o unilaterales. Dichos marcos legales, donde se tipifique las nuevas figuras que nacen a través del avance tecnológico y delimiten el manejo usual de los sistemas informáticos, lo que tiene una directa relación con la naturaleza humana.

Durante la investigación, se ha puesto en evidencia la vulnerabilidad de los sistemas de procesamiento automático de datos e información, como cualidad que la hace susceptible de ser alterada, destruida o dañado para el logro de beneficios ilícitos, si bien es cierto que estas conductas pueden encuadrarse en determinados tipos paneles, no es menos cierto que el Derecho Penal, como ordenamiento jurídico destinado a resguardar, cuidar y preservar bienes y valores de la sociedad en su conjunto, cumpla este papel, sancionando conductas antisociales de acuerdo al actual sistema jurídico – penal o creando nuevas figuras delictivas, o bien agravando la penalidad de las conductas comisivas u omisivas ya sancionados.

Dado la importancia y el actual crecimiento de la aplicación de sistemas informáticos, por ello, las personas naturales o jurídicas, públicas o privadas, deben ser consientes de la responsabilidad de establecer un adecuado sistema de control informático que proteja ordenadamente a su empresa u organización, prevención y paralelamente, es necesario un refuerzo legislativo que contemple las diferentes infracciones informáticas.

La legislación vigente todavía presenta grandes vacíos en cuanto a su normatividad sobre informática en general y la delincuencia emergente de ella. En tal sentido, el Prof. Carlos Maria Correa que dice: "La difusión de la informática da origen a nuevas formas delictivas que utilizan los sistemas informáticos como medio comisivo, o bien que tiene a aquellos en parte o en todo como su objeto". Si bien la incipiente difusión de la informática no ha dado dimensión mayor a este problema, es previsible que su importancia crecerá a medida que aquello progrese, en particular en sentido financiero.

Ante esta realidad, el Estado Boliviano tiene la obligación con la sociedad civil de proteger el trabajo y las actividades lícitas que emplean y desarrollan sistemas informáticos, de posibles actos que atenten contra esos sistemas incorporando a la legislación penal previsiones legales protectivas.

Por su parte las Naciones Unidas ha reconocido una tipología de delitos informáticos, con más detalle y distinta distribución, agrupándolos en tres grandes grupos:

Fraudes cometidos mediante manipulación de computadoras.

a) Manipulación de los datos de entrada: *Conocido como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática.*
b) La manipulación de programas: *es muy difícil de descubrir y a menudo pasa inadvertido debido a que el delincuente debe tener conocimiento técnicos concretos de informática.*
c) Manipulación de los datos de salida: *se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude, es a los cajeros automáticos mediante la falsificación de instrumentos para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robados, sin embargo en la actualidad se usan ampliamente equipos y programas de computadora especializados para descodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.*
d) Fraude efectuado por manipulación informática: *aprovecha las repeticiones automáticas de los procesos de computo. Es una técnica especializada que se denomina técnica de salchichón en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando rápidamente de una cuenta y se transfieren a otra.*

Falsificaciones informáticas.

a) Como objeto: *cuando se alteran datos de los documentos almacenados en forma computarizada.*
b) Como instrumentos: *Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercia. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificadores, y los documentos que producen son de tal calidad que solo un experto puede diferenciarlos de los documentos auténticos.*

Daños o modificaciones de programas o datos computarizados.

a) 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 con:*

I. 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 infectado, así como utilizando en método del Caballo de Troya.*

II Gusanos*: se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamientos de datos o para modificar o destruir los datos, pero es diferente del virus por que no puede regenerarse. Las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus. Por ejemplo, un programa gusano que eventualmente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.*

III Bomba lógica o cronológica: *exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. 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. Puede utilizarse este método como instrumento de extorsión y se puede pedir un rescate a cambio de hacer conocer el lugar en donde se halla la bomba.*

b) Acceso no autorizado a servicios y sistemas informáticos: *se produce por diversos motivos, desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.*

I Piratas informáticos o hackers*: el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso. El*

delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso.

Por otra parte existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligado directamente a acciones efectuadas contra los propios sistemas como son:

- ∝ Interceptación de correo electrónico: lectura de una mensaje electrónico ajena.
- ∝ Estafas electrónicas: a través de compras realizadas haciendo uso de la red.

También a través de la red Internet permite dar soporte para la comisión de otro tipo de delitos.

I. Espionaje Informático: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

II. Terrorismo Informático: mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

III. Narcotráfico: transmisión de formulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas recogidas.

IV. Otros delitos: las mismas ventajas que encuentran en el Internet los narcotraficantes pueden ser aprovechados para la planificación de otros delitos, como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas.

Para la Organización de las Naciones Unidas, estas son las conductas más frecuentes que se cometen a través de sistemas informáticos.

1. Fraudes: Cometidos mediante manipulación de computadoras, por ejemplo, sustraendo o colocando datos falsos en un sistema y manipulación de programas, representa el delito informático más común. [7]

[7] En http://cnnenespanol.com/2001/tec/02/27/museo/index.html Fecha de acceso: 05 de enero del año 2002.

2. Falsificación: Por medio de la Informática, de dinero, ticket, así como cuando se alteran datos de los documentos almacenados en forma computarizada.
3. Daños a Datos: Por medio de virus, accesos no autorizados por *hacker* o *cracke*r, esto es por diversos motivos desde la simple curiosidad, como en el caso de muchos piratas informáticos hasta el sabotaje o espionaje informático.
4. 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.
5. Fraude Informático: es la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador, con ánimo de lucro y en perjuicio de tercero.

Cabe resaltar que el objetivo de la presente numeración es presentar todos aquellos elementos que han sido considerados tanto por organismos gubernamentales como por diferentes Estados, para enfrentar la problemática de los delitos informáticos a fin de incorporar a la vida jurídica la regulación de dichas conductas.

La asociación Internacional de Derecho Penal, durante un coloquio celebrado en Wursburgo, Alemania, en 1992, adopto diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplan que en la medida en que el Derecho Penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes a la creación de otros nuevos. Además las nuevas disposiciones deberán ser precisas y claras.

Es en este sentido que nuestra preocupación de todos los elementos anteriormente descritos tenemos el **SABOTAJE INFORMÁTICO**, al respecto es importante destacar que entre los servicios que brinda Internet, el más utilizado por las empresas paceñas es el correo electrónico o (e-mail) siendo que de 1.066 empresas comerciales inscritas en la Cámara de comercio de la ciudad de La Paz, 700 registraron dirección electrónica.

Así, este es el servicio más popular y el medio más eficaz para la comisión del sabotaje informático empresarial, pues es mediante el conocimiento de la dirección electrónica de la

empresa, que cualquier sujeto puede enviar a la misma inofensivos mensajes que contengan peligrosos programas informáticos con la intención de borrar, suprimir o modificar sin autorización funciones o datos de computadora para obstaculizar el funcionamiento normal del sistema, a través de virus informáticos, bombas lógicas y otros.

3.8 **Código Penal Vigente.**

Art. 363.- bis "(Manipulación Informática) El que con la intención de obtener un beneficio indebido para sí o un tercer, 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 delito es básicamente de resultado por su naturaleza y por decisión de la ley porque si no hay resultado no hay una transferencia patrimonial ilícita, no hay consumación pero puede darse la tentativa, es decir realizar la manipulación pero no lograr el fin propuesto. Es delito doloso que excluye toda posibilidad de que pueda ser una delito de carácter culposo. Su antijuricidad radica en que intencionalmente se manipulen datos informáticos ya sea para lograr resultados incorrectos o evitar un procesamiento correcto a fin de lograr de modo ilícito una transferencia patrimonial en perjuicio de un tercero que sufre un detrimento una disminución en su patrimonio. Esta transferencia de activos sin que el titular de ellos lo conozca, la condición objetiva de punibilidad se constituye cuando hay una ilícita transferencia patrimonial basándose en manipulaciones de informática en perjuicio de tercero. De lo anteriormente se establece las siguientes puntualizaciones:

- Sujeto Activo, de manipulación informática es determinado.
- Sujeto pasivo, es indeterminado.
- El bien jurídico protegido , son los bienes incorporales ejemplo los datos informáticos, software.
- Objeto material, son básicamente los bienes informáticos ejemplo un ordenador, modem.

- El objeto del delito puede ser el procesamiento o transferencia de datos informáticos.
- Como elemento psicológico, está en la voluntad de manipular un procesamiento o transferencia de datos informáticos.
- En cuanto a la tipicidad es doloso.
- Es de resultado, cuando se consuma a través de la manipulación de datos informáticos en beneficio propio o de un tercero.

Art. 363.- ter "(Alteración, acceso y uso indebido de datos informáticos) 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 la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días".

La antijuricidad radica en apoderarse, penetrar, utilizar, modificar o inutilizar datos almacenados en un sistema informático que corresponde a otra persona. Desde el momento en que se almacenan esos datos que pueden ser personales, de la vida privada o situación económica, comercial, empresarial, etc. Es de resultado debido a que el apoderamiento, acceso deben causar perjuicio de carácter económico. La sanción de estas conductas van dirigidas a proteger a las personas contra terceros en uso indebido e ilícito de datos que son reservados. Si bien causan daño no, son a través de manipulaciones que son inmateriales. Los delitos informáticos establecidos en el capítulo XI artículos 363 bis y 363 ter del Código Penal resultan ser conductas típicas y antijurídicas distintas al fraude informático, sabotaje informático, etc., tanto en los elementos estructurales que lo componen como en el modus operandi de la conducta, debiendo destacarse que estas nuevas formas de delinquir es atípica en la legislación penal vigente.

3. 9. Formas de comisión de los delitos

Como se ha venido mencionando según Mezger, delito es "La acción típicamente antijurídica y culpable". Los delitos pueden ser dolosos o culposos. El delito es doloso cuando el agente

quiere o acepta el resultado, o cuando este es consecuencia necesaria de la conducta realizada. En la culpa se debe distinguir entre.

- La culpa consciente, cuando se tiene conciencia que al realizar una conducta se puede incidir en un tipo penal.
- La culpa inconsciente, cuando no se tiene conciencia de las consecuencias y no toman las precauciones pero se tiene como posible la realización del tipo penal.

De acuerdo al presente punto se determina que hay culpa cuando el sujeto no toma conocimiento y considera posible su realización pero tiene la esperanza de que no se dará el resultado típico. El sujeto pudo evitarlo, pero se comporto como lo hizo.

3.10 Estudio de las bases jurídico penales

Las bases jurídico penales como conjunto de condiciones determinantes en el ámbito del Derecho Penal, configuran los elementos constitutivos del delito, así como las acciones a ser consideradas delictivas, fijando la apreciación del bien jurídico que ha de ser protegido penalmente sobre esos principios, variables en tiempo y espacio, establecer la sancionabilidad del mismo. El Derecho Penal en la prevención de la licitud de la conducta delictiva, para que este evite incurrir en ella en protección de la defensa social y de la convivencia humana.

El Derecho Penal como señala, el Dr. Benjamín Miguel Harb, es normativo, en el sentido de la división ontológica que hace en las ciencias de ser y las del deber ser. Estas últimas tratan de reglamentar o normar la conducta para que se adecue a los fines perseguidos por el Estado de Derecho. Por ello es que solo en la norma se halla la definición de la conducta correcta y en su caso legal. Es también valorativo en el sentido que la conducta para nuestra ciencia tiene una significación que cae en un valor o en un antivalor, en lo jurídico o antijurídico. En tal sentido cuando apreciamos una conducta para calificarla de delictiva o no, estamos haciendo un juicio de valor que se refiere a lo valorativo que en última instancia califica la conducta y su resultado. La normativa correctamente determinada hace imposible la amenaza de los actos arbitrarios de la autoridad que usa el poder punitivo del Estado. El análisis jurídico de la

descripción del delito como hecho antijurídico punible, presenta la combinación de un elemento objetivo (ofensa o daño) con otro espiritual. Téngase en cuenta que la prevención de la norma legal genera la obligación de un comportamiento que evita que su actuación se realice.

En estricto sujeción al principio de legalidad y las restricciones que se manifiestan en lo referente a la exclusión de la analogía, nos hacen comprender que la única fuente del derecho penal es la ley en sentido formal, esto es la ejercida por el Poder Legislativo. En este sentido estos principios expresados a través de la formula plasmada por el jurisconsulto Aleman Feuerbach Lehrbuch "Nullum crimen, nulla poena, sine lege", lo que equivale a expresar que nadie puede ser castigado si no hay delito ni pena sin una ley previa que haya definido el delito que motiva la condena y fijado la pena correspondiente.

La presente regla conocida también como el principio de legalidad de los delitos y las penas, es la consecuencia necesaria de garantía en la prohibición de la aplicación analógica de la ley penal.

Como lógica consecuencia del principio de legalidad, todo delito debe ser juzgado de acuerdo con la ley vigente en el momento de la comisión del hecho, de ahí que no pueda admitirse de ninguna forma la aplicación de una ley penal más severa a hechos cometidos con anterioridad a su sanción (principio de la irretroactividad absoluta de la ley penal más severa). De estos principios se desprenden las formulas y garantías penales, que supone la existencia del delito sin que expresamente y con carácter previo lo establezca (Nulla Crimen sine Pravia lege), no puede aplicarse pena alguna que no este conminada por la ley anterior como garantía penal (Nulla poena sine pravia lege), la ley penal solo puede aplicarse por los órganos y jueces constituidos para esa función (nemo iudez sine lege), por otro lado tenemos que donde no hay ley no hay delito (Ubi non estlex, nec praevaricatio).

Así mismo nadie puede ser castigado sino en virtud de juicio legal expresado como garantía constitucional. Estos principios consagrados en la Ley Fundamental de la República y el Código Penal Boliviano reafirman las bases jurídicas, enmarcadas en el Derecho Penal.

tomando en cuenta el carácter irrefragable, ineludible de la ley y de la obligatoriedad de la misma. También debemos resaltar que en el ámbito del Derecho Penal no es admitido la analogía, no lo admite pues la tipificación rigurosa de los delitos es una garantía contra la arbitrariedad a la que podría llevar la analogía en la aplicación de las penal

Es de esta manera, que el derecho como garantía de las condiciones de vida de la sociedad, asegurado por el poder que ejerce el Estado (Jus Puniendi), se halla hoy en un momento histórico en la que debe responder a los nuevos avances y complejos problemas que plantea sociedad en permanente transformación resultante del avance tecnológico y científico de la sociedad moderna.

3.11 La victima en los delitos informáticos

Esta nueva realidad que plantea formas sofisticadas de comisión delictiva, no solo crea nuevos delitos y nuevos delincuentes sino un grupo humano más vulnerable a sus ataques y arremetidas, precisamente el de sus victimas, que pueden ser personas jurídicas o naturales. Otra consideración sobre las victimas del delito informático lleva a conclusiones referidas a que "la mayor parte de las victimas de estos delitos con las empresas así como personas naturales afectados por el uso del sistema de computación.

Para la victima del Delito Informatico suele ser más perjudicial por su imagen y prestigio ante el público, denunciar la comisión de este tipo de delitos que asumir las perdidas que se los ocasiona. Otorga mayores posibilidades de impunidad al delincuente y de seguridad en sus hechos.

La mayoría de las victimas de este tipo de conductas no las denuncian por el desprestigio que esto pudiera ocasionar y las consecuentes perdidas económicas, así como por la atipicidad de esta conducta en la legislación penal vigente.

Es necesario resaltar que el tipo penal al ser un instrumento legal, necesario y de naturaleza predominantemente descriptiva tiene por función la individualización de conductas humanas

penalmente relevantes, siendo imposible sancionar como delitos, hechos no descritos en el ordenamiento jurídico penalmente vigente.

Por tanto la atipicidad del fraude informatico, sabotaje informático por decir algunos en la legislación vigente, imposibilita una calificación jurídica penal que individualice a la misma llegando a existir una alta cifra negra de criminalidad e impunidad sobre el particular.

3.12 Características y Clasificación de los Delitos Informáticos

Para la comisión de dicha conducta antisocial, encontraremos a uno o varios sujetos activos como también pasivos, los cuales tienen características propias. El Sujeto Activo, posee ciertas características que no presentan el denominador común de los delincuentes, por que los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentra en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando en muchos de los casos no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Son sujetos dedicados y motivados dispuestos a aceptar un reto tecnológico.

El Sujeto Pasivo o victima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, las victimas pueden ser individuos, instituciones crediticias, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito es sumamente importante, ya que mediante el podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionados debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos. Dado lo anterior " ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades, y si a esto se suma la falta de leyes que protejan a las victimas de estos delitos; la falta de preparación por parte de las autoridades para comprender para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática.

Cabe resaltar el especial modus operandi de esta clase de conductas, es lo que las hace particularmente difíciles de pesquisar. Es por esta consideraciones que para su esclarecimiento no bastan los métodos clásicos de criminalística sino se requiere el manejo de conocimientos en el área informática, en la policía técnica, en especial por el modus operandi de esta clase de conductas, es lo que las hace particularmente difíciles de pesquisar. Es por estas consideraciones que para su esclarecimiento, no bastan los métodos clásicos de criminalística sino que se requiere el manejo de conocimientos en el área informática, y la colaboración de unidades especializadas en el tema. Es así que en Estado Unidos, el "FBI crea un centro de lucha contra el fraude en Internet", el organismo atenderá quejas de los consumidores sobre el comercio electrónico y la compraventa de valores. Por otro lado un informe del banco de Francia, "El riesgo de fraude en pagos por Internet es potencialmente elevado" textualmente señala que el riesgo de fraude en los pago por Internet es "potencialmente elevado" y los métodos utilizados para las transacciones, según un estudio del Banco de Francia. En España, sevilla"Descubren un fraude de 1.500 millones en tarjetas de movil", la guardia civil, en el transcurso de la operación denominada Pack-Movil, ha puesto al descubierto un fraude en mas de 1.500 millones de peseta relacionado con el uso ilegal de tarjetas de telefonía movil.

Por otro lado el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes perdidas, entre otras, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada"cifra oculta o cifra negra".

En forma general, las principales características son:

a) Conductas conocidas como de cuello blanco
b) Son conductas ocupacionales, muchas veces se realizan cuando el sujeto se halla trabajando.
c) Provocan serias perdidas económicas.
d) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

e) Son muchos los casos y pocas las denuncias.
f) Son muy sofisticados y relativamente frecuentes en el ámbito militar.
g) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
h) Ofrecen facilidades para su comisión a los menores de edad.
i) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

Por lo anterior, para cometer estas conductas, deben ser personas con conocimiento sobre la informática los cuales se encuentran en lugares estratégicos o con facilidad para poder acceder a información de carácter delicado, como puede ser instituciones crediticias o del gobierno, empresas o personas naturales, dañando en la mayoría de los casos el patrimonio de la victima, la cual por la falta de una ley aplicable al caso concreto no es denunciado quedando impune estos tipos de conductas antisociales, por lo que se pretende en el presente trabajo, es crear una conciencia sobre la necesidad urgente de regular estas conductas.

En cuanto a su clasificación, a este tipo de acciones es de dos formas:

1.- Como instrumento o medio, son conductas que se valen de las computadoras como método, medio en la comisión del ilícito, por ejemplo, la falsificación de documentos vía computadoras (tarjetas de créditos, etc.),. La variación de los activos y pasivos en la situación contable de las empresas, sustracción o copiado de información confidencial, la alteración en el funcionamiento de los sistemas (virus informáticos) y el acceso a áreas informatizadas en forma no autorizados, etc.

2.- Como fin y Objeto, en esta categoría las conductas van dirigidas en contra de la computadora, accesorios o programas como entidad física, los cuales pueden ser la programación de instrucciones que producen el bloqueo total al sistema, la destrucción de programas por cualquier método, el daño a la memoria, o el atentado físico contra la máquina o sus accesorios como (discos, cintas, terminales, etc.).

3.13 Principales manifestaciones de Delincuentes Informáticos

3.13.1 Piratas o *Hackers*

El termino hacker deriva etimológicamente de la palabra Inglesa Hack que significa corte, tajo, puntapié. Dicho termino se utilizaba para describir, la peculiar forma en que personas con conocimientos técnicos arreglaban cajas defectuosas mediante un golpe sobre las mismas. Actualmente, el termino hacker es utilizado para referirse a los sujetos que incurren en conductas disvaliosas mediante el computador, los cuales se ganaron esa aceptación criminal por la peligrosidad que conlleva su actuar en la sociedad moderna.

Son quienes interceptan dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas. El termino de hacker en castellano significa "cortador". Las incursiones de los piratas son muy diferentes y responden a motivaciones dispares, desde el lucro económico a la simple diversión. Los "hackers", son fanáticos de la informática, generalmente jóvenes, que tan solo con un ordenador personal, un modem, gran paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, saltándose odas las medidas de seguridad, y leer información, modificarlo, preparando las condiciones idóneas para realizar el fraude o bien destruirla. Se puede considerar que hay dos tipos;

1) Los que solo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos o satisfacer su propia vanidad.

2) Los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables.

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso, 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. Normalmente, 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.

3.13.2 *Crackers*

Etimológicamente, el termino Cracker deriva de la palabra Inglesa Crash que significa estallar o desplazar. Sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender, es decir, presenta dos vertientes:

1) El que ingresa a un sistema informático y roba información o produce destrozos en el mismo.
2) Y el que se dedica a desproteger todo tipo de programas completos comerciales que presentan protecciones anticopia.

3.14.3 *Phreackers*

Son sujetos especializados básicamente en el manejo de sistemas informáticos, realizan toda clase de conductas, mediante el computador, previamente burlando los sistemas de seguridad de telefonía para no pagar el usos de Internet o pagar menos por el servicio. Al ser conocedores de la informática, se infiltran fácilmente en los sistemas informáticos de las empresas y/o particulares. *Ejemplo de un preacker:*

1ª Un ordenador, un modem, un programa de búsquedas numéricas, una conexión telefónica;
2ª Actúa, cuando el programa comienza a llamar a todos los números, a través del modem hasta que alguien contesta, si una persona contesta, el programa desestima el número y continua buscando, el programa sigue escaneando los números hasta que encuentre el número siguiente, si un modem comprueba que el ordenador esté conectado a Internet, guarda este número para usarlo después.

3ª La próxima vez que el preacker quiera conectarse a Internet gratis, llamará a este número y se conectará a través de su modem. El coste de la llamada correrá a cargo del dueño del número.

Como hemos visto de los tipos de delincuentes informáticos, todos ellos necesitan del acceso a un sistema informático para poder realizar conductas ilícitas.

Por ello, nuestra posición en cuanto al bien jurídico en los delitos informáticos, ya que desde el momento en que se proteja claramente la informática, se podrá sancionar a esta categoría de delincuentes cibernéticos y/o informáticos previniendo de manera antelada la afectación de otros bienes jurídicos individuales como por ejemplo, la intimidad, el patrimonio, el honor, etc.

3.15 Tipología del "Delincuente Informático"

Como hemos visto al ocuparnos de las conductas lesivas en la red, los comportamientos pueden ser agrupados y clasificados por la doctrina, sucede lo mismo respecto de aquellos sujetos que los realizan, la doctrina viene discutiendo acerca de una posible tipología del delincuente informático.

Por ello, las conductas ilícitas cometidas a través de las funciones de las computadoras son originadas por autores que devienen en ser llamados delincuentes informáticos. A este tipo de delincuentes también se le conoce como "ladrones de guante virtual", en aras a distinguir la necesidad de conocimientos técnicos especiales por parte del agente.

Entendemos el concepto de delincuente informático como aquel individuo que realiza ataques a la seguridad informática; sin embargo, la tendencia de la doctrina es denominar delincuentes informáticos a aquellos sujetos que llevan a cabo conductas lesivas a la intimidad, patrimonio u honor a través del empleo de medios informáticos. Ello con la finalidad de poder destacar las características propias de las personas que llevan a cabo estas modalidades delictivas en relación con aquellos sujetos que cometen estos delitos desde otros medios.

Años atrás el sujeto activo de estos delitos era considerado como la persona que oscilaba entre los 15 y 30 años, de clase media, con una inteligencia dentro del promedio, que ingresaba a sistemas informáticos más que con un ánimo de lucro o de dañar un sistema informático, con un afán de reto, de curiosidad y de superioridad por ingresar a sistemas que le eran ajenos.

Años más tarde se señalaba que el avance tecnológico desarrollaba cada vez más sofisticados sistemas de seguridad, que los sujetos activos ya no eran personas con un simple sentido de curiosidad, sino que, por el contrario, eran personas que poseían altos conocimientos en informática, con un nivel de inteligencia superior. Así, la doctrina argumentaba que los sujetos activos eran un 90% de los individuos que laboraban dentro de la empresa perjudicada. Hoy en día la doctrina establece que los autores de conductas nocivas en sistemas informáticos no son ya personas que laboran en empresas, como anteriormente se señalaba, ya que uno puede desde su casa ingresar a cualquier sistema.

Con respecto a este tema, somos de la opinión que debido al desarrollo tecnológico que cada día se acrecienta más. Somos de la idea que mientras mayor seguridad en el ingreso a sistemas informáticos, mayor será el conocimiento especial que requerirá el delincuente informático. asimismo, a mayor expansión de Internet –a mayor crecimiento de la ciberpoblación en la red mayor será la intervención del hombre medio. Por lo tanto, conductas que originen mayor impacto, estarán en relación a aquellas conductas que tengan mayor protección.

Otro problema que se adiciona es que la mayoría de los autores son jóvenes, recordemos que fueron adolescentes de 16 y 17 años los que ingresaron en 1985 a los sistemas informáticos del Pentágono de los Estados Unidos, modificando y alterando información sobre la construcción de material de defensa y ubicación de satélites artificiales en el espacio. O el célebre caso Morris, en donde un joven interfirió los sistemas informáticos del Ministerio de Defensa, infectando con un virus más de seis mil computadoras oficiales que contenían valiosa información clasificada.

En relación con las características personales de aquellos que cometen delitos de Alta Tecnología, debe tenerse presente generalmente lo siguiente:

- En general son personas que no poseen antecedentes delictivos.
- La mayoría de sexo masculino.
- Actúan en forma individual.
- Poseen una inteligencia brillante y alta capacidad lógica, ávidas de vencer obstáculos.
- Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en si mismo.
- También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se trata de delincuentes profesionales típicos y por esos son socialmente aceptados.
- En el caso de los "hackers", realizan sus actividades con una especie de deporte de aventura donde el desafió esta allí y hay que vencerlo. Aprovecha la falta de rigor de las medidas de seguridad para tener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad. Esto suele suceder con frecuencia en los sistemas en que los usuarios emplean contraseñas comunes o de mantenimiento que esta en el propio sitio.
- Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadores.

Capítulo IV

LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN COMPARADA

Como ha sido explicado anteriormente, el desarrollo de la tecnología ha producido y sigue produciendo problemas por malos usos de sistemas informáticos y de la red. Por ello, el tratamiento que el derecho penal le otorga al ámbito internacional varía mucho según cada legislación. Se puede decir, que aún no se ha llevado a cabo un consenso internacional a favor de la tipificación de los delitos informáticos.

A continuación, explicaremos como los países de España, Estados Unidos de Norteamérica y Chile han dado un tratamiento para estas clases de conductas ilícitas que se producen en la red y en los sistemas informáticos.

4.1 El sistema Penal Español

El 26 de octubre de 1995 se aprobó, por el pleno del Senado, la nueva Ley Orgánica 10/1995 del nuevo Código Penal Español el mismo que entro en vigor el 24 de mayo de 1996. Así, el Código penal español se ha visto obligado a intentar solucionar el problema de conductas delictuosas que surge a raíz del incremento de las nuevas tecnologías. Así, se introdujo nuevos figuras jurídicas y se modificó algunos de los existentes con el fin de adaptar la norma positiva al uso delictivo de los ordenadores, sistemas lógicos y tecnologías de la información.

El tipo de "estafa informática" esta en el artículo 248.2, cuando "con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero." El numeral dos fue introducido recién en el texto penal de 1995, debido a las crecientes estafas mediante sistemas informáticos. Dicho texto se debió a que la doctrina española rechazaba la aplicación del tipo tradicional de estafa a los casos de transferencias informáticas de fondos, consistentes en introducir datos u órdenes falsas o efectuar alteraciones en los programas que gestionan

automáticamente transferencias bancarias, ingresos o reconocimiento de créditos a favor de quien realiza la manipulación. Por el principio de legalidad sin incurrir en formas de analogía en contra del reo, el Derecho penal español encontró la solución al incorporar un tipo específico de estafa que acogiera la peculiaridad de que la transferencia del activo patrimonial se realizara mediante "alguna manipulación informática o artificio semejante", ya sea por modificaciones de programas o alteraciones en el procesamiento.

El artículo 256 señala lo siguiente; "El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses."

El artículo 278, por su parte, comprende el delito de espionaje informático. Conducta que está constituida por la obtención sin autorización de datos almacenados en un fichero informatizado, que se caracterizan por su confidencialidad, exclusividad y valor económico.

1.- " El que, para descubrir un secreto de empresa se apoderase por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mecanismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2.- Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3.- Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos".

4.2 El Sistema Penal Norte Americano

Igual que en todos los países del mundo, Estados Unidos se ve envuelto en actividades delictuales mediante sistemas informáticos y dentro de la Red.

Con respecto a la legislación sobre delitos informáticos en los Estados Unidos de Norteamérica, existen dos Estatutos importantes sobre Leyes Federales de Delitos Informáticos; el 18 USC, Capítulo 47, Sección 1029, y Sección 1030, conocida como el Pronunciamiento sobre el Abuso y el Fraude Informático de 1986.

Estas no son las únicas leyes sobre el delito informático en los Estados Unidos, lo que sucede es que estas son las dos leyes más importantes usadas en los Juzgados Federales de los Estados Unidos para poner a los delincuentes informáticos en prisión.

El Departamento Nacional de Delitos Informáticos del FBI estima que entre el 85 y el 97 por ciento de las intrusiones en ordenadores no son detectadas. En un reciente informe del Departamento de Defensa, las estadísticas eran alarmantes. Se registraron un total de 8,932 sistemas atacados. A 7,860 de ellos los *hackers* accedieron con éxito. Se detectaron 390 de esas 7,860 intrusiones, y sólo 19 de ellas fueron denunciadas. "La razón de por qué sólo 19 de esos ataques fueron denunciados fue porque las organizaciones que asustan a sus empleados, clientes y accionistas harán que se pierda la fe en esa compañía si se admite que sus ordenadores han sido atacados. [8] Además, muy pocos de los delitos informáticos que se denuncian se resuelven alguna vez. De acuerdo con el CSI (Computer Security Institute) es decir, el Instituto de Seguridad Informática), estos son los tipos de delitos y pérdidas informáticos:

1. Errores humanos 55%.
2. Problemas de seguridad físicos 20% (p. ej. desastres naturales, o caídas de tensión).
3. Ataques internos con objetivo de beneficiarse de esos delitos informáticos 10%.
4. Empleados descontentos buscando venganza 9%
5. Virus 4%
6. Ataques externos 1.3%

[8] En www.delitosinformaticos.com. Art. Pub. por Richard Power del Computer Security Institute. Fecha de acceso 27/01/02

Si tenemos en cuenta que muchos de los ataques externos provienen de delincuentes informáticos profesionales muchos de los cuales son empleados de la competencia de las víctimas, los *hackers* son responsables de casi ningún daño producido a todos estos ordenadores. Con esto estaríamos diciendo que el *hacker* "recreacional" que disfruta únicamente con curiosear por los ordenadores de otras personas no es el tipo de persona del que debemos tener miedo, ya que posiblemente el causante del daño sea un empleado que trabaje en la empresa de la víctima.

Para los Estados Unidos de Norteamérica el delito informático es considerado como tal, cuando entra en alguna de las siguientes categorías:

1. Implica el compromiso o el robo de información de defensa nacional, asuntos exteriores, energía atómica , u otra información restringida.
2. Implica a un ordenador perteneciente a departamentos o agencias del gobierno de los Estados Unidos.
3. Implica a un banco o cualquier otra clase de institución financiera.
4. Implica comunicaciones interestatales o con el extranjero.
5. Implica a gente u ordenadores en otros países o estados.

En estos casos, el FBI ordinariamente tiene jurisdicción sobre los casos que impliquen o sean referentes a la seguridad nacional, terrorismo, desfalcos a bancos y crimen organizado. El Servicio Secreto americano tiene jurisdicción en cualquier momento que el Ministerio de Hacienda sea atacado, o si los ataques no están bajo la jurisdicción del FBI.

En los Estados Unidos existen leyes federales que protegen contra el ataque de ordenadores, uso ilegítimo de passwords, invasiones electrónicas en la privacidad, y otras transgresiones. El Pronunciamiento sobre Abuso y Fraude Informático de 1986 es la principal pieza legislativa que gobierna la mayoría de los delitos informáticos, aunque muchas otras leyes pueden ser usadas para perseguir diferentes tipos de delitos informáticos. El pronunciamiento fue modificado con Título 18 USA Código 1030. También complementó a la Ley de Privacidad de las Comunicaciones Electrónicas de 1986, que dejó fuera de la ley el interceptar

comunicaciones digitales y había sido recién aprobada. Las Modificaciones de la Ley de Abusos Informáticos de 1994 amplió la Ley de 1986 al acto de transmitir virus y otra clase de código dañino.

En adición a las leyes federales, la mayoría de los estados han adoptado sus propias leyes de delitos informáticos. Como se mencionó líneas arriba, las dos leyes federales más importantes en los Estados Unidos de Norteamérica contra los delitos informáticos son 18 ASC: Capítulo 47, Secciones 1029 y 1030.

La Sección 1029 prohíbe el fraude y cualquier actividad relacionada que pueda realizarse mediante el acceso o uso de dispositivos falsificados como claves, tarjetas de crédito, números de cuentas, y algunos tipos más de identificadores electrónicos.

Existen nueve áreas de actividad criminal que se encuadran en la Sección 1029, las mismas que son las siguiente:

1 Producción, uso o tráfico de dispositivos de acceso falsificados. Pena: Multa de $50.000 o dos veces el valor del crimen cometido y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

2 Uso u obtención sin autorización a dispositivos de acceso para obtener algo de valor totalizando $1000 o más durante un periodo de un año. Pena: Multa de $10,000 o dos veces el valor del crimen cometido y/o hasta 10 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

3 Posesión de 15 o más dispositivos de acceso no autorizados o falsificados. Pena: Multa de $10,000 o dos veces el valor del crimen cometido y/o hasta 10 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

4 Fabricación, tráfico o posesión de equipo de fabricación de dispositivos de acceso ilegales. Pena: Multa de $50,000 o dos veces el valor del crimen cometido y/o hasta 15 años de cárcel, $1,000,000 y/o 20 años de cárcel si se reincide.

5 Realización de transacciones con dispositivos de acceso pertenecientes a otra persona con objetivo de obtener dinero o algo de valor totalizando $1000 o más durante un periodo de un año. Pena: Multa de $10,000 o dos veces el valor del crimen cometido y/o hasta 10 años de cárcel, $100,000 y/o hasta 20 años si se reincide.

6 Solicitar a una persona con objetivo de ofrecerle algún dispositivo de acceso o venderle información que pueda ser usada para conseguir acceso a algún sistema. Pena: Multa de $50,000 o dos veces el valor del crimen y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años si se reincide.

7 Uso, producción, tráfico o posesión de instrumentos de telecomunicación que hayan sido alterados o modificados para obtener un uso no autorizado de un servicio de telecomunicaciones. Pena: Multa de $50,000 o el doble del valor del crimen cometido y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años de cárcel si se reincide.

8 Uso, fabricación, tráfico o posesión de receptores, escaneadores o hardware o software usado para alterar o modificar instrumentos de telecomunicaciones para obtener acceso no autorizado a servicios de telecomunicaciones.[9] Pena: Multa de $50,000 o dos veces el valor del crimen y/o hasta 15 años de cárcel, $100,000 y/o hasta 20 años si se reincide.

9 Hacer creer a una persona que uno es un miembro de su compañía de tarjeta de crédito o su agente para obtener dinero o realización de transacciones hechas con un dispositivo de acceso, y viceversa; tratar de hacer creer a la compañía de crédito que somos la persona legítima. Pena: Multa de $10,000 o dos veces el valor del crimen y/o hasta 10 años de cárcel, $100,000 y/o hasta 20 años si se reincide.

9 http://publicaciones.derecho.org/redi/No.13_agosto_de_1999/ponencia

En el 18 USC, Capítulo 47, Sección 1030, decretado como parte de la Ley sobre Abuso y Fraude Informático de 1986, prohíbe el acceso no autorizado o fraudulento a ordenadores gubernamentales, y establece diversas condenas para esa clase de accesos. Esta ley es considerada una de las pocas piezas de legislación federal únicamente referidas a ordenadores.

Bajo la Ley de Abuso y Fraude Informático, el Servicio Secreto americano y el FBI tienen jurisprudencia para investigar los delitos definidos en este decreto. Las seis áreas de actividad criminal cubiertas por la Sección 1030 son:

1 "Adquisición de información restringida relacionada con defensa nacional, asuntos exteriores, o sobre energía nuclear con el objetivo o posibilidad de que sean usados para dañar a los Estados Unidos o para aventajar a cualquier otra nación extranjera. Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

2 Obtención de información en un registro financiero de una institución fiscal o de un propietario de tarjeta de crédito, o información de un cliente en un archivo de una agencia de información de clientes. Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

3 Atacar un ordenador que sólo corresponda usar a algún departamento o agencia del gobierno de los EEUU, o, si no sólo puede ser usada por esta agencia, atacar un ordenador usado por el gobierno en el que la intrusión producida afecte el uso que el gobierno hace de él Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide.

4 Promover un fraude accediendo a un ordenador de interés federal y obtener algo de valor, a menos que el fraude y la cosa obtenida consistan solamente en el uso de dicho ordenador. Pena: Multa y/o hasta 5 años de cárcel, hasta 10 años si se reincide.

5 A través del uso de un ordenador utilizado en comercio interestatal, transmitir intencionadamente programas, información, código o comandos a otro sistema

informático. Pena con intento de dañar: Multa y/o hasta 5 años de cárcel, hasta 10 años si se reincide. Pena por actuación temeraria: Multa y/o hasta 1 año de cárcel.

6 Promover el fraude traficando con passwords o información similar que haga que se pueda acceder a un ordenador sin la debida autorización, todo esto si ese tráfico afecta al comercio estatal o internacional o si el ordenador afectado es utilizado por o para el Gobierno. Pena: Multa y/o hasta 1 año de cárcel, hasta 10 años si se reincide".

Así, la legislación americana amplia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos, imponiendo para ambos, además de la aplicación de multa, un año de prisión para los primeros y 10 años para los segundos. Asimismo, se contempla la regulación de los virus, conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

4.3 El Sistema Penal Chileno

La estructura de los tipos penales informáticos en la legislación en análisis gira en torno a la regulación de distintas conductas de sabotaje informático, sin considerar conductas vinculadas a la afectación de la intimidad o del patrimonio. Desde esta perspectiva, podemos sostener que se ha pretendido dotar a los delitos informáticos de una autonomía e identidad propias, distinguiéndolos de aquellas modalidades de delitos contra la intimidad o contra el patrimonio realizados por medios informáticos. Esta orientación político criminal coincide con la tesis asumida en la presente investigación, en cuanto somos de la opinión que las afectaciones a la intimidad y al patrimonio mediante el empleo de medios informáticos no constituyen delitos informáticos, sino modalidades de estos delitos en cuya realización se ha empleado una computadora o un sistema informático.

Ahora bien, en cuanto a lo que es la protección misma de la información o datos contenidos en los sistemas y los sistemas como tales, se advierte que el legislador expresamente hace la distinción de la afectación de ambos, considerando así la importancia del funcionamiento del sistema.

El artículo 1 de la Ley sanciona la conducta de sabotaje informático en los siguientes términos:

"Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. [10]

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

Este primer párrafo del artículo 1° de la Ley hace alusión directa al soporte y a su funcionamiento, de esta forma queda recogida también la protección del software y el hardware. Este acento puesto por el legislador penal chileno en cuanto al funcionamiento de los propios sistema no se observa en la legislación nacional ni en la de aquellos países que comentamos en la presente investigación, por lo que podemos señalar que es una cualidad propia de esta legislación.

Ahora bien, el funcionamiento del sistema informático se encontraría en función de la seguridad informática, ya que, precisamente, lo que se pretende proteger salvaguardar son las funciones de acceso y transmisión propias de la red y sistemas informáticos, lo cual implicaría el acceso a la misma y su libre tránsito por la red, estos se ven afectados, sin lugar a dudas, cuando se atenta contra el funcionamiento del sistema informático. Adicionalmente, el término "maliciosamente" contenido en este precepto hace alusión al conocimiento por parte del autor del carácter indebido de la conducta, lo cual permitiría comprender por qué el legislador no ha consignado expresamente que la conducta ha de ser sin la autorización del titular. Este tema está vinculado con la repercusión del consentimiento del titular en este delito, ya que a pesar de

[10] En www.latinlex.com/cl/contenido/leg4.asp.

no haberse consignado expresamente que la conducta ha de ser sin la autorización del titular, el consentimiento tiene enorme significación para la tipicidad de la conducta, en la medida que el sujeto puede disponer de sus sistemas de tratamiento de información, sus datos e información.

El segundo párrafo del artículo 1° se refiere expresamente a la afectación de los datos contenidos en los sistemas (la información codificada) a través de las conductas descritas en el primer párrafo, esto es, la destrucción o inutilización de los sistemas de tratamiento de información o la alteración de su funcionamiento, esta referencia a los datos como objeto de protección los realza precisamente al dotársele de protección penal y al sancionar su afectación con una mayor penalidad respecto de los ataques a los sistemas mismos. No obstante, la afectación al sistema aparejada de la afectación de los datos encierra un mayor desvalor de resultado y, en consecuencia, a ello también obedecería la elevación de la pena para este supuesto.

El artículo 2° de la Ley sanciona el denominado delito de intrusismo informático en los siguientes términos:

"Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio"

En este precepto se sanciona el acceso, la interceptación o interferencia a un sistema de tratamiento de información. Lo especial de este artículo es que no se hace una referencia a si este tipo de ingreso ha de ser sin la autorización del titular, lo cual muestra un vacío, ya que podría interpretarse que quedaría comprendido también el ingreso consentido, bastando sólo alguna de las finalidades señalas en la norma: apoderarse, usar o conocer indebidamente la información. Por ello, resultaría necesario en este caso acudir a una interpretación restrictiva de este tipo penal, con la finalidad de evitar excesos en la intervención penal.

Por otra parte, no se trata del mero intrusismo blanco que se caracteriza por el solo hecho de entrar a un sistema sin una finalidad distinta al ingreso, sino de un intrusismo con una finalidad

específica que es la de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento, por lo que se trataría, como en el caso de la legislación penal peruana, de un elemento subjetivo de intención trascendente cuya materialización no es requerida por el tipo penal, ya que éste sólo exige la realización de las conductas de interceptar, interferir o acceder al sistema informático.

El artículo 3° de la Ley sanciona la lesión de los datos informatizados en los siguientes términos:

"Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio" Se trata de una modalidad de afectación de los datos distinta a la contenida en el segundo párrafo del artículo 1° de la Ley, ya que en este último caso lo que se sanciona es la afectación de los datos contenidos en sistemas de tratamiento de información a través de la destrucción o inutilización del propio sistema, mientras que en el dispositivo en análisis se trata de la alteración, destrucción o inutilización de los datos por cualquier otra forma distinta a la mencionada.

Aquí también se puede que la expresión "maliciosamente" es para acentuar el carácter doloso de la conducta, descartando así la sanción de cualquier forma de realización culposa de esta conducta.

5. Otras Legislaciones en el Ámbito Internacional

Algunas legislaciones del contexto internacional que cuentan con una legislación apropiado sobre el presente tema de investigación entre ellos, se destacan, Alemania, Gran Bretaña, Holanda y Francia.

A continuación se mencionan algunos aspectos relacionados con la ley en dichos países, así como los delitos informáticos que persiguen.

5.1 Alemania

Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

- ✓ Espionaje de datos.
- ✓ Estafa informática.
- ✓ Alteración de datos.
- ✓ Sabotaje informático.
- ✓ Fraude Informático.

5.2 Holanda

El 1° de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

- ✓ El hacking.
- ✓ Sabotaje informático.
- ✓ El preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).
- ✓ La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).
- ✓ La distribución de virus.

5.3 Francia

En enero de 1988, este país dictó la Ley relativa al fraude informático, en la que se consideran aspectos como:

- ✓ Intromisión fraudulenta que suprima o modifique datos.
- ✓ Conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.

- ✓ Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.
- ✓ Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

En el presente capítulo se han dejado fuera muchos países que en la actualidad regulan las actividades informáticas en sus respectivas legislaciones, sin embargo se han mencionado las naciones que se mostraron más interesados en incluir dichas conductas en sus ordenamientos legales. En vista, de que los delitos informáticos, son un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de computadoras podría tener consecuencias desastrosas. A este respecto el Octavo congreso sobre Prevención del delito y Justicia Penal, celebrado en 1990 en la Habana Cuba, recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Por su parte, el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena Internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertado. Asimismo, la ONU resume de la siguiente manera los problemas que rodean a la cooperación internacional en el airea de los delitos informáticos:

a) Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
b) Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
c) Falta de especialización de los policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
d) No existe armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

e) Carácter transnacional de muchos delitos cometidos mediante el uso de las computadoras.
f) Ausencia de tratados de extradición, de acuerdos, y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Teniendo presente esa situación, es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. Consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada.

CONCLUSIONES

PRIMERO

Para que una conducta sea considerado como delito debe ser definido claramente de manera inequívoca la licitud del hecho y descrito en la tipificación penal, la cual lesione o ponga en peligro, sin una justa causa, el interés jurídicamente tutelado. Que no es delito por el principio Nullum crimen sine conducta, de esta manera siendo el resultado, como consecuencia de la acción u omisión del sujeto, así que en el momento de la ejecución del hecho, posea la capacidad de comprender la licitud del hecho.

SEGUNDO

Por el principio de legalidad, propio del Derecho Penal, es imposible sancionar como conductas delictivas hechos no descritos en el ordenamiento jurídico penal vigente, pues la tipificación de los delitos es una garantía contra la arbitrariedad a la que podría llevar la analogía en la aplicación de las penas. La ausencia de figuras concretas que se puedan aplicar en esa materia daría lugar a que los autores de esos hechos quedaran impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos.

TERCERO

Las características de los delitos informáticos son:

- La impunidad de los delitos, por falta de denuncia de la persona natural o damnificado, por el temor a la perdida de imagen y desprestigio en el público.
- Este tipo de delitos puede desenvolverse sin dejar rastros.
- El delincuente no asume riesgos físicos, tampoco desarrolla violencia.
- El importe medio de un delito es muy superior al de un delito manual.
- Este tipo de delitos es muy rentable.

CUARTO

Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometen mediante el uso de los ordenadores. De la misma forma debe destacarse el papel del Estado, que aparece como el principal e indelegable regulador de la actividad de control y flujo informativo a través de las redes informáticas.

QUINTO

Dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

SEXTO

Así mismo, la problemática de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (microprocesadores, redes, internet, etc.), evitando que la norma jurídica quede desfasado del contexto en el cual se debe aplicar.

SÉPTIMO

Una de las causas de comisión de estos delitos, se debe al descuido de controles que requiere el tratamiento de información automatizada, debido a la equivocada opinión pública de que el uso de computadoras es garantía suficientes de seguridad.

RECOMENDACIONES

PRIMERO

Políticas de seguridad: En cuanto a acceso de los servicios de la red de una empresa, a mayor acceso, mayor es el peligro de que alguien explote lo que resulta del incremento de vulnerabilidad. Así mismo comprende la identificación de los activos organizativos: Por ejemplo (hardware, Software, Datos), la implementación de las herramientas y tecnologías disponibles para hacer frente a los riesgos y la definición de una política aceptable debe considerar:

- ¿Quién tiene privilegios de administración del sistema?
- ¿Qué hacer con la información confidencial?
- ¿Cuáles son los derechos y responsabilidades de los usuarios?
- ¿Quién está autorizado a conceder acceso y aprobar los usos?
- ¿Con que frecuencia deben cambiar sus contraseñas?

SEGUNDO

Protección hacia el sistema informático frente a las nuevas y diferentes figuras de conductas criminales, y la necesidad de tomar medidas preventivas y preventivas en cuanto se refiere a las conductas no tipificadas en el Código Penal vigente. De esta manera es recomendable al usuario:

- Debe crearse un procedimiento de auditoria que revise el uso de la red y servidores de forma periódica.
- Capacitar constantemente personal informático, para evitar hechos negligentes.
- No ejecutar ningún archivo adjunto a un mensaje de correo electrónico que sea diferente, desconocido, y si fueren conocidos si es que no hayan sido solicitados por el usuario.

TERCERO

Por el modus operandis de esta clase de conductas, es lo que las hace particularmente difíciles de pesquisar, para su esclarecimiento, no bastan los métodos clásicos de criminalística sino que se requiere el manejo de conocimientos en el área de la informática y la colaboración y actualización constante con otras unidades especializados con otros países.

BIBLIOGRAFIA

ENCICLOPEDIA DE INFORMATICA Y COMPUTACIÓN, Edición 1997, Cultural S.A., Polígono Industrial Arroyomolinos, Madrid España.

MANUAL DE PREVENCIÓN DEL FRAUDE. Rodríguez Zarco Juan Manuel, primera edición 1991, ESABE EDITORIAL S.A. Gran Via 67,2° Madrid.

TRATADO DE DERECHO PENAL, Fontan Balestra Carlos, Ed. Abeledo Bs.As., 2ª edición

DERECHO INFORMÁTICO, M. Correa Carlos, Ed. Depalma ,1987, Bs As.

CODIGO PENAL BOLIVIANO CON LAS REFORMAS Y LEYES CONEXAS, Benjamín Miguel Harb, edición 2ª, Ed. Urquizo S.A.

DERECHO PENAL, Benjamín Miguel Harb, T.I, edición4ª,Ed. La Juventud.

CODIGO DE PROCEDIMIENTO PENAL, Norales Guillén Carlos, 2ª Edición 1995. Ed. Gisbert y Cia. S.A..

CODIGO PENAL DE ESPAÑA, www.law.unicon.es/incade/lex/cpo1.htm

CODIGO PENAL DE CHILE, www.viajuridica.cl/index.asp

CODIGO PENAL DE LA NACIÓN ARGENTINA (Legislación complementaria). Ed. Universidad, 1997.

CODIGO PENAL ALEMÁN, Emilio Eiranova Encinas, Ed. Jurídicas Sociales. S.A.

DICCIONARIO DE CIENCIAS JURÍDICAS, POLÍTICAS Y CIENCIAS SOCIALES. Ossorio Manuel, Ed. Heliasta S.R.L. Buenos Aires, 1987.

Hoja electrónica:

- http://publicaciones.derecho.org/redi/No.06_Enero_de _1999/cuervo. Fecha de acceso: 27 de enero del año 2002.
- http://publicaciones.derecho.org/redi/No.13_agosto_de_1999/ponencia
- http://publicaciones.derecho.org/redi/No._06_Enero_de_1999/cuervo. Fecha de acceso: 27 de enero del año 2002.
- http://delitosinformaticos.com/noticias/98378704517479.htm Fecha de acceso: 28 de enero d el año 2002.
- http://publicaciones.derecho.org/redi/No._09_-_Abril_de_1999/viega Fecha de acceso: 27 de enero del año 2002
- www.latinlex.com/cl/contenido/leg4.asp.
- http://publicaciones.derecho.org/redi/No.13_agosto_de_1999/ponencia Fecha de ingreso 26 de enero de 2002
- http://www.el-mundo.es/2000/08/05/economia/05n0098.html Fecha de ingreso 16 de enero de 2002
- http://www.el mundo.es /navegante/2000/05/09/fbi -alataque.html Fecha de ingreso 16 de enero de 2002
- http://www.elmundo.es/navegante/2002/02/26/seguridad/1014729000. html fecha de ingreso 30 de marzo de 2002
- http://www.elmundo.es/navegante/99/agosto/26/tarjetas.html Fecha de ingreso 18 de enero de 2002
- www.abity.com/navegar/internet/historia.com
- www.reuna.cl/central-apunte/reporte.g.htm