UNIVERSIDAD VILLA RICA

ESTUDIOS INCORPORADOS A LA
UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE DERECHO

"PROTECCIÓN PENAL DE LA PROPIEDAD INTELECTUAL EN INTERNET"

TESIS

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN DERECHO

PRESENTA:

LUIS ALBERTO LINARES PRIETO

Director de Tesis:	**Revisor de Tesis**
LIC. FELIPE DE JESUS RIVERA FRANYUTI	LIC. GENARO CONDE PINEDA

BOCA DEL RIO, VER. **2009**

AGRADECIMIENTOS

Esta tesis, sin duda esta dedicada **A MIS PADRES,** Gracias por su amor, por su paciencia y por su compresión. Gracias también por la familia y el ejemplo que siempre me han dado; GRACIAS PACHO Y TERRIBLE POR SER LOS MEJORES PAPAS DEL MUNDO. Los quiero mucho.

Agradezco también **A MI HERMANA,** Por siempre estar ahí para darme esas palabras de apoyo, por hacerme ver las cosas de la mejor manera, por aguantarme en esos malos ratos y quererme aun después de ellos, simplemente por ser mi hermana, GRACIAS MOROC. Te quiero mucho.

Finalmente a Dios y a todas las personas que siempre estuvieron a mi lado regañándome, apoyándome, dándome siempre esos consejos que a la larga me ayudaron a finalizar esta etapa tan importante en mi vida, GRACIAS.

I N D I C E

CAPITULO II

ANTECEDENTES INFORMATICOS

CAPITULO III

FENOMENO INFORMATICO.

CAPÍTULO IV

DELITOS INFORMÁTICOS

CAPITULO V

PROTECCION PENAL DE LA PROPIEDAD INTELECTUAL EN INTERNET.

INTRODUCCION

La presente investigación es de gran importancia en el campo del Derecho Penal Informático, ya que de un tiempo a la fecha ha crecido de una manera impresionante, llegando a ser el futuro de una gran variedad de actividades indispensables para la vida y convivencia del ser humano, volviéndose necesario contar con una regulación especifica y funcional para el buen uso de la Internet en general.

Consta de seis capítulos, los cuales contienen información indispensable para la realización de este trabajo de investigación. En el segundo capitulo se da una reseña de los antecedentes históricos así como la relación creciente con la actividad cotidiana de las personas, el tercer capitulo habla sobre el fenómeno informático en sí, en el cuarto capitulo nos enfocamos en hacer una pequeña recopilación de los diversos delitos informáticos que existen, en el capitulo quinto nos dedicamos a analizar a fondo el tema de la presente investigación, terminando en el sexto capitulo con mis conclusiones e ideas finales.

CAPITULO I
METODOLOGÍA DE LA INVESTIGACIÓN.

1.1. PLATEAMIENTO DEL PROBLEMA.

¿Existe verdadera protección penal de la Propiedad Intelectual en Internet?

1.2. Justificación del Problema.

Uno de los más graves errores que se puede cometer al desarrollar un tema de Derecho Penal es circunscribirse a un ordenamiento en específico, por tal motivo, cuando se habla de Derecho Penal Informático debido a su natural trasnacionalidad de los actos dañosos que esta nueva tecnología implica. Dicha trasnacionalidad se debe tomar siempre en cuenta con el fin de realizar una aproximación coherente con las conductas de los posibles transgresores de los derechos ajenos. Esta trasnacionalidad de los actos lesivos y la dificultad de encuadramiento personal de los

sujetos activos hace que se presente un panorama muy difícil de resolver en la mayoría de las situaciones prácticas, por lo tal debe quedar en claro que es casi imposible identificar a los transgresores en forma fehaciente durante sus actividades en la red.

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

Por otro lado, la posibilidad de incompetencia de los jueces, la imposibilidad de extradición, la garantía del juez natural reconocida en los tratados internacionales de Derechos Humanos, así como el debido proceso y el “in dubio pro reo”, presentan limites infranqueables para una legislación que no haya tenido una debida planificación para otorgar una función preventiva de la cual se nutre el Derecho Penal.

Es claro que para los posibles infractores al ver las lagunas en la aplicación de las normas penales, será fácil para ellos hacer caso omiso de ellas y encontrarse así en la directa inaplicabilidad del sistema.

1.3. Delimitación de Objetivos.

1.3.1. Objetivo General.

Analizar la posible protección penal con respecto a la Propiedad Intelectual.

1.3.2. Objetivos específicos.

1.3.2.1. Conocer la Propiedad Intelectual.

1.3.2.2. Enlistar las leyes aplicables para la protección de la Propiedad Intelectual.

1.3.2.3. Examinar las conductas lesivas que afectan la Propiedad Intelectual en Internet.

1.3.2.4. Demostrar la dificultad de proteger Penalmente a la Propiedad Intelectual en Internet.

1.4 Formulación de la Hipótesis.

1.4.1 Enunciación de la Hipótesis.

No existe una verdadera protección Penal de la Propiedad Intelectual en Internet, debido a la dificultad que se presenta en la aplicación de las disposiciones de la Ley aplicable.

1.5. Determinación de Variables.

1.5.1. Variable Independiente.

Es patente la inaplicabilidad de las disposiciones Penales que protegen a la Propiedad Intelectual en Internet, ya que la legislación resulta limitada porque no esta diseñada acorde a la realidad “imperante”.

1.5.2. Variable Dependiente.

“Encontramos” un sinnúmero de conductas lesivas hacia la propiedad intelectual a través de Internet, que son imposibles de sancionar por la forma en que se encuentran regulados estos delitos.

1.6. Tipo de Estudio.

1.6.1. Investigación Documental.

Se hizo una investigación exhaustiva en diversos medios de consulta, como libros, Leyes, manuales y páginas de Internet.

1.6.1.1. Bibliotecas Públicas.

Unidad de Servicios Bibliotecarios y de Información Ubicada en Boulevard Ruiz Cortinez Esq. Juan Pablo Segundo S/N, Col. Costa Verde, C.P. 94299, Boca del Río, Veracruz.

1.6.1.2. Bibliotecas Privadas.

Biblioteca del Despacho Jurídico “PECA y ASOCIADOS” Barragán # 305 Col. Flores Magón. C.P. 91900.

Biblioteca Particular del Lic. Alberto Linares Vernet. Paseo Costa de Oro #747. Fracc. Costa de Oro. C.P. 94299, Boca del Río, Veracruz.

1.7 Técnicas Empleadas.

Se estructuraron Fichas Bibliográficas y Fichas de Trabajo.

1.7.1 Fichas Bibliográficas.

Se elaboraron diversas fichas con todos los requisitos necesarios de metodología que son: Nombre del autor, título, edición, editorial y lugar de fecha de edición.

1.7.2 Fichas de Trabajo.

Se estructuraron dichas fichas cumpliendo con los requisitos metodológicos.

CAPITULO II
ANTECEDENTES INFORMATICOS

2.1. DESARROLLO INFORMÁTICO

Internet surge como desde los años 60's dentro del ejército norteamericano, como un proyecto, dentro del área de defensa para crear un sistema de información imposible de destruir debido a su complexión: intangible.

Antes de 1991 Internet era exclusivo del gobierno norteamericano y de instituciones educativas. En 1991 se fundo la Asociación de Intercambio Comercial de Internet (CIX), con el objetivo de promover una "carretera libre de barreras" para empresas y personas de todo tipo.

A pesar de que Internet fue creado para ayudar a la milicia y a la investigación educacional ahora Internet está construida por 21,000 redes de información, 15 millones de usuarios, 2 millones

de computadoras, con un crecimientos del 7 al 10% mensual.

Internet no es algo tangible ni una organización. Nadie es su dueño, nadie la corre. Simplemente Internet es una telaraña de computadoras interconectadas que toma forma con muy poco planteamiento.

Pero Internet es más que una simple conexión de computadoras y cables, es una comunidad mundial de personas que comparten una gran variedad de intereses y necesidades.

2.2. INFORMATIZACION SOCIAL Y DEL DERECHO.

Es indudable que así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un verdadero instrumento de actos ilícitos. Este tipo de actitudes concebidas por el hombre encuentran sus orígenes desde el mismo surgimiento de la tecnológica informática.

La facilitación de las labores que traen consigo las computadoras, propicia que en un momento dado, el usuario se encuentre ante una situación de ocio, la cual canaliza a través de la computadora, cometiendo sin darse cuenta una serie de ilícitos.

La evolución tecnológica ha generado un importante número de conductas nocivas que, aprovechando el poder la información, buscan lucros ilegítimos y causan daños. El derecho que por esencia se muestra reticente al cambio, no ha reaccionado adecuadamente a las nuevas circunstancias.

Esta marcha de las aplicaciones de la informática no solo tiene un lado ventajoso sino que también plantea problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Debido a esta vinculación el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los estados, Europa occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a Paris en Mayo de 1983, el término “delitos relacionados con las computadoras” se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o trasmisiones de datos.

La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, preventivos o legales.

Se define al delito o crimen informático como toda interrupción, uso indebido, modificación o fabricación de datos ajenos que se encuentren en sistemas de computación, sin autorización expresa o implícita de su dueño y/o de quien ostente la propiedad intelectual, con el objeto de obtener un provecho económico o no.

De la definición arriba descrita podemos diferenciar entre dos clases de delitos informáticos:

Ataque pasivos.

- Divulgación de contenido de mensajes ajenos.
- Análisis del tráfico de información de terceros.

Ataques Activos.

- Utilización de passwords ajenos.
- Modificación o alteración de mensajes y/o archivos.
- Obstaculización de accesos legítimos.

En la actualidad la informatización se ha implantado en casi todos los países. Tanto en la organización, administración de empresas, administraciones públicas, en la investigación científica, en la producción industrial, en el estudio e incluso en el ocio; el uso de la informática es en ocasiones indispensable y hasta conveniente, sin embargo junto a las incuestionables ventajas que presenta, comienzan a surgir algunas facetas negativas como por ejemplo, lo que ya se conoce como “criminalidad informática”.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con animo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales y morales.

Pero no solo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia

tradicional, sino que también son mucho mas elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de datos.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme que va mucho mas allá del valor material de los objetos destruidos.

A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos y ser descubiertos.

En consecuencia la legislación sobre protección de los sistemas informáticos ha de conseguir acercarse lo mas posible a los distintos medios de comunicación ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, en base a, las peculiaridades del objeto de protección sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades, como bancarias, financieras, tributarias y de identificación de las personas.

Y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un estado o particulares, se comprenderá que están en juego o podrán llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, si no la utilización real por el hombre de los sistemas de información con fines de espionaje.

Tampoco son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco concientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no está frente al peligro de la informática, sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puedes conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Así mismo la amenaza será directamente proporcional a los adelantos de las tecnologías informáticas.

Dar un concepto sobre delitos informáticos no es una labor fácil y esto es en razón de que su misma denominación alude a una situación por demás especial, ya que para hablar de “delitos” en el sentido de acciones tipificadas o contempladas en textos jurídicos-penales se requiere que la expresión “delitos informáticos” este consignada en los códigos penales, lo cual en nuestro país, al igual que en muchos otros, no ha sido objeto de tipificación aun, sin embargo, muchos especialistas en derecho informático emplean esta alusión a los efectos de una mejor conceptualización.

2.3. INFORMATICA JURIDICA.

Es una disciplina bifronte en la que se entrecruzan una metodología tecnológica con sus posibilidades y modalidades de la aplicación. La informática jurídica estudia el tratamiento automatizado de: las fuentes del conocimiento jurídico a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (informática jurídica documental); las fuentes de producción jurídica, a través de la elaboración informática de los factores lógico-formales que concurren en proceso legislativo y en la decisión judicial (informática jurídica decisional); y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el derecho (informática jurídica de gestión).

2.4. IMPORTANCIA DE LA INFORMATICA.

2.4.1. REGULACIÓN JURÍDICA DEL BIEN INFORMATICO.

Los intereses difusos, que bien pueden llamarse asimismo intereses de “pertenencia difusa”, porque pertenecen a muchos en

común, integrando todos ellos un conjunto difuso, con lo que “lo difuso” es el grupo humano que coparticipa en el interés, y no tanto el interés mismo, que se puede percibir como concreto, se confunden con frecuencia con los intereses colectivos, en ambos casos, el bien jurídico protegido es indivisible.

Sin embargo, mientras entre los titulares de un interés difuso no existe relación jurídica alguna (pensemos por ejemplo en los consumidores y usuarios, si bien es cierto que últimamente han surgido organizaciones de tales, o en quienes reclaman que cesen las agresiones al medio ambiente), si que existe una relación de base entre los titulares de un interés colectivo, relación que viene dada por la vinculación directa de los miembros del colectivo (una asociación o conjunto de asociaciones), o por un vinculo jurídico que se les relaciona con la parte contraria, por así llamarla (los disidentes universitarios, por ejemplo).

En todo caso, la diferencia tiende a atenuarse porque cada vez son mayores los intentos de amplios sectores sociales de vertebrarse, de organizarse jurídicamente con vistas precisamente a una defensa mas eficaz de esos intereses difusos.

Al tratarse de un interés comúnmente compartido pro muchas personas, su afectación plantea de inmediato la problemática de si accionabilidad, esto es, de la legitimación procesal para recurrir, que con los criterios individualistas tradicionales requiere de una afectación actual y directa en la esfera jurídica (derechos o intereses legítimos) de una determinada persona, con la que la pervivencia, en estos supuestos de interés difuso, de un criterio de legitimación procesal clásico puede poner en peligro la tutela de tales intereses.

Aun cuando admitiéramos con Bidart Campos que estamos ante "situaciones jurídicas subjetivas", que no se esfuman ni pierden la naturaleza de tales por la circunstancia de que cada uno de los sujetos que las titularicen compongan un grupo o conjunto humano al que le es común ese mismo interés (la afectación del interés perjudica al conjunto, y por lo mismo, también a casa persona que forma parte de él), si mantenemos, en coherencia con ello, los criterios de legitimación procesal tradicionales y entendemos que un individuo esta legitimado para recurrir en defensa de un interés difuso que, sin embargo, en cuanto tal también le es propio, es mas que probable que nos encontremos con notabilísimos desequilibrios entre las partes de ese proceso: una persona en defensa del medio ambiente frente a los vertidos contaminadores de una gran empresa multinacional; un consumidor enfrentado a un gran grupo de distribución de mercancía, etcétera.[1]

A la vista de todo ello, se impone, pues, una radical mutación de los esquemas tradicionales de la tutela jurisdiccional, una, como dice Cappelletti, profunda metamorfosis del derecho procesal para evitar que permanezcan prácticamente desprovistos de protección los intereses difusos, cambio que posiblemente exija un abandono en ciertos casos de la idea de subjetividad como categoría del derecho público, cuya insuficiencia y efectos negativos[2]; como bien apunta De Cabo, se han manifestado en diversos sectores, uno de ellos, desde luego, el que ahora nos ocupa[3].

Parece necesario, consecuentemente, la búsqueda de nuevas categorías jurídicas que vinculen en estos casos la protección no

[1] Bidart Campos, Germán José, Teoría General de los Derechos Humanos, 1° Ed., 1991, P. 425.
[2] Cappelletti Mauro, Access to Justice; Milan, Italia. 4° Ed., 1979, P. 281.

tanto a un sujeto cuanto a un elemento objetivo como puede ser la protección del interés colectivo, difuso o general. A ello se vincula íntimamente la necesaria revisión del concepto tradicional de legitimación procesal, que también Fix-Zamudio ha reivindicado últimamente[4].

En la misma dirección, Haberle ha entendido que el reconocimiento de una legitimación para recurrir a ciertos grupos u organizaciones podría tener una indudable virtualidad instrumental en orden a la efectividad práctica de los derechos fundamentales, porque tal efectividad se produce también a través del pluralismo de la opinión pública.

2.4.2. PROTECCION DE DATOS PERSONALES

En México, la privacidad y los datos de las personas en las relaciones entre empresas y consumidores se encuentra regulada en la Ley Federal de Protección al Consumidor y en otras disposiciones sobre privacidad contenidas en ordenamientos jurídicos a nivel federal.

Sin embargo, en la medida en la que se extienda la penetración y uso de Internet, se deberá evaluar la posibilidad de crear un marco jurídico mas amplio y eficiente que proteja los datos y la información proporcionada por los ciudadanos no solo a os sitios Web de las empresas comerciales, sino sobre todo a los órganos gubernamentales cuyos servicios y tramites se ofrecerán en línea a un futuro cercano.

---

[3] De Cabo, Filosofía del Derecho y Filosofía de la Cultura. 3° Ed., 1982. P.154.
[4] Fix-Zamudio, Héctor y Ovalle Favela, José; Derecho Procesal; 1° Ed. 1991, México, P.127.

Resulta conveniente, que en sectores altamente sensibles en donde la confidencialidad de la información de las personas en considerada primordial, como son el sector salud, bancario y laboral, se contemple la posibilidad de incluir aspectos puntuales sobre privacidad y protección de datos personales en el ámbito de sus respectivas leyes, reglamentos y ordenamientos.

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos representa el marco de la privacidad en nuestro país. El primer párrafo de este articulo consagra una de las garantías individuales mas importantes que es el derecho que tenemos a no ser molestados en nuestras personas, familia, domicilio, papeles o posesiones, sino en virtud de un mandamiento estricto de la autoridad competente, que funde y motive la causa legal del procedimiento, y en el penúltimo párrafo de este mismo articulo, se contempla que la correspondencia que bajo cubierta circule por las estafetas, deberá estar libre de todo registro y su violación será penada por la ley.

2.4.3. FLUJO DE DATOS TRANSFRONTERIZOS.

Las disposiciones tendientes a proteger la información personal y la confidencialidad de los datos correspondientes a los consumidores de bienes o servicios en Internet, La Ley Federal de Telecomunicaciones en su Articulo 49 establece que: la información que se transmita a través de redes y servicios de telecomunicaciones será confidencial, salvo aquella que, por su propia naturaleza sea pública o cuando medie orden de autoridad competente.

Existen otras disposiciones sobre la confidencialidad de los datos que se transmiten electrónicamente tanto de personas como de empresas en la Legislación Bancaria y del Mercado de Valores, así como en otras leyes administrativas en las que los particulares deben proporcionar información confidencial a las autoridades competentes.

No obstante lo anterior, México no cuenta con una legislación especifica integral sobre este tema y desde luego, no existe disposición alguna que regule, restrinja o prohíba el flujo el flujo de datos transfronterizos de sus ciudadanos.

2.4.4. PROTECCION DE LOS PROGRAMAS DE CÓMPUTO.

En el ámbito nacional hasta hace muy poco tiempo se le ha dado la debida importancia a la problemática jurídica derivada del uso de las computadoras y de los programas de computación. Esto se debe fundamentalmente, como ya se menciono anteriormente, al atraso de la recepción de la tecnología proveniente del extranjero.

Afortunadamente, gracias al esfuerzo de algunos juristas mexicanos se ha hecho resaltar la trascendencia jurídica que trae consigo la falta de una legislación adecuada que proteja tanto a los autores de los programas de cómputo como a los usuarios de los mismos. Al efecto, existen dos ordenamientos jurídicos que contienen disposiciones referentes a los programas de cómputo y que son: La Ley sobre el Control y Registro de la transferencia de tecnología y el Uso y Explotación de Patentes y Marcas y La Ley de Derechos de Autor.

La inclusión de los programas de cómputo en el primero de estos ordenamientos (LRTT) se debió en gran medida a la preocupación de las autoridades mexicanas por frenar, en la medida de los posible, las importaciones de insumos tecnológicos o por lo menos llevarlos a su racionalización. Tratándose específicamente de los programas de cómputo, las autoridades de SECOFIN consideraron que, al importar como obligación la solicitud de aprobación de inscripción de los contratos por los que se comercialicen los programas establecida en la LRTT, se podría controlar su desarrollo en el país en todas sus facetas, es decir, en su importación, exportación, fomento de desarrollos nacionales y sobre todo el control de flujo de divisas al extranjero.

2.4.5. LOS CONTRATOS INFORMATICOS.

El desarrollo de las nuevas tecnologías ha propiciado el nacimiento de una nueva forma de contratación y de nuevas modalidades contractuales. En cada uno de los contratos de ha de prestar especial atención a su redacción, formulación y negociación

Un simple modelo de contrato no garantiza los efectos deseados, ya que una mala redacción de las mismas puede dar lugar a resultados y consecuencias jurídicas no deseadas. Se hace necesario conocer y respetar la legislación contractual a la hora de redactarlos, por ello las empresas y los consumidores en general han de poner en manos de abogados y profesionales del derecho la redacción de sus contratos, dada la complejidad de la materia y del lenguaje jurídico y técnico empleado en su redacción.

Los centros informáticos tienen varias funciones como aquellas relativas al procesamiento de datos y la entrega de resultados veraces y oportunos para la toma de decisiones; pero eso no es todo, también se realizan estudios previos a fin de satisfacer los requerimientos de equipo y materiales que dichos centros exigen para su adecuado funcionamiento, así como para satisfacer las necesidades de los usuarios. Para que se dé dicha situación, los centros informáticos se ven precisados a establecer contratos con las empresas proveedoras de bienes y servicios informáticos en aquello en aquello que se ha tenido a bien en llamar los “Contratos Informáticos”

Los bienes y servicios informáticos no dejan de ser el “producto” de una “transferencia tecnológica” originaria de los países altamente industrializados, provocando una marcada relación de dependencia en relación a los países en desarrollo.

Por contratos informáticos podemos entender todo acuerdo de partes en virtud del cual se crean, conservan, modifican o extinguen obligaciones relativas a los sistemas, subsistemas o elementos destinados al tratamiento sistematizado de la información.

Para tal efecto se han establecido dos criterios básicos como lo son el funcional en el que las prestaciones se relacionan con el tratamiento sistematizado de la información y el estructural en el que las prestaciones se relacionan con el equipo físico, el soporte lógico, la organización, la información, los suministros, la interacción de los elementos con el medio ambiente y los elementos o relaciones que integran los sistemas.

La importancia de dichos contratos estriba en que ante las lagunas y falta de certeza que presenta el derecho civil contractual, la redacción y negociación de estos contratos se ha convertido en la única “oportunidad” de que las partes se dicten por sus propias normas con el grado de precisión que requieren las circunstancias. Esta situación no se encuentra tan marcada como en otro tipo de contrataciones que llevan a cabo otros sectores que cuentan con legislación, jurisprudencia, costumbre y doctrina en grado suficiente como para integrar los casos no previstos e interpretar las cláusulas equívocas.

Tan importantes y especiales son los contratos informáticos que las grandes empresas norteamericanas en su calidad de proveedoras o usuarias suelen tener un área específica integrada por equipos interdisciplinarios de informáticos, contadores y abogados para la redacción y negociación de dichos contratos; sin embargo, en nuestro país aún no se les ha atribuido la debida importancia.

La existencia de sistemas destinados al tratamiento automatizado de la información es el hecho técnico que da fundamento a los llamados “contratos informáticos”, ya que se trata del concepto principal que permite predicar la unidad de la nueva rama frente a la multiplicidad aparente de los fenómenos jurídicos que la integran.

La practica comercial de contratar por separado las prestaciones informáticas no debe hacer perder de vista el enfoque esencial que permite contemplar en su verdadera dimensión a los contratos de bienes y servicios informáticos consistente en tener siempre presente que el objetivo de estos, son los sistemas informáticos, subsistemas o elementos de interacción entre sí o con el medio ambiente.

Cuando se contratan por ejemplo bienes informáticos, sea en conjunto o por separado, debe ser explicito en cuanto a la interacción anteriormente mencionada, de tal manera que cumplan con la función instrumental para la que fueron diseñados de acuerdo con sus respectivas especificaciones técnicas en el contexto de la finalidad concreta a la cual se destinaran en el sistema informático al que serán integrados como partes componentes.

Por eso cabe afirmar que en la experiencia jurídica, además de la tipicidad legal de algunos contratos como la compraventa, existe también la tipicidad consuetudinaria de los contratos de equipos, soporte lógico, desarrollo de sistemas, y demás; ya que se plantea una serie de problemas recurrentes que exigen soluciones repetitivas y adecuadas, es decir, “típicas”, que solo adquieren pleno sentido cuando se les contempla bajo la perspectiva del sistema informático.

A fin de evitar sorpresas desagradables, los contratos informáticos deben contener en forma explicita y precisa, elementos generales tales como el objeto (creación y transmisión de derechos y obligaciones respecto de los bienes y servicios informáticos), duración, rescisión, precio, facturación y pago, garantías y responsabilidades y disposiciones generales.

Las garantías (obligación inherente a una persona de asegurar a otra el goce de una cosa o derecho, de protegerla contra un daño o de indemnización en casa de determinados supuestos). Estas cláusulas señalan la manifestación de compromiso fundamentalmente de los proveedores aunque en nuestro ámbito contractual en la mayoría de las ocasiones se trata de cláusulas limitativas de responsabilidad que constituyen verdaderos contratos de adhesión.

Normalmente las garantías tienen su origen en el contrato, pero en caso de no estar estipuladas, se encuentran previstas por la ley bajo un carácter supletorio o imperativo, con la posibilidad por parte de los contratantes de ampliarlas, limitarlas o suprimirlas.

Las garantías mas importantes en los contratos informáticos son las de conformidad por las cuales el proveedor se compromete a entregar al usuario aquello previsto en el contrato conforme a lo pactado por las partes; la de buen funcionamiento, por la cual el proveedor se constriñe a mantener funcionando el equipo en forma adecuada durante un cierto tiempo, luego el cual puede celebrarse un contrato de mantenimiento; la garantía contra vicios, la cual obliga al proveedor a una acción de saneamiento en caso de aparición de vicios ocultos y finalmente la garantía de evicción, referida a la obligación del proveedor a responder contra la reivindicación por parte de terceros respecto a la propiedad industrial o intelectual de los materiales y/o programas provistos al usuario.

Por otra parte las responsabilidades que son las que determinan el accionar de las garantías, como es el caso de la obligación de reparar el daño causado al contratante pro la falta de ejecución del compromiso adquirido en los contratos informáticos; las responsabilidades mas importantes son las referidas a la seguridad material del equipo y aquello concerniente a los daños causados por el material o el personal del proveedor. Lo anterior no exime a los contratantes de convenir otras cosas a manera de disposiciones generales.

El ambiente informático en muchas ocasiones se convierte en fuente de ambigüedades en cuanto que su léxico esta integrado por

numerosos vocablos de orden técnico, a los que comerciantes, juristas y aun los mismos “expertos” en informática llegan a atribuir contenidos diferentes, lo cual puede traer como consecuencia que los derechos y obligaciones contractuales lleguen a ser diversos de aquellos que las partes pensaron haber suscrito.

El usuario debe ejercer un estricto control y supervisión en el funcionamiento del equipo informático que adquiera, siendo conveniente un asesoramiento externo por parte de un experto en la materia para que vigile el buen desarrollo de dichas actividades.

Por otra parte, es importante que el usuario dé un buen mantenimiento a su equipo, y si en este proceso intervienen funcionarios del proveedor deberá tener un control discreto sobre ellos a efecto de prevenir una eventual actitud dolosa que pudiera suscitarse, como por ejemplo que los empleados del proveedor pretexten mal funcionamiento del equipo y pretendan hacer creer al usuario una “necesaria” reparación y su consiguiente aumento en el cobro de honorarios o llegando aun al extremo de “robar” los programas creados por el usuario.

Los contratos de asistencia técnica al usuario de sistemas informáticos son específicos, sin embargo, en algunos contratos informáticos ya se prevé una cláusula especial sobre dicha asistencia técnica, la cual debe ser periódica y oportuna.

Este servicio lo puede ofrecer el proveedor o bien una empresa que se encargue de ello, quedando al usuario la elección según las circunstancias. En este sentido, la formación se refiere a la capacitación que el proveedor dé al personal de la empresa del

usuario, especialmente a quienes se vayan a encargar de manejar el sistema.

Es indudable que el éxito que pueda tener la informatización de una empresa radica fundamentalmente en que tenga un buen equipo, eficientes programas de cómputo y personal debidamente capacitado.

Esto consiste en el carácter confidencial que el proveedor debe dar a la información de su cliente; si por el contrario, realiza o permite su divulgación a un tercero, eventualmente o no competidor, el usuario estará en todo su derecho de demandarlo por la vía civil o aún por abuso de confianza. Es esencial que en una empresa informática se sigan estos principios de secrecía y confidencialidad para su buen funcionamiento, seguridad y reputación.

Son Cláusulas que se refieren a un concepto en especial y que las partes convienen en insertarlas en los contratos informáticos. Por citar alunas tenemos: la cláusula de no solicitud de personal, en la que el cliente se compromete a no contratar al personal del proveedor para que trabaje con él. Esta cláusula se interpreta como una obligación de no hacer.

Existe otra cláusula que se refiere a la restricción de acceso al equipo y que se utiliza frecuentemente en los contractos de mantenimiento para liberar al proveedor de toda garantía en caso de intervención del usuario o de una tercera persona sobre el equipo informático. Esta cláusula es limitativa de responsabilidad.

Las partes que conforman la relación contractual de índole informática como lo son los proveedores; que son los fabricantes,

distribuidores y vendedores de bienes informáticos y son aquellos obligados a salvaguardar los intereses del cliente y darle consejo e información, cumplir con la entrega de los bienes o con la prestación de sus servicios en los plazos estipulados, realizar la prestación conforme a las especificaciones del contrato, garantizar los vicios ocultos que pudiera llegar a tener la prestación realizada, y el estudio de viabilidad para el usuario, actuando en todo momento con probidad y honestidad, así como con una asesoría y apoyo adecuados.

Los usuarios son aquellas entidades (públicas o privadas) o individuos que requieren satisfacer determinadas necesidades a través de los bienes informáticos, y entre sus principales obligaciones están; informarse, documentarse, visitar exposiciones y demostraciones de equipo de servicios informáticos en general, solicitar folletos explicativos sobre las características y funcionamiento de los centros de cómputo, así como de los programas ya existentes, determinar de manera precisa sus necesidades de automatización fijando y comunicando sus objetivos precisos, suministrar al proveedor de informaciones exactas de su empresa, acompañadas de documentos, graficas, proyectos y demás; capacitar adecuadamente a su personal para el manejo del centro de cómputo (funcionamiento, seguridad, programación), obtener una mejor adaptación de su empresa a los imperativos de funcionamiento del material instalado, realizar la elección final de entre las ofertas que le presenten los proveedores, considerando los elementos de apreciación de orden financiero y técnico, aceptar y recibir el material o los servicios que ha solicitado, acordar un periodo de prueba a efecto de verificar el funcionamiento del equipo, respetar las directrices propuestas y formuladas por el proveedor sobre el modo

de empleo del material o de los programas, pagar el precio convenido según las modalidades fijadas entre las partes.

Los principales contratos informáticos asimilables dentro de las categorías jurídico-contractuales son: la compraventa, arrendamiento, arrendamiento con opción a compra de bienes informáticos, así como la prestación de servicios informáticos.

Compraventa

Se refiere a los equipos y suministros (componentes, accesorios, etc.) Su esencia es similar a la de cualquier contrato de compraventa referido a otros bienes, sin embargo, reviste una serie de elementos peculiares que los tornan aún más más complejos.

En este contrato informático se debe establecer en primer término que el proveedor venderá al usuario el material de acuerdo con los planes de contratación ofrecidos, debiendo incluirse una relación de las maquinas que integren el centro de computo materia de la compraventa, indicando asimismo, el modelo, descripción, cantidad, precio de compra y cargo mensual de mantenimiento.

Se deberá asentar en el contrato la fecha de entrega del equipo de cómputo, así como el sitio y las condiciones. Los pagos deberán hacerse de conformidad con el plan de contratación específico establecido en el contrato y ningún cargo comenzara a “surtir efecto” hasta que haya sido aceptado el sistema de cómputo y demás productos amparados por el contrato.

Es importante que se establezca en el contrato el momento en que el usuario adquiere la propiedad; por otra parte podrá haber un periodo de prueba del equipo que comience desde la fecha de entrega del sistema y termine después de treinta días. Si después de sesenta días no se ha alcanzado un nivel de eficacia, el usuario podrá solicitar el reemplazo total del equipo o de la unidad que no funciona.

El proveedor deberá responder por los daños y perjuicios que le cause al usuario en caso de incumplimiento; asimismo, asumirá cualquier responsabilidad para el saneamiento en caso de evicción. Es por ello que deberá establecer el contrato informático que el proveedor garantizará que el equipo y sus dispositivos no tendrán algún efecto.

El proveedor deberá garantizar también el tiempo que se obligue a suministrar al usuario las partes y refacciones necesarias para mantener los equipos en las condiciones adecuadas de funcionamiento. Por otro lado, el proveedor proporcionará por escrito al usuario toda la información técnica necesaria para que éste haga el uso adecuado del equipo.

Durante el tiempo que dure el contrato y aún después, ambas partes deberán convenir en mantener con discreción cualquier información recibida de la otra parte que haya sido clasificada como confidencial. El proveedor será responsable de las violaciones que se causen en materia de patentes o derechos de autor respecto de los objetos materia del contrato proporcionados al usuario. A este respecto, debe comprometerse al pago de daños y perjuicios.

Las partes deben establecer el plazo durante el cual el usuario puede cancelar temporal o definitivamente el equipo solicitado mediante aviso por escrito. En caso de que el usuario, por así convenir a sus intereses, adquiera equipos de compañías extranjeras, teniendo la obligación de pagar el impuesto sobre la renta.

Este contrato constituye un acuerdo entre las partes y deja sin efecto cualquier negociación, obligación o comunicación ya sea oral o escrita, hecha con anterioridad a la firma del mismo.

Arrendamiento

Aplicándolo en materia informática, existen diversas cláusulas específicas para el arrendamiento de sistemas de cómputo, debiéndose en el contrato una relación de las maquinas y sistemas operativos indicando su modelo, descripción, cantidad, precio de compra, renta mensual y cargo mensual de mantenimiento.

Se deberá estipular la duración del contrato en los términos y condiciones acordados respecto los mecanismos de prorroga que se presenten, asimismo, se deberán definir claramente la fecha, el sitio y las condiciones de entrega del sistema de cómputo.

Una vez que las partes han fijado los precios que regirán las operaciones del contrato, se estipulará el compromiso de no alterar los precios pactados originalmente durante la vigencia del mismo; el pago del precio le da derecho al arrendatario de usar en forma ilimitada el sistema de cómputo con sus fases operativas y de programación. El usuario tiene derecho de solicitar que se estipule bien en el contrato que el equipo de cómputo se pruebe en las

instalaciones del proveedor de acuerdo con ciertos estándares establecidos, debiendo proporcionar el arrendador documentos, formularios y publicaciones referentes a ese equipo de cómputo.

El arrendatario podrá cancelar cualquier de equipo dando aviso al arrendador con treinta días de anticipación y podrá dar por terminado el contrato si el proveedor incurre en violación de cualquiera de las cláusulas del mismo.

Se deberá estipular en el contrato que el arrendador notificará al usuario con uno o dos años de anticipación según sea pactado, su retiro del mercado nacional y mientras esté en el mercado deberá comprometerse a prestar los servicios amparados por el contrato.

En el contrato informático de arrendamiento existen varias cláusulas similares a las que se pactan en un contrato de compraventa, entre ellas que el arrendador deberá mantener en forma confidencial toda documentación que le haya sido facilitada por el arrendatario a fin de realizar el estudio de viabilidad.

El proveedor y arrendador será responsable de las violaciones que se causen en materia de patentes o derechos de autor y se comprometerá a indemnizar por daños y perjuicios a un tercero afectado.

Por otro lado el arrendador deberá garantizar la que el equipo y sus dispositivos estarán libres de cualquier defecto de materiales o mano de obra y comprometerse a mantener el objeto materia del contrato en condiciones satisfactorias de operación ajustando, reparando o reemplazado las piezas o artículos defectuosos que

causen una operación anormal, así como hacerse cargo de la instalación del sistema de cómputo.

El proveedor también debe hacerse responsable de los empleados que envía a las instalaciones de usuario y asumir cualquier responsabilidad para el saneamiento en caso de evicción, así como indemnizar al usuario en caso de actuar dolosamente.

Arrendamiento con opción a compra.

Esta figura es una modalidad del contrato de arrendamiento muy empleado en materia informática y generalmente conocido bajo el nombre de leasing. Este contrato establece que la opción se compra se podrá ejercer en cualquier momento después de la fecha de aceptación del sistema de cómputo respecto a todo o parte del mismo, considerando los porcentajes pactados de las rentas pagadas que abonarán al precio de la compra.

Al ser la compra de equipo informático un gasto muy fuerte para las empresas, es frecuente que en un principio tomen en arrendamiento el centro de cómputo y lo paguen a plazos hasta adquirir la propiedad del mismo.

A este tipo de contrato informático se aplican las cláusulas del contrato de arrendamiento y las del contrato de compraventa en cuanto a la adquisición del equipo.

Prestación de Servicios

Este tipo de contrato se refiere a todos aquellos trabajo que sobre determinadas materias se realicen. El contrato que más se asemeja en nuestro derecho civil a este tipo de contrató informático es el de prestación de servicios profesionales, que se refiere a los servicios que presta el profesionista a una persona llamada cliente, quien se obliga a pagarle una determinada retribución llamada honorarios.

En esta figura se requiere que el prestador de servicios tenga una adecuada preparación técnica además de un título profesional, así como capacidad general para contratar. A este respecto, cabe mencionar que se entiende por ejercicio profesional “La actividad habitual de todo acto o la prestación de cualquier servicio propio de cada profesión”.

Algunas de las principales características de este contrato son: Bilaterales, onerosos, conmutativos y formales o consensúales según acuerden las partes. Los elementos reales son: el servicio profesional y los honorarios. En el mismo contrato de prestación de servicios informáticos hay una categoría que se refiere a la utilidad o provecho que se obtiene de la realización de acciones o actos de personas fisicas o morales que coadyuven de manera directa o indirecta al manejo de la información estando su aplicación relacionada con la estructuración y composición de datos.

Las partes en este contrato informático se denominan “proveedor” siendo aquel que presta el servicio de (prestador) y que la mayoría de las veces sin empresas de computación, así como el “cliente” o “usuario” (prestatario) siendo aquel que recibe el servicio y lo retribuye.

Entre dichos contratos de servicios informáticos podemos manifestar que existen el de explotación de programas, de consulta de archivos y banco de datos, en de estudio de mercados en informática, el de documentación técnica, el de mantenimiento correctivo y preventivo o de sistemas, el manejo de datos, el de desarrollo de estudios de viabilidad para la selección de bienes y servicios, el de consultoría, el de diseño de sistemas, asistencia técnica, formación, etc. La importancia que ha ido adquiriendo este tipo de contratos es el resultado de la necesidad cada vez mayor de asesoramiento y servicios informáticos varios que requieren los usuarios.

La problemática fundamental de este tipo de contratos, consiste en el desequilibrios notorio existente entre las partes en razón de que comúnmente el proveedor de bienes o servicios se vale de sus conocimientos técnicos sobre la materia y el correlativo desconocimiento por parte del usuario para imponer sus condiciones mediante una redacción contractual con términos pronunciadamente técnicos en detrimento de los elementos jurídicos los cuales, en la mayoría de las ocasiones, son aceptados por los usuarios en razón de sus necesidades informáticas y su falta de adecuada asesoría técnica, convirtiendo a estos en verdaderos contratos de adhesión.

Este tipo de contratos manifiestan una gran cantidad de lagunas jurídicas , las cuales, a su vez, son eventualmente fuente de controversias y conflictos en cuanto a la falta de precisión en caracteres tan importantes como las garantías, responsabilidades, reparación del sistema, pago de daños y perjuicios, etc.

De esta forma nos percatamos que los contratos informáticos ameritan un tratamiento pormenorizado, especialmente en cuanto a las diversas implicaciones hasta hoy desconocidas por el derecho tradicional a efecto de contemplar un régimen jurídico regulador efectivamente aplicable.

CAPITULO III.
FENOMENO INFORMATICO.

3.1 ORÍGENES DEL FENÓMENO INFORMÁTICO.

Antes de analizar a la informática propiamente dicha, es menester hacer unas breves alusiones al rubro general de donde desprende, es decir, la cibernética; un notable personaje matemático originario de Estados Unidos, Norbert Wiener, escribió un libro que intituló Cibernética, empleando este término para designar a la nueva ciencia de la comunicación y control entre el hombre y la máquina.

Su aparición obedeció princi0palmente a tres factores, a saber:

a) Un factor social, porque eran tiempos que requerían un aumento de la producción y, por consiguiente, en la capital. Eran tiempos duros, sin embargo, se necesitaba más que una emergencia racional para que se gestara una nueva ciencia. Es así como Stafford Beer en Cibernética y Administración señalo que el clima intelectual debe ser

tal que favorezca el surgimiento de una nueva disciplina.

b) El factor técnico-científico fue muy importante porque varias líneas de pensamiento originadas en muy diversas esferas de actividad, como lo fue la ciencia y la técnica, se empezaron a reunir, y lograron avances tales que hicieron menester una ciencia que facilitara su interrelación y desenvolvimiento.

c) Un tercer factor, el histórico, porque surge de la mencionada necesidad del nacimiento de una ciencia de unión que controlara y vinculara a todas las demás. Surge entonces la cibernética como una unidad multidisciplinaría. Para Wiener esto es lo que constituye el propósito de la cibernética: abarcar de manera total y multidisciplinaría a todas las ciencias.

Ya Engels en su Dialéctica de la naturaleza escribió que en los puntos de unión o contacto de las ciencias es donde se podían esperar los mejores resultados. El vislumbraba ese punto de unión interdisciplinario aunque solo hablara de las ciencias sin incluir a las técnicas.

3.2 NOCIONES Y CONCEPTO.

Si entendemos a la etimología de la palabra, el vocablo “cibernética” toma su origen de la voz griega kybernetes piloto, y kybernes, concepto referido al arte de gobernar. Esta palabra alude a la función del cerebro con respecto a las máquinas.

La cibernética es la ciencia de la comunicación y el control. Los aspectos aplicados de esta ciencia están relacionados con cualquier

campo de estudio. Sus aspectos formales estudian una teoría general del control, extractada de los campos de aplicación y adecuada para todos ellos.

3.3 CARACTERÍSTICAS Y ORIGEN DE LA INFORMÁTICA.

Una vez desentrañadas las generalidades básicas de la cibernética, procedamos a profundizar en algunas de ellas en torno a la informática.

Surge de la misma inquietud racional del hombre, el cual, ante la cada vez mas creciente necesidad de información para una adecuada toma de decisiones, es impulsado a formular nuevos postulados y a desarrollar nuevas técnicas que satisfagan dichos propósitos.

A lo largo de la historia, el mundo ha sufrido diversas revoluciones tecnológicas relacionadas con la información, que han repercutido en tal forma que han transformado y reorganizado la economía y la sociedad.

En la actualidad, como sostienen algunos autores, estamos sufriendo una nueva revolución tecnológica. La informática, junto con sus micros, minis y macrocomputadoras, los bancos de datos, las unidades de tratamiento y almacenamiento, la telemática, etcétera, están transformando de manera indudable nuestro mundo.

La palabra informática es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en el año de 1962.

En sentido general, la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones.

Mora y Molino la definen como el estudio que delimita las relaciones entre los medios (equipo), los daños y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado.

Mario G. Losano caracteriza a la informática como producto de la cibernética, en tanto un proceso científico relacionado con el tratamiento automatizado de la información en un plano interdisciplinario.

En este capitulo realizare un análisis hermenéutico de los conceptos Delitos Electrónicos y Delitos Informático, a fin de establecer su correcta interpretación legal, que, como es sabido, dista de lo común, en vista al inminente dictado de normas que penalizan estos actos en la mayoría de los países y, así evitar malas interpretaciones que puedan conducir a superposiciones de tipo penal, o bien a la producción de lagunas jurídicas que, a fin de cuentas, dañan a la sociedad, a quien el Derecho Penal intenta proteger.

La necesidad de análisis de los términos electrónica e informática.

Puede ser que quien no haga del Derecho Penal una práctica habitual y constante no encuentre alguna diferencia, o la necesidad de definir estos dos términos que hoy, en lenguaje común, y aun en el de algunos medios especializados, son considerados sinónimos.

Para la mejor comprensión de dichos términos, es necesaria la definición de los vocablos informático y electrónico.

Electrónica: “Ciencia que estudia dispositivos basados ene. Movimiento de electrones libres en el vació, gases o semiconductores, cuando dichos electrones están sometidos a la acción de campos electromagnéticos.

Informática - Computación: Conjunto de disciplinas y técnicas desarrolladas para el tratamiento automático de la información mediante maquinas computadoras (hardware) que funcionan con distintos programas (software).

Los delitos comprendidos y el amito de aplicación de cada uno.

Para construir las bases de un sólido andamiaje jurídico es menester en este momento describir el ámbito de aplicación de cada uno de los casos que se encuentran bajo análisis.

Tenemos así que los delitos cometidos en contra de equipos electrónicos son aquellos en los cuales el receptor físico del daño perpetrado resulta expresamente un equipo electrónico.

Muy torpe sería dentro de esta categoría pretender, incluir el delito específico de daños, reconocido en todas las legislaciones penales, por ejemplo en aquellos casos en que alguien destruye un cajero electrónico, salvo que este tuviere que ver con destrucciones totales o parciales producidas a través de la utilización de medios informáticos.

En contra posición observamos los delitos cometidos por medio de elementos informáticos, los cuales presentan una variada gama que pasa por los daños, las injurias y calumnias, las estafas (las realizadas en subastas on line encabezan todos los listados conocidos) y otros muchos.

De esta diferencia notoria podemos extraer una quizás más sutil pero mucho más científica, ¿cuál es el bien jurídico protegido en cada caso? En el primero se advierte que es la integridad física y lógica de los equipos electrónicos, y por ende el derecho de propiedad del sujeto pasivo; en el segundo, en cambio, advertimos que son múltiples las posibilidades de bienes jurídicos a proteger y altamente disímiles entre si como el honor, la protección de datos, el patrimonio, etc.

Determinado el bien jurídico protegido, podremos inducir que, en el caso de los delitos informáticos, los múltiples posibles, ya se encuentran en su mayoría protegidos por medio de figuras como el robo, la estafa, las injurias y calumnias, etc., contenidos en códigos penales o leyes especiales.

Algo que nos separa de una correcta aplicación de las leyes penales preestablecidas, es la pretendida falta de legislación en materia de delitos informáticos, y digo pretendida porque no es así, ya que al perpetrarse el delito a través de medios informáticos no se esta si no en presencia de un nuevo método comisivo del delito y no, como erróneamente se piensa, ante un nuevo delito, ya que para que lo sea debe estar correctamente tipificado.

En resumen, los delitos informáticos, en su gran mayoría, dependen para su persecución penal, de la correcta interpretación de la ley penal y de la toma de conciencia de los jueces de que solo encontramos ante nuevos métodos para estafar o para injuriar, pero en ningún caso ante nuevos delitos, ya que una postura semejante nos llevaría al absurdo de pensar, que por ejemplo, que si mañana se pudiese quitar la vida a alguien por medio de la Internet habría que establecer una nueva figura penal, ya que el homicidio estaría cubriendo esta posibilidad; cuando en derecho, si se lesiona el bien jurídico protegido, no importa cual sea el medio utilizado, corresponde la aplicación de la ley penal vigente y no se requiere una nueva y específica.

En este caso no me queda menos que analizar puntualmente el caso de que aquellos delitos que no se encuentran tipificados, ya que no corresponden a bienes jurídicos protegidos- al menos a primera vista- como el caso especifico del hacking u otros similares.

Pues bien, ahora nos encontramos dentro del ámbito especifico de los que dijimos son delitos electrónicos, por el tipo de bien afectado, y salvo algunos casos en que pueda entenderse validamente- sin violar la prohibición de analogía que pesa sobre la norma penal- que nos encontramos frente a un caso de delitos de daños, para el que, por regla general no existe legislación.

Para estos casos se requiere una rápida acción del legislador para definir los tipos penales y agregarlos a los vigentes. Sin perjuicio de que hacer las respectivas modificaciones y según la legislación de cada país, puedan agravarse algunos tipos existentes en función del

uso de nuevas tecnologías para, esta forma, desalentar su utilización indefinida.

3.4 DERECHO DE LA INFORMÁTICA.

Si bien es cierto que los precursores informáticos nunca imaginaron los alcances que llegarían a tener las computadoras en general o aun en campos tan aparentemente fuera de influencia como el jurídico, todavía más difícil hubiera sido concebir que el Derecho llegaría a regular a la informática.

A finales de los años sesenta y luego de cerca de diez años de aplicaciones comerciales de las computadoras, empezaron a surgir las primeras inquietudes respecto a las eventuales repercusiones negativas motivadas por el fenómeno informático, las cuales requerían de un tratamiento especial.

El Derecho de la Informática se define como el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática. Es decir, es un conjunto de leyes en cuanto que, si bien escasos, existen varios ordenamientos jurídicos nacionales e internacionales con alusión específica al fenómeno informático.

El concepto de normas se debe a aquellos lineamientos que integran la llamada política informática, la cual, según veremos posteriormente, presenta diferencias respecto a la legislación informática.

El termino principios es en función de aquellos postulados emitidos por jueces, magistrados, tratadistas y estudiosos del tema.

3.5 FUENTES DEL DERECHO INFORMÁTICO.

Para atribuir una eventual autonomía a esta disciplina jurídica es menester hacer alusión, entre otras cosas, a aquellas fuentes de donde emana propiamente este conjunto de conocimientos.

A nivel interdisciplinario, están aquellas provistas por el mismo Derecho, como es el caso de la legislación, que es relativamente incipiente al respecto, sin embargo, aquí cabría señalar aquellas disposiciones sobres otras áreas caracterizadas por guardar un nexo estrecho con respecto al fenómeno informático, como es el caso de los ordenamientos en materia constitucional, civil penal, laboral, fiscal, administrativa, procesal, internacional, entre otras.

Así mismo, en cuanto a la jurisprudencia, doctrina, y literatura sobre el tema, existen algunos pronunciamientos, teorías y artículos respecto a los problemas jurídicos suscitados por la informática.

Por otra parte, en cuanto a las fuentes transdisciplinarias existen aquellas provistas por ciertas y técnicas como la Filosofía, Sociología, Economía, Estadística, Comunicación y desde luego la Informática.

CAPÍTULO IV
DELITOS INFORMÁTICOS

4.1. GENERALIDADES DEL DELITO.

4.1.1. DEFINICIÓN DE "DELITO".

Para determinar la existencia de los delitos informáticos, es necesario en primer término definir qué se entiende por delito. De acuerdo a lo establecido por el autor Fernando Castellanos Tena en su obra "Lineamientos Elementales de Derecho Penal", la palabra delito "se deriva del verbo latino delinquere, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley"[5].

Los simpatizantes de la "Escuela Clásica" elaboraron diversas definiciones respecto al término delito. El principal exponente de esta corriente, Fernando Carrara, lo define como "la infracción de

[5] Castellanos. Tena, Fernando. Lineamientos Elementales del Derecho Penal (Parte General). Trigésima Cuarta Edición. Editorial Porrúa., México, D.F., 1994, p. 125.

la Ley del estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso"[6].

Para Carrara, el delito es un ente jurídico, en virtud de que su esencia deriva de una violación al Derecho. También lo considera como una infracción a la ley del Estado, toda vez que un acto se convierte en delito al transgredir dicha Ley, la cual ha sido promulgada para proteger la seguridad de los ciudadanos. Además, precisa que el delito es una infracción resultante de un acto externo, positivo o negativo del hombre; con lo cual se determina que solamente el hombre puede ser agente activo del delito, tanto en sus acciones como en sus omisiones. Y finalmente considera que dicho acto es moralmente imputable al hombre por estar el individuo sujeto a leyes criminales en virtud de su naturaleza moral.

Para la Escuela del Positivismo, cuyo principal exponente fue el jurista Rafael Garófalo; el delito es un fenómeno o hecho natural que se da como consecuencia necesaria de factores hereditarios, de causas físicas y de fenómenos sociológicos.

De acuerdo a la concepción sociológica de Rafael Garófalo, el delito natural es "la violación de los sentimientos altruistas de probidad y de piedad, en la medida media indispensable para la adaptación del individuo a la colectividad"[7].

---

[6] Idem.
[7] Ibidem p. 126.

Esta noción sociológica del delito no tiende a definir al delito como un hecho natural, ya que el delito como tal debe entenderse como un acto; en cierto sentido lo que buscaba dicha definición, era describir la esencia del delito como fruto de una valoración de ciertas conductas, según determinados criterios de utilidad social, de justicia, de altruismo, de orden, de disciplina, etc., que determinen aquéllas conductas que habrán de ser consideradas como delictuosas.

4.1.2. CONCEPTO JURÍDICO DE "DELITO".

La concepción jurídica del término delito es formulada desde el punto de vista del Derecho; y al respecto se han elaborado tanto definiciones de tipo formal como de carácter sustancial.

Por lo que hace a la noción formal del término delito, ésta es proveída por la ley positiva, al advertir la imposición de una pena o sanción por la ejecución u omisión de ciertos actos. De ahí que no sea posible hablar de delito, sin la existencia de una ley que sancione una determinada conducta.

Para Edmundo Mezger, el delito es en su acepción jurídica "una acción punible; esto es, el conjunto de los presupuestos de la pena"[8]. Lo que Mezger quería significar al referirse al delito como una acción punible, era que por delito debía entenderse toda acción que estuviera sancionada con una pena.

En México, el ordenamiento jurídico que define al delito es el Código Penal Federal; el cual dispone en su artículo 7°, primer

párrafo, que “delito es el acto u omisión que sancionan las leyes penales”. De tal modo, que de esta definición se advierte, que nada puede ser castigado sino por hechos que la ley ha definido previamente como delitos; ni tampoco podrá ser sancionado con otras penas que las establecidas en la propia ley. De igual forma se entiende, que la consumación de un delito se obtiene por el simple hecho de infringir la ley, independientemente del resultado que se dé a consecuencia de ello. En el momento preciso en que se vulnera la ley, se provoca el delito.

El Código Penal para el Estado de Veracruz, define en su articulo 18 lo que debe concebirse como “delito”, “El delito es la acción u omisión que sancionan las leyes penales”.

Por lo que respecta a la noción jurídica - sustancial del término delito, existen dos sistemas encargados del estudio jurídico - esencial del delito: el sistema unitario o totalizador, y el sistema analítico o atomizador.

El primer sistema establece que el delito no puede dividirse, por ser parte integrante de un todo orgánico, se trata pues, de un concepto indisoluble. Para los seguidores de esta doctrina, el delito se presenta como un bloque monolítico, que no es fraccionable de modo alguno.

En cambio, los afiliados al sistema analítico o atomizador; estudian el ilícito penal por sus elementos constitutivos. Ellos consideran que para entender el todo, se precisa del conocimiento

---

[8] Ibidem. p. 128.

cabal de cada una de sus partes integrantes; sin embargo aceptan que el delito integra necesariamente una unidad.

En base a estos dos sistemas, Mezger elabora una definición jurídica - sustancial del término delito, en la cual expresa que "el delito es la acción típicamente antijurídica y culpable"[9].

En el mismo sentido, Cuello Calón, concibe al delito como "la acción humana antijurídica, típica, culpable y punible"[10].

Por su parte, Jiménez de Asúa, considera que el "delito es el acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal"[11].

La definición jurídico - sustancial de delito formulada por Jiménez de Asúa, integra como elementos del delito: la acción, la tipicidad, la antijuridicidad, la imputabilidad, la culpabilidad, la punibilidad y las condiciones objetivas de punibilidad; elementos que serán descritos a continuación.

4.1.3. ELEMENTOS POSITIVOS Y NEGATIVOS DEL DELITO.

Los elementos del delito son estudiados desde dos perspectivas o puntos de vista, de acuerdo al sistema propuesto por Guillermo Sauer y retomado a su vez por Jiménez de Asúa.

---

[9] Ibidem p. 129.
[10] Idem.
[11] Ibidem p.130

De acuerdo a dicho método se contrapone lo que el delito es, a lo que no es; así se tiene que los elementos integrantes del delito son en su:

ASPECTO POSITIVO	ASPECTO NEGATIVO
Conducta.	Ausencia de Conducta.
Tipicidad.	Ausencia de tipo o Atipicidad.
Antijuridicidad.	Causas de justificación.
Imputabilidad.	Causas de inimputabilidad.
Culpabilidad.	Causas de inculpabilidad.
Punibilidad.	Excusas absolutorias.

El primer elemento objetivo del delito en su aspecto positivo lo es la Conducta. En sentido amplio, el delito es ante todo una conducta humana, en la cual se incluye tanto el hacer positivo “acción”, como el negativo “omisión”.

Ahora bien, se advierte que en este primer elemento objetivo del delito puede presentarse en forma de acción, omisión o comisión por omisión. Mientras que la acción se manifiesta a través de la ejecución de una actividad voluntaria, la omisión y la comisión por omisión se conforman por una inactividad. El aspecto que diferencia a la omisión y a la comisión por omisión es, que en la omisión hay violación de un deber jurídico de obrar, en tanto que en la comisión por omisión hay violación de dos deberes jurídicos, uno de obrar y otro de abstenerse.

En sentido estricto, la acción “es todo hecho humano voluntario, todo movimiento voluntario del organismo humano capaz de modificar el mundo exterior o de poner en peligro dicha modificación”[12].

En cambio, la omisión, radica en una abstención de obrar; es “dejar de hacer lo que se debe de ejecutar”[13]. Por lo tanto, se considera que la omisión es una forma negativa de la acción; ya que en los delitos de acción el sujeto activo ejecuta un acto prohibido por la ley, en tanto que en los delitos de omisión, éste deja de hacer lo estipulado expresamente por la misma.

Por lo que hace a la ausencia de acción, como aspecto negativo del primer elemento objetivo del delito; se afirma que si falta alguno de los elementos esenciales del delito, éste no puede integrarse; en consecuencia, si hay ausencia de conducta, no se produce el delito.

El segundo elemento objetivo del delito en su aspecto positivo lo es, la tipicidad, entendiéndose por ésta “el encuadramiento de una conducta con la descripción hecha en la ley”[14]. Es en pocas palabras, la adecuación de la conducta al tipo penal descrito por la ley.

En tal sentido, se considera que no existe delito sin tipicidad. Cuando no se integran todos los elementos descritos en el tipo penal, se da el aspecto negativo de la tipicidad, que es la ausencia de adecuación de la conducta al tipo o también llamada “atipicidad”. Si la conducta no se amolda al tipo descrito por la ley, no puede ser considerada un delito.

---

[12] Ibidem. p. 152.
[13] Ibidem p. 152, 153.
[14] Ibidem p. 168.

En cuanto a la antijuridicidad como tercer elemento objetivo del delito, se dice que éste es un concepto negativo. La antijuridicidad radica en "la violación del valor o bien protegido a que se contrae el tipo penal respectivo"[15]. En otras palabras, una conducta es antijurídica, cuando transgrede una norma jurídica establecida por el Estado, causando en ese acto un daño o perjuicio social producto de dicha rebeldía.

La ausencia de antijuridicidad como factor negativo del elemento del delito en cuestión, lo constituyen las causas de justificación. Puede ocurrir que la conducta típica esté aparentemente en oposición al Derecho, sin embargo, no será antijurídica si existe una causa de justificación. Las causas de justificación, son aquellas condiciones que tienden a excluir la antijuridicidad de una conducta establecida en el tipo penal; de tal modo, que en tales condiciones, la acción realizada no será considerada antijurídica, en virtud de existir una justificante que hace que dicha conducta resulte apegada a Derecho. Las causas de justificación previstas por la ley son: la legítima defensa, el estado de necesidad, cumplimiento de un deber, ejercicio de un derecho, obediencia jerárquica e impedimento legítimo.

La imputabilidad es el cuarto elemento objetivo del delito, y se define como "la capacidad de entender y de querer en el campo del Derecho Penal"[16]. Se puede considerar entonces que un sujeto será imputable, si reúne todas aquellas condiciones psíquicas exigidas por la ley al momento de realizar el acto típico penal, las cuales lo capacitan por tanto para responder del mismo. Se afirma que la

[15] Ibidem p. 178.
[16] Ibidem p. 218.

imputabilidad está determinada por dos aspectos de tipo psicológico: un mínimo físico representado por la edad del sujeto (desarrollo mental), y otro de carácter psíquico consistente en la salud mental.

La inimputabilidad constituye el aspecto negativo de la imputabilidad. Son causas de inimputabilidad, todas aquéllas capaces de anular o inhabilitar el desarrollo o salud mental del sujeto, en cuyo caso, éste carecerá de aptitud psicológica para ser sujeto del delito. En el Código Penal Federal son consideradas causas de inimputabilidad: la minoría de edad, el trastorno mental, el desarrollo intelectual retardado, el miedo grave y el temor fundado. De esta forma, los protegidos por las eximentes de inimputabilidad deben quedar al margen de toda consecuencia represiva o asegurativa, en virtud de haber realizado el hecho penalmente tipificado sin capacidad de juicio y decisión.

La culpabilidad es otro de los elementos objetivos del delito, y se considera como la capacidad que tiene el sujeto para entender y querer en el campo del Derecho Penal; por lo tanto, se afirma que la imputabilidad funciona como presupuesto de la culpabilidad. Un sujeto será culpable, siempre y cuando se dé el nexo intelectual y emocional que ligue al sujeto con el acto que perpetró, de tal manera que dicho acto pueda serle reprochado jurídicamente. La culpabilidad reviste tres formas: el dolo, la culpa y la preterintencionalidad.

El factor negativo de la culpabilidad lo constituye la inculpabilidad. La inculpabilidad se da ante la ausencia del conocimiento y de la voluntad, que conforman los elementos esenciales de la culpabilidad; por lo tanto, toda causa eliminatoria de alguno de estos dos aspectos, es considerada como causa de

inculpabilidad. Para muchos autores las causas de inculpabilidad son el error y la no exigibilidad de otra conducta; o dicho en otras palabras, el error esencial de hecho (que ataca el elemento intelectual) y la coacción sobre la voluntad (que afecta al elemento volitivo).

Por lo que respecta a la punibilidad como sexto elemento objetivo de delito, se dice que ésta consiste en la imposición de una pena en función de la realización del acto penalmente tipificado y sancionado por la ley. Es punible una conducta, cuando por su propia naturaleza amerita ser sancionada.

Cuando hay ausencia de punibilidad se dice que se está en presencia de las excusas absolutorias, las cuales como se pude apreciar, constituyen el factor negativo de la punibilidad. Al concurrir en el acto alguna excusa absolutoria, no es posible determinar la aplicación de una pena.

El autor Fernando Castellanos Tena, hace mención en su obra “Lineamientos Elementales de Derecho Penal2, de las que a su juicio son consideradas como las principales excusas absolutorias y menciona como tales las siguientes: excusa en razón del arrepentimiento y mínima temibilidad del agente, excusa en razón de la maternidad consciente (en el caso de un aborto causado sólo por imprudencia de la mujer, o cuando el embarazo sea resultado de una violación), excusa por inexigibilidad de la conducta (como en el caso del encubrimiento de parientes y allegados, o de la falsa declaración de un encausado), excusa por graves consecuencias sufridas por el sujeto activo, en su persona, de tal manera que se hace notoriamente innecesario e irracional la imposición de una pena.

4.2. ASPECTOS GENERALES DE LOS DELITOS INFORMÁTICOS.

4.2.1. ORIGEN DE LOS DELITOS INFORMÁTICOS.

Como ya se ha mencionado, la informática ha irrumpido en el mundo y ha ido penetrando en cada uno de los aspectos de la vida cotidiana, brindando múltiples beneficios a la sociedad; sin embargo, de la misma manera en como representa una herramienta muy favorable, también se ha convertido en un instrumento para la comisión de verdaderos actos ilícitos.

Este tipo de actitudes ilícitas encuentra sus orígenes en el propio surgimiento de la tecnología informática, ya que es imposible concebir al delito informático, sin la existencia de las computadoras.

Es así como en las últimas cuatro décadas, aparece un nuevo tipo de acto delincuencial, cuyo sujeto activo no usa herramientas típicas para cometerlo; sino que ahora maneja y tergiversa la información, valiéndose de los medios electrónicos a su alcance y en la más completa libertad, de ahí su peligrosidad.

La misma facilitación de actividades que trae aparejado consigo el uso de los medios informáticos, ha suscitado que el usuario de los mismos se encuentre en un momento dado en un estado de ocio, el cual canaliza a través de las computadoras, cometiendo en muchas ocasiones, una serie de ilícitos.

El delito informático o electrónico aumentó su número de acciones delictivas en un término muy corto. La popularidad que últimamente han tenido las computadoras personales, ha provocado

un mayor número de usuarios y con ello, el potencial delictivo ha ido en aumento.

Hay una infinidad de ilícitos que se producen a trepes de las computadoras, y los delincuentes electrónicos proliferan día a día; es por tal motivo que se hace cada vez más necesaria, la existencia de una reglamentación jurídica adecuada a los nuevos tiempos, que trate de evitar en lo posible, la comisión del delito electrónico informático y sus efectos.

4.2.2. CONCEPTO DE LOS DELITOS INFORMÁTICOS.

Establecer un concepto sobre “delitos informáticos” es una labor difícil, en virtud de que para hablar del término “delitos informáticos”, se requiere que éstos estén contemplados en los textos jurídicos - penales de los países.

En México, tanto en el Código Penal Federal como en el Código Penal Veracruzano, se establece lo siguiente:

- CODIGO PENAL FEDERAL

Titulo Noveno

Revelación de secretos y acceso ilícito a sistemas y equipos de informática.

Capitulo II

Acceso ilícito a sistemas y equipos de informática.

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y deciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de Informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

- CODIGO PENAL VERACRUZANO

Capítulo III

Delitos Informáticos

Artículo 181.-Comete delito informático quien, sin derecho y con perjuicio de tercero:
I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; o
II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red.
Al responsable de este delito se le impondrán de seis meses a dos años de prisión y multa hasta de trescientos días de salario. Si se cometiere con fines de lucro las penas se incrementarán en una mitad.

Algunos tratadistas penales que han incursionado en el tema, se han dado a la tarea de conceptualizar el término “delitos informáticos o electrónicos”.

Al respecto la Dra. Luz Ma. Del Pozo y Contreras considera que “delito electrónico es aquél que se comete con el uso de las

computadoras o cualquier otro medio electrónico como pueden ser las telecomunicaciones"[17].

El autor Julio Téllez Valdés elabora un concepto típico y uno atípico para definir el término "delitos informáticos". De esta manera establece que "los delitos informáticos son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)"[18].

En el mismo sentido, María de la Luz Lima define el delito por computadora como "cualquier acto ilícito penal en el que las computadoras, su técnica y funciones desempeñan un papel ya sea como método, medio o fin"[19].

El autor español Romeo Casabona se refiere a la definición propuesta por el Departamento de Justicia Norteamericana, según la cual, "delito informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución"[20].

Para el autor Davara Rodríguez, resulta inadecuado hablar de "delito informático", ya que considera que como tal éste no existe, si se atiende a la necesidad de una tipificación en la legislación penal para que pueda existir un delito; y en virtud de que el Código Penal

---

[17] http://www.cddhcu.gob.mx/camdip/foro/, "Foro de Consulta Sobre Derecho e Informática (Memorias)", ponencia: "Mecanismos Existente con Ausencia de Estructuras, el Derecho Informático, el Delito Electrónico", Autor: Dra. Luz Maria del Pozo y Contreras, Poder Legislativo Federal, Biblioteca del H. Congreso de la Unión, Guadalajara, Jalisco., Septiembre 1996. (Consultada el 29/XII/08).
[18] Téllez. Valdés, Julio. Obra citada, P. 104.
[19] Ríos. Estavillo, Juan José. "Derecho a la Información en México", Ed. Porrua, México. 2000 P. 116.

Español no introduce el delito informático, resulta inapropiado referirse a dicho término.

Sin embargo, admite la expresión por conveniencia y define como delito informático "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"[21].

Parker conceptualiza a los delitos informáticos como "todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la victima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría de obtener un beneficio"[22].

La definición que presenta la Organización para la Cooperación Económica y el Desarrollo señala que "cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. También comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras o los datos contenidos en la misma, en la base, sistema o red"[23].

---

[20] http://www.jose_cuervo.lettera.net , Pagina de José Cuervo Álvarez, "Delitos Informáticos Protección Penal de la Intimidad", España, 29 de mayo de 1997. (Consultada el 29/XII/08).
[21] Pagina de Internet citada.
[22] Pagina de Internet citada.
[23] Ríos. Estavillo, Juan José. Ob cit No.19 p. 116.

Y finalmente, para el autor Ruiz Vadillo, que recoge la definición aportada por la Organización para la Cooperación Económica y el Desarrollo, "delito informático, es todo comportamiento ilegal o contrario a la ética o no autorizado, que concierne a un tratamiento automático de datos y/o transmisión de datos"[24].

En virtud de lo anteriormente descrito, se puede concluir estableciendo que por "delito informático" se debe entender, toda conducta no ética, típica, antijurídica, culpable y punible cometida a través de cualquier sistema informático y/o telemático, ya sea que éste sea empleado como medio o como fin para llevar a cabo el delito.

4.2.3. CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS.

Desde un punto de vista general, se han determinado ciertas características fundamentales de los delitos informáticos, entre las cuales se mencionan las siguientes:

Son conductas criminógenos de cuello blanco, en virtud de que sólo un determinado número de personas con los conocimientos suficientes en el ámbito de la informática puede llegar a cometerlos; sin embargo en la actualidad, el número de delincuentes informáticos se ha incrementado, debido a que los medios para cometer un delito de esta naturaleza están al alcance de casi todos los individuos.

[24] http://www.jose_cuervo.lettera.net (Consultada el 29/XII/08).

Son acciones que en múltiples ocasiones se llevan a cabo durante el desarrollo de las actividades profesionales del individuo, es decir, cuando el sujeto se encuentra laborando.

Son acciones que se llevan a cabo aprovechando una ocasión, en a mayoría de las veces, creada por el propio sujeto, por lo que se les llama acciones de oportunidad.

Son de consumación casi instantánea ya que en milésimas de segundo y sin requerir necesariamente de una presencia física, pueden llegar a realizarse.

Provocan grandes daños y pérdidas económicas a sus víctimas.

Los casos de delitos informáticos son cada vez más, y las denuncias contra éstos son muy pocas, lo cual, ante la ausencia de disposiciones reguladoras al respecto, contribuye a que la delincuencia informática siga proliferando.

Debido a su carácter técnico, son muy difíciles de comprobar; por lo que procuran a sus autores una probabilidad bastante alta d alcanzar sus objetivos sin ser descubiertos.

Por estar los sistemas informáticos al alcance de todos los individuos; ofrecen grandes facilidades para su comisión, incluso a menores de edad.

Carecen de regulación jurídica en las Legislaciones Penales del país, por lo que siguen considerándose como ilícitos impunes en México.

Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

De lo anterior, se advierte a peculiaridad que guardan los delitos informáticos frente a otro tipo de conductas criminales, lo que los distingue como una nueva modalidad de ilícitos cometidos a través de los medios informáticos.

4.2.4. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

Para algunos autores, los delitos informáticos se pueden clasificar, atendiendo al provecho que producen para el autor del delito y el daño que provocan en los sistemas informáticos como entes físicos; o bien, en atención al agravio que le ocasionan a un individuo o grupos de individuos, en su integridad física.

Para otros, la clasificación de los delitos informáticos se realiza de acuerdo a los fines que se persiguen al cometer las conductas delictivas en los sistemas informáticos, desde esta perspectiva dichos delitos se clasifican atendiendo a dos puntos de vista:

Delitos con medios informáticos, que son aquéllos en los cuales la computadora o sistemas informáticos son empleados como herramientas o medios de comisión de delito.

Delitos contra medios informáticos: que son aquellos en los cuales se provoca una lesión en el contenido de la información de un sistema, causando un perjuicio o afectación a los datos procesados o almacenados, o bien, a los propios programas del sistema.

Por su parte, el autor Juan Diego Castro Fernández establece que hay ciertos delitos informáticos que se adecuan a figuras tipificadas en el Código Penal, y en atención a los bienes jurídicamente afectados, realiza la siguiente clasificación de los delitos informáticos:

Delitos contra las personas: Lo cual se puede dar desde el punto de vista de que la medicina moderna ya cuenta con sistemas informáticos como medios para diagnóstico clínico, por lo que es posible que se pueda dar un uso indebido e la computadora, por dolo o culpa del médico, ocasionando con ello un agravio en contra del paciente.

Delitos contra el honor: Esto puede suceder en el caso de que se incluya información falsa de carácter injurioso en un archivo electrónico de un determinado individuo, lo cual al momento de darse a conocer cause un perjuicio al honor de la persona; o bien, que se conserve información falsa de alguna persona en registros electrónicos.

Delitos contra la propiedad: La mayoría de los delitos informáticos encuadran dentro de esta subclasificación, en virtud de que en múltiples ocasiones el móvil de éste tipo de delitos es afectar un bien propiedad de alguien. En este sentido, los principales delitos contra la propiedad, según lo establecido por el autor Castro Fernández son los siguientes:

Manipulación (Fraude Informático): Existe manipulación en el programa o consola, lo cual puede afectar tanto a la fase de

suministro o alimentación de datos, como a su salida o procesamiento.

Espionaje: Mediante esta actividad se obtienen datos o programas sin autorización de su propietario o titular, o bien, se divulgan aquéllos que han sido obtenidos legítimamente.
Sabotaje: Este tipo de conductas se propone la destrucción o incapacidad de los sistemas informáticos o de algún elemento que las estructura (hardware o software).

Hurto de tiempo: Es la utilización indebida de los sistemas informáticos por parte de los empleados o extraños, cuestión que puede provocar pérdidas considerables, especialmente en los sistemas de procesamiento de datos a distancia, en los cuales se emplean accesos con números de cuenta ajenos.

Para Julio Téllez Valdés, los delitos informáticos deben clasificarse en atención a dos criterios: como instrumentos o medio, o como fin u objetivo. De tal forma entre las principales conductas criminógenas que emplean a as computadoras como medio para la comisión del delito, se encuentran:

- Falsificación de documentos a través de los sistemas informáticos (tarjetas de crédito, cheques, etc.).
- Variación de los activos y pasivos de la contabilidad de las empresas.
- Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etc.).
- Robo de tiempo de computadora.

- Lectura, sustracción o copiado de información confidencial de la base de datos.
- Modificación de datos (en su entrada o salida).
- Aprovechamiento indebido o violación de un código para introducirse a un sistema con el fin de infiltrar instrucciones inapropiadas (esto es lo que se conoce con el nombre de Caballo de Troya).
- Variación en cuanto al destino de cantidades de dinero hacia cuentas bancarias apócrifas, método comúnmente conocido como “Técnica del Salami”.
- Uso no autorizado de programas de acceso universal (Superzzaping o Llave Maestra).
- Puertas con trampa, es decir, utilización de interrupciones en la lógica de un programa en la fase de desarrollo para su depuración y uso posterior de éstas con fines lucrativos.
- Alteración del funcionamiento de los sistemas informáticos a través de los “virus informáticos”.
- Obtención de información residual, obtenida a través de la impresión de trabajos o de la captura en cinta magnética en memoria después de la ejecución de un trabajo.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención de las líneas de comunicación para acceder o manipular los datos que son transmitidos.

Dentro de las conductas criminógenas que van dirigidas en contra de los sistemas informáticos como entidad física (clasificación de los delitos informáticos como fin u objetivo) se encuentran los siguientes:

- Programación de instrucciones que tienen como fin bloquear en forma total el sistema.
- Destrucción de programas.
- Daño a la memoria de los sistemas informáticos.
- Daños o atentados físicos contra la computadora y sus accesorios.
- Sabotaje político o terrorismo, en los cuales se destruye o haya un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos que contengan información valiosa con fines de chantaje (pago de rescate, etc.).

Para otros, a pesar de que el término delito informático engloba tanto a los delitos cometidos en contra de los sistemas informáticos, como a los cometidos mediante su uso, proponen realizar la siguiente clasificación:

Delitos e infracciones tradicionalmente denominados informáticos: Dentro de los cuales se pueden destacar:

- El acceso no autorizado a sistemas informáticos, mediante el uso ilegítimo de passwords.
- Destrucción de datos (a través de los llamados “virus informáticos”, bombas lógicas y demás actos de sabotaje informáticos).
- Infracción de los derechos de autor.
- Infracción del copyright de bases de datos.
- Interceptación de e-mail (violación de la correspondencia).

- Estafas electrónicas (a través de la proliferación de compraventas telemáticas).
- Transferencia de fondos.

En un segundo término, clasifican a los delitos informáticos en “delitos convencionales”, es decir, aquéllos que están plenamente tipificados por las legislaciones penales de los países, y en los cuales no se requiere el empleo de medios informáticos para su comisión, y son los siguientes:

- Espionaje (se han dado casos de acceso no autorizados a sistemas informáticos gubernamentales, así como interceptación del correo electrónico del servicio secreto).
- Espionaje Industrial (la existencia de hosts, que permiten guardar la identidad de los remitentes, ha sido aprovechada en muchas ocasiones por terroristas, para remitirse consignas y planear su actuación a nivel internacional.
- Narcotráfico: Es común el envío de mensajes encriptados entre narcotraficantes, para ponerse de acuerdo con los cárteles, por lo que el FBI y el Fiscal General de los Estados Unidos, han alertado sobre la necesidad de establecer medidas que permitan interceptar y descifrar dichos mensajes.

Y en una tercera clasificación establecen los malos usos o también llamados cybertorts, entre los cuales se encuentran los siguientes:

- Usos comerciales no éticos.

- Actos parasitarios (como obstaculización de comunicaciones ajenas, mensajes con insultos personales, interrupciones en formas repetidas, etc.).
- Obscenidades: Entre los cuales se pueden encontrar los insultos; mensajes raciales, satánicos u otros; y el llamado terrorismo informático, que consiste en mostrar fotografías pornográficas e imágenes que muestran violencia, muerte y destrucción en páginas a niños y a adolescentes.

De acuerdo a lo reseñado con anterioridad, se puede concluir estableciendo que la clasificación general que se hace en torno a los delitos informáticos, atiende principalmente al fin que se persigue al momento de llevar a cabo la conducta ilícita que llega a afectar negativamente a un tercero.

Es así como finalmente se puede llegar a considerar que por cuanto hace a los delitos informáticos, existen tres tipos de comportamiento que se adecuan básicamente a su comisión:

El acceso no autorizado, que hace deliberadamente un usuario a una red, un servidor o un archivo.

Actos dañinos o circulación de material dañino, que se traduce en el robo o copia de archivos (piratería); introducción de información negativa o de virus informáticos; alteración, modificación o destrucción de datos o de software (sabotaje).

Interceptación no autorizada, en la cual el infractor obtiene información no dirigida a é, mediante la intrusión de comunicaciones relativas a sistemas informáticos o telemáticos.

El autor Olivier Hance cita en su obra “Leyes y Negocios en Internet” que las estadísticas más recientes sobre la comisión de delitos informáticos, indican alrededor de 72 mil intentos diarios por lograr acceso ilegal a algún sistema informático, además establece que “se estima que aparecen seis virus nuevos cada día y se han identificado más de mil virus informáticos”[25].

La cantidad de estas operaciones fraudulentas da una idea del daño informático y económico que se genera con la comisión de este tipo de ilícitos. Tan sólo en Estados Unidos, se calcula que se generan perjuicios económicos por los delitos informáticos que superan los 10.000 millones de dólares; en México la situación es menos impactante, sin embargo la necesidad de establecer una solución que frene tal problemática la brevedad posible es algo de vital importancia.

4.2.5. BIEN JURÍDICO TUTELADO EN LOS DELITOS INFORMÁTICOS.

El concepto de bien jurídico fue empleado por primera vez por Ihering para precisar el objeto de protección de las normas de derecho. Para algunos otros juristas como Nawiasky, se debe hablar de fin jurídico o interés jurídicamente protegido, pues el concepto positivista de derecho subjetivo cabe perfectamente en estos términos.

---

[25] Hanse, Oliver. Suzan Dionea Balz. Leyes y negocios de Internet. Traducción: Jasmín Juárez Parra. Revisión Técnica: Gabriel Barrios Garrido. Ed. Mcgraw Hill (Sociedad Internet de México). México, 1996. Traducido de la primera edición en Ingles de Bissnes and Law on the Internet., Pág. 101.

De acuerdo a la teoría positiva, el bien jurídico es arbitrariamente fijado por el legislador de acuerdo a su criterio. Según la misma, el legislador observa la realidad social, y de acuerdo a ésta y a su ideología, determina cuáles son los objetos a proteger. Puede determinar que sean la vida, la libertad, la propiedad, etc.; y la forma que se utiliza para proteger dichos bienes jurídicos determinados por el legislador, es mediante el uso de una sanción que puede ser civil o penal.

La Constitución Mexicana, consigna los bienes jurídicos que el legislador consideró que deberían estar protegidos. De esta forma, el Artículo 14 Constitucional indica que nadie puede ser privado de la vida, de la libertad, de sus propiedades, posesiones o derechos, sino como la propia Constitución prescribe.

El hablar de bienes jurídicos, es hablar de valores esenciales para la sociedad que, por su importancia, son protegidos por el derecho penal mediante la tipificación de delitos que atentan en su contra. Así, cada tipo delictivo consignado en el Código Penal protege un bien jurídico.

Sin embargo, por lo que se refiere a la materia que se analiza en este trabajo de investigación; existe una gran problemática, ya que no se ha llegado a identificar y justificar plenamente, desde la perspectiva normativa y doctrinal, el bien jurídicamente tutelado en los delitos informáticos; tal parece que los autores y legisladores de los países en donde dichos ilícitos ya se encuentran regulados aún no se ponen de acuerdo en cuál es el bien jurídico vulnerado al cometerse un delito de esta índole.

En su obra “Derecho e Informática en México”, Juan José Ríos Estavillo, establece que se debe de identificar plenamente en su esquema primario, el bien jurídicamente tutelado en los delitos informáticos. Al respecto opina, “no podemos decir que lo que se tutela es la intimidad o la protección de la información personal, porque no sólo se protegen éstos, sino también aquellos que deriven de la seguridad nacional, o datos en materia de seguridad pública o en seguridad industrial, por lo cual no podemos tomar una parte como el todo sino al todo con todas sus partes”[26].

Por lo tanto, según lo aseverado por este autor, se debe considerar que el bien jurídicamente tutelado en los ilícitos informáticos es la “información” en general, ya que, por las características de los delitos informáticos, lo que se protege es la información contenida en los bancos y bases de datos, redes de computadoras o simples computadoras personales; comprendiendo dentro de dicha información, tanto la que se deriva de un lenguaje natural como del informático.

De allí que el término “información” deba ser entendido en este sentido, no solo como una simple acumulación de datos, sino como el proceso de “almacenamiento, tratamiento y transmisión de datos mediante los sistemas de procesamiento e interconexión”[27]. Dicho significado le ha concedido al término en cuestión un gran valor, al grado de considerarlo un interés social valioso, dotado de autonomía y objeto del tráfico, lo que justifica su tutela en el campo del derecho penal.

---

[26] Ríos, Estavillo, Juan José. Ob Cit No. 19 p. 128.

Ahora bien, una vez que se ha establecido que la "información" es el interés social digno de tutela penal en los delitos informáticos; hay que determinar si se está frente a un bien jurídico penal de carácter individual o colectivo.

Luis Miguel Reyna Alfaro sostiene que "el bien jurídico propuesto está dirigido a resguardar intereses colectivos, cercanamente relacionado al orden público económico, aunque pueden concurrir a su vez intereses individuales, que en éste específico caso serían los de los propietarios de la información contenida en los sistemas de tratamiento automatizado de datos"[28].

El carácter colectivo que se le atribuye al bien jurídico tutelado en los delitos informáticos, se da tomando en consideración que la información es un interés social vinculado a la actividad empresarial.

La valoración del merecimiento de protección que se le debe otorgar a aquellos intereses que, como la información, tienen un inminente carácter colectivo, debe abordarse en función de la trascendencia que dicho bien tenga para los individuos.

Mir Puig señala que "la valoración de la importancia de un determinado interés colectivo exigirá la comprobación del daño que cause a cada individuo su vulneración"[29], esto quiere decir que no resulta suficiente que el interés social trascienda a la generalidad para que se compruebe el merecimiento de su protección, sino que

---

[27] www.vlex.com , Perú: el Bien Jurídico en el Delito Informático, Luís Miguel Reyna Alfaro, Doctrina-análisis y Artículos. (Consultada el 29/XII/08).
[28] Pagina de internet citada.
[29] Mir Puig, S. Delincuencia informática. Promociones y Publicaciones Universitarias. Librería Babara de Bragaza, 8. Oficinas y Revistas Tamayo y Baus, 728004. Barcelona, 1992, Pág. 98.

precisa también que su lesión o puesta en peligro puedan provocar un daño a los individuos integrantes del grupo social.

En contraposición a lo anteriormente señalado; para otros autores como Luis Manuel C. Meján, el bien que se debe tutelar en los delitos informáticos es la “intimidad”, y más específicamente la “intimidad informática”.

Dicho autor establece que aunque el derecho vigente en el país contiene un buen número de disposiciones que regulan la materia de la intimidad y la información, es evidente que hay lagunas que han sido creadas por el avance tecnológico, las cuales deben ser colmadas con una adecuada legislación sobre la intimidad y en específico, sobre la intimidad informática, en la que se estipulen y regule los derechos de los individuos a conocer, modificar, extraer las informaciones que sobe sí obtienen, tanto de los particulares, como el Estado, y el uso correcto que debe hacerse de dicha información.

Asimismo afirma, que la inclusión de la intimidad informática como garantía fundamental en el texto de la Carta Magna, “sería un reconocimiento justo a la dignidad del ser humano en la problemática que nuestro tiempo pide”[30].

En efecto, tal como lo asevera Fabio Rubén Troncozo Auld, en su estudio titulado “México: El Derecho a la Intimidad y el Derecho a la Información ¿Garantías Encontradas?”, el hombre al nacer lo hace libre físicamente, y él mismo, tiene libertad para dar a conocer de sí

[30] Meján, Luís Manuel C. El Derecho a la Intimidad y la Informática. Ed. Porrúa. 2° Edición. México, 1996, Pág. 130.

ante los demás lo que su voluntad le sugiera; pero con la informatización de la sociedad, esto parece ser imposible. Con la gran inseguridad existente en el almacenamiento, ensayo, recopilación o transmisión de datos en las redes de las empresas públicas o privadas; así como con la manipulación de sistemas informáticos ajenos, la intimidad de las personas se ve quebrantada.

Si bien es cierto que la información es un elemento indispensable en la vida del hombre para la adecuada toma de decisiones, y que el hombre nace con el derecho a estar informado; también es cierto que el mismo tiene plena facultad para decidir qué información desea compartir con los demás individuos de su sociedad y cuál desea reservar para sí mismo.

En este sentido es posible apreciar que, "tanto el derecho a la información como el derecho a la intimidad, son derechos fundamentales en la vida del hombre de estos tiempos. No obstante la distancia que guardan ambos conceptos, se encuentran, hoy en día, estrechamente vinculados, esto debido al mal sentido que se le ha dado al derecho de ser informado, pues abusando de este último es como se transgrede el derecho a la intimidad"[31].

Algunos otros estudiosos del derecho consideran que detrás del delito informático no existe un bien jurídico específico, y que sólo se tratan de formas de ejecución de delitos que afectan bienes jurídicos de protección penal ampliamente reconocida; pero quienes sostienen esto confunden a los delitos informáticos con los ilícitos convencionales que ya están regulados en el Código Penal, sin

[31] www.vlex.com.mx , México: El Derecho a la Intimidad y el Derecho a la Información: ¿Garantías encontradas?, Favio Rubén Troncazo Auld, Doctrina-análisis y artículos. (Consultada el 29/XII/08).

entender que los delitos informáticos son conductas nuevas que por su peculiar naturaleza no se subsumen en la típica descripción de los delitos convencionales, por lo que se debe de admitir la existencia de un bien jurídico propio para esta nueva modalidad de delitos.

Se considera apropiado el criterio seguido por los autores que afirman que el bien jurídico a protegerse dentro de un análisis de delitos informáticos es la “información”, ya que si bien es cierto que hasta hace unos años el merecimiento de protección penal en el interés social aquí abordado hubiese resultado cuestionable; hoy en día, el fenómeno informático en el que se halla inmersa la sociedad ubica al bien jurídico de la “información” en una posición de absoluto y comprensible merecimiento de resguardo en sede penal.

4.2.6. SUJETO ACTIVO EN LOS DELITOS INFORMÁTICOS.

Con la informatización de la sociedad, la proliferación de centrales de cómputo y el aumento en el número de usuarios de éstas; ha surgido un nuevo tipo de acto delincuencial, y con él, un nuevo tipo de delincuente que para cometerlo no usa las herramientas típicas; sino que en su lugar maneja y tergiversa la información contenida en las bases de datos de los sistemas informáticos.

Los sujetos que cometen los “delitos informáticos”, o mejor conocidos como “delincuentes informáticos”, son personas que poseen ciertas características que no presentan el común denominador de los delincuentes.

Por lo regular, estos sujetos activos son individuos que tienen habilidades para el manejo de los sistemas informáticos y que por su situación laboral se encuentran en lugares estratégicos donde se maneja cierto tipo de información de carácter sensible; aunque no se puede generalizar en este sentido, ya que a pesar de que las estadísticas más recientes muestran que el "90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada"[32], otro estudio realizado en América del Norte y Europa indicó que "el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% de la actividad delictiva era externa"[33].

Esto demuestra que en muchos de los casos no necesariamente se requiere que el sujeto activo desarrolle actividades laborales que faciliten la comisión de este tipo de delitos, sino que basta tan sólo con que dicho sujeto sea diestro en el manejo de los sistemas informatizados.

El nivel de aptitud de los delincuentes informáticos, ha sido tema de controversia para diversos autores; ya que mientras que unos sostienen que el nivel de aptitudes no es indicador de delincuencia informática, otros aducen que los posibles delincuentes informáticos son personas sumamente inteligentes, decididas, motivadas y ansiosas de aceptar un reto tecnológico; aunque se puede afirmar que en la mayoría de los casos son personas carentes de principios.

---

[32] www.vlex.com , España: "legislación al Respecto Sobre Delitos Informáticos", (Doctrina-artículos y análisis), Marcelo Manson. (Consultada el 29/XII/08).
[33] Pagina de internet citada.

Al respecto, la Dra. Luz María del Pozo y Contreras manifiesta: "casi la totalidad de este tipo de delincuentes no ven a las computadoras ni a los sistemas informáticos como algo asociado con las personas, las consideran solamente en su aspecto material"[34].

Asimismo, explica que por lo general, estas personas tienden a ser solitarias, ya que prefieren trabajar con cosas y no con gente. Otro factor que influye en el aislamiento de estos individuos del resto de la sociedad, es que pasan largas horas frente a las computadoras en busca de su objetivo, ya que sin trabajo no hay resultados.

La tendencia educacional que presenta la sociedad actual basada en una "racionalización hueca", hace pensar a los jóvenes en el delito informático como algo atrayente, lleno de audacia; y el cometerlo les produce en la mayoría de los casos una situación visceral, de ahí que parte el material humano que comete este tipo de ilícitos.

Hay otra situación preocupante en cuanto a los delincuentes informáticos; ya que debido a la gran disponibilidad de los sistemas informáticos, los cuales se encuentran fácilmente al alcance de cualquier persona sea ésta adolescente o adulto, se ha detectado que la edad de los delincuentes de esta naturaleza está ya entre los 13 a 15 años en adelante, de ahí que en cuanto más avanza la edad y la experiencia de impunidad, se desarrollan mayores capacidades para delinquir.

---

[34] http://www.cddhcu.gob.mx/candip/foro/. (Consultada el 29/XII/08).

Como se puede apreciar de acuerdo a lo anteriormente reseñado, el sujeto activo del delito es una persona de cierto status socioeconómico, puede ser menor o mayor de edad, la comisión de este tipo de delitos no puede explicarse por pobreza del delincuente, ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional. Más bien se trata de personas carentes de principios, que consideran sus desviaciones morales y éticas como algo audaz, y no como un conflicto.

Tomando en consideración las características de los sujetos activos en los delitos informáticos, los estudiosos en la materia los han catalogado como “delitos de cuello blanco”; sin embargo, esta caracterización obedece no al interés protegido como sucede en los delitos convencionales, sino tomando en cuenta al sujeto activo que los comete.

4.2.7 EL SUJETO PASIVO EN LOS DELITOS INFORMÁTICOS.

En primer término se debe distinguir que el sujeto pasivo o víctima del delito es “el titular del derecho violado y jurídicamente protegido por la norma”[35], o “el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo”[36]; por lo que en el caso de los delitos informáticos, las víctimas o sujetos pasivos pueden ser personas físicas o morales, instituciones crediticias, entes gubernamentales, etc., que usan sistemas automatizados de información, generalmente conectados a otros.

---

[35] Castellanos. Tena, Fernando. Obra citada p. 151.

Pero para poder ser considerado sujeto pasivo en los delitos informáticos, requiere ser cumplida una condición específica, que es la de ser titular de la información de carácter confidencial y privada, almacenada en formato digital, es decir, en un sistema informático, la cual es vulnerada por el delincuente informático al llevar a cabo la conducta ilícita. De tal forma, que no puede ser sujeto pasivo de un delito informático, quien no posea una información digital que revista cierto valor que requiera su confidencialidad; o quien detente dicha información pero ésta no se encuentre en formato digital, o sea registrada en un medio informático.

El sujeto pasivo es sumamente importante en el estudio de los delitos informáticos, ya que es a través de él como se pueden conocer las diversas conductas delictivas en las que incurren los sujetos que cometen este tipo de ilícitos y de esta forma tener la posibilidad de actuar en prevención de las acciones antes mencionadas.

Sin embargo, en México e incuso en muchos de los países desarrollados resulta prácticamente imposible conocer la verdadera magnitud de los delitos informáticos, ya que gran parte de éstos no son descubiertos o lo que es peor, no son denunciados ante las autoridades, aunándole a ello la inexistencia de leyes que protejan a las víctimas de este tipo de delitos y la falta de preparación por parte de las autoridades para comprender, investigar y aplicar un tratamiento jurídico adecuado a esta problemática.

---

[36] http://www.monografias.com/trabajos6/delin/delin.shtm , delitos informáticos y computacionales cuyos efectos se producen en el extranjero. (Bolivia). (Consultada el 29/XII/08).

En muchos de los casos esta situación es provocada debido al temor de las empresas víctimas de delitos informáticos, de denunciar este tipo de ilícitos, por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes repercusiones económicas que ello traería aparejado consigo.

Para poder tener una prevención efectiva de la criminalidad informática se requiere entre otras cosas, educar a las víctimas potenciales (sujetos pasivos) de los delitos informáticos sobre las técnicas de manipulación y de encubrimiento utilizadas por los delincuentes informáticos para cometer sus ilícitos; así como estimular en ellos la confianza pública de denunciar esta clase de delitos ante las autoridades encargadas de detectar, investigar y prevenir los delitos informáticos, otorgándoles de esta manera protección penal.

4.3. CONDUCTAS DELICTIVAS TÍPICAS EN LOS DELITOS INFORMÁTICOS.

4.3.1. TIPOS DE CONDUCTAS Y SUS CARACTERÍSTICAS.

En el marco de los delitos informáticos existen ciertas conductas ilícitas que por su relevancia han sido de especial análisis por el derecho internacional público y privado, y que ya son reconocidas en la mayoría de los estados que cuentan con una legislación penal especializada en delitos de esta índole.

Dentro de la clasificación de conductas ilegítimas que comúnmente se llegan a dar en los delitos informáticos se encuentran las siguientes: Hacking, Cracking, Phreaking, Virucker y Carding.

Hacking: La palabra “hacking” proviene del inglés “hack” que significa “hachar” y es el término que se usaba hacia los años cincuenta en los Estados Unidos para describir la manera en que los técnicos telefónicos reparaban las cajas descompuestas, ya que éstos utilizaban como herramienta principal de reparación un golpe seco al artefacto con fallas, es decir un “hack”, de ahí que a estos individuos se les diera el nombre de “hackers”.

En la terminología informática un “hacker” es aquél individuo que “intercepta 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”[37].

La actividad de “hackear” puede tener diferentes finalidades y alcances, Así, en la mayoría de los casos, los “hackers” acceden sin autorización a los sistemas informáticos con el objeto de satisfacer su curiosidad al husmear el contenido de la información protegida en los archivos o programas, o bien, para superar los controles, probar la vulnerabilidad del sistema para mejorar su seguridad, sustraer, modificar, dañar o eliminar información; y éstas motivaciones pueden deberse también a diversos intereses: ya sea que lo hagan con ánimo de lucro, por posturas ideológicas anarquistas, avidez de conocimientos, orgullo, propaganda política, etc.

Para algunos autores, el término “hacker” no significa más que intrusismo informático ilegítimo. Sin embargo, si bien todo intrusismo informático no autorizado resulta ilegítimo, ya que supone el acto de violentar las barreras de seguridad predispuestas por su titular para

proteger la información para acceder al sistema, o bien, porque el ingreso se realiza en contra de la presunta voluntad de aquél, no es posible identificar, de acuerdo a las circunstancias especiales, como es el caso de aquellos informáticos que desarrollan seguridad de redes; que todas estas conductas, en forma indiscriminada, deben de ser objeto de sanción penal.

En efecto, el intrusismo informático, es la penetración por la fuerza a un sistema informático, pero el denominado "hacker ético" es aquel que posee autorización o consentimiento expreso del titular del sistema para verificar su seguridad. En este caso, es lógico pensar que en determinados ambientes como los empresariales por ejemplo; bajo los más estrictos controles y reglas básicas, así como en base a los pertinentes acuerdos contractuales, el intrusismo informático constituye una actividad ilícita, y obviamente debe ser exenta de sanción penal, ya que no concurre el presupuesto de la antijuridicidad.

El jurista chileno claudio Manzur, expresa en su artículo "Chile: Los Delitos de Hacking en sus diversas manifestaciones" publicado en la Revista Electrónica de Derecho Informático; que el hacking puede dividirse en directo e indirecto.

Este autor expresa que el hacking propiamente dicho "es un delito informático que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por e desciframiento de los códigos de acceso o

---

[37] Barrios Garrido, Gabriela; Muñoz de Alba M., Marcia; Pérez Bustillo, Camilo. Obra citada. Pág. 103.

passwords, no causando daños inmediatos o tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor"[38].

Para Claudio Manzur, en el hacking directo, el hacker solo busca la intromisión a los sistemas informáticos por diversión. Entre las características propias de esta clase de hacking están las siguientes: el hacker es una persona experta en materias informáticas y sus edades fluctuarán comúnmente entre los 15 y 25 años, y su motivación no es la de causar un daño, sino que se trata más bien de obtener cierta satisfacción u orgullo, basándose para ello en la burla de los sistemas de seguridad dispuestos. Esta clase de hacking según el autor citado, no representa un importante nivel de riesgo, toda vez que el hacker no busca causar un daño.

Contrario a lo anterior, el mismo autor considera que el hacking indirecto "es el medio para la comisión de otros delitos como fraude informático, sabotaje informático, piratería y espionaje"[39].

La característica principal en el hacking indirecto según lo aseverado por este autor, es que el ánimo del delincuente está determinado por su intención de accesar indebidamente a un sistema informático con el fin de dañar, de defraudar, de espiar, etc. Sin embargo, en este sentido, es menester hacer una distinción entre la conducta que desarrolla un hacker y la que desarrolla un cracker, ya que suele haber confusión entre ambas.

---

[38] www.vlex.com.mx , Argentina: "Presupuestos Para la incriminación del Hacking", Autor Hugo Daniel Carrión. Buenos Aires, Argentina. (Consultada el 29/XII/08).
[39] Pagina de internet citada.

Cracking: Se les llama así, a las entradas ilegales a los sistemas informáticos, que tienen por objeto la destrucción de dichos sistemas, y a los sujetos que las realizan se les denomina "crackers".

"Cracking" es una expresión idiomática derivada del inglés cuya traducción al español se puede entender como "quebrar, vencer las barreras de seguridad y romper lo que hay detrás de ellas"[40]. Según algunos estudiosos de la materia, en el supuesto del cracking; la intencionalidad del agente es accesar ilícitamente a un sistema informático con el fin de obstaculizar, dejar inoperante o dañar el funcionamiento de dicho sistema.

A simple vista, los términos hacker y cracker pudieran significar lo mismo, sin embargo, la diferencia radica en el elemento subjetivo que delimita la frontera de cada comportamiento; mientras que en el cracking la intencionalidad del agente es obstaculizar, dejar inoperante o dañar el funcionamiento de un sistema informático; en el hacking, el sujeto busca únicamente el ingreso a tales sistemas sin dirigir sus actos a la afectación de la integridad o disponibilidad de la información, pero sí vulnerando la confidencialidad y exclusividad de la misma, y la intimidad de su titular.

Aún cuando de lo anterior se pudiera desprender que la conducta que llevan a cabo los hackers al introducirse ilícitamente a los sistemas informáticos no genera daños, su actuar se encuentra dentro del plano de la ilegalidad y ellos lo asumen, de ahí que adopten muchas precauciones para evitar ser descubiertos.

---

[40] http://www.monografias.com/trabajos6/delin/delin.shtm (Consultada el 29/XII/08).

Además, debe destacarse que desde el punto de vista técnico, el ingreso ilegítimo implica la utilización de los recursos del sistema y un riesgo concreto de dañar accidentalmente la información contenida en dicho sistema con la simple intrusión con fines aventureros, por lo que debe destacarse la hipótesis de que el mero acceso sin fines específicos de causar un daño determinado, no genera ninguna consecuencia sobre el sistema informático.

Por tal motivo existe disconformidad con la idea del Dr. Manzur, quien afirma que dicha conducta no representa un importante nivel de riesgo, toda vez que como se puede apreciar, el simple acceso genera consecuencias sobre los sistemas, al mismo tiempo que priva a su titular de la confidencialidad y exclusividad de la información y vulnera el ámbito de su intimidad.

Retornando a la explicación de la figura del cracking, Claudio Manzur expone que "si el acceso ilegítimo al sistema informático es el medio para alterar, modificar o suprimir la información, no habrá hacking sino cracking que supone una acción concreta de daño sobre la información y el elemento subjetivo en el autor -dolo- constitutivo del conocimiento y voluntad de provocarlo"[41].

Entonces, en estricto apego a lo anterior, se puede considerar que el hacking es el presupuesto necesario para que se dé el cracking, sin embargo al consumarse la conducta del cracking se sobreentiende que para su consecución tuvo que haber un hacking previo, por lo que ésa conducta queda subsumida en la otra.

[41] www.vlex.con.mx, Argentina.

Lo que es un hecho en definitiva, es que en ambos casos, tanto en el hacking como en el cracking, hay una afectación al bien jurídico tutelado en los delitos informáticos, es decir, a la información, de ahí la peligrosidad de este tipo de conductas que hacen inminente la comisión de los delitos informáticos.

Phreaking: La actividad del phreaking, es una de las conductas ilícitas más comunes en el medio de los delitos informáticos; y se define con este término, a la actividad de obtener ventajas de las líneas telefónicas para los efectos de no pagar los costos de comunicación. Es decir, básicamente se trata de encontrar el medio para evitar el pago por el uso de la red telefónica, ya sea ésa pública o privada, digital o inalámbrica.

El phreaking, es considerado como un delito informático por la mayoría de los autores en la rama; no obstante lo anterior, esta conducta es generalmente extra PC, es decir, raramente se realiza a través de las computadoras; su gestión se efectúa básicamente vía telefónica y se lleva a cabo por medio de la ingeniería en electrónica y no como en los delitos informáticos, los cuales se realizan propiamente a través de ingeniería en sistemas computacionales.

Virucker: Esta conducta consiste "en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus informáticos" y destruir, alterar y/o inutilizar la información contenida"[42].

[42] Barrios Garrido, Gabriela; Muñoz de Alba., Marcia. Perez Bustillo, Camilo. Obra Citada. p. 103.

Los virus informáticos son programas secuenciales que tienen como objetivo bloquear los sistemas informáticos, destruir los datos contenidos en dichos sistemas o causar un daño en la memoria de éstos, y que tienen una gran capacidad de preproducción en el ordenador y de expansión y contagio a otros sistemas informáticos. Su incidencia es similar a la que ejercen los virus propiamente dichos en el organismo humano, de ahí su denominación. El origen de los virus informáticos es desconocido, pero se tiene conocimiento de que Bulgaria es el país productor de la mayoría de ellos, seguido por Rusia, y Estados Unidos. Entre los virus informáticos más conocidos están: el Data Crime, Alabama, Disk Killer, I Love You y Melissa.

De acuerdo a lo expuesto en líneas anteriores, la conducta "virucker" se puede llegar a encuadrar dentro de la que se denomina "cracking", ya que como se vio con anterioridad, el cracking supone el acceso ilegítimo a un sistema informático con el fin de obstaculizar, dejar inoperante o dañar el funcionamiento de dicho sistema; y como se aprecia en la definición de la conducta "virucker", ésta se lleva a cabo de igual manera, a través del ingreso ilícito y doloso a un sistema informático con el objeto de destruir, alterar y/o inutilizar la información contenida en éste, mediante la introducción de un virus informático.

Carding: Se le llama carding a la actividad de cometer un fraude o estafa a través del uso ilegal de tarjetas de crédito. Pero no todo fraude cometido con una tarjeta de crédito supone que se éste realizando carding, ya que si una tarjeta de crédito es robada o encontrada y se usa por otra persona que no es su titular, ello no constituirá carding, sino un fraude convencional.

El carding consiste propiamente en el uso de un número de tarjeta de crédito (ya sea real o creado a través de procedimientos digitales), con el fin de realizar compras a distancia por Internet y efectuar pagos.

El nivel de seguridad en Internet para realizar transacciones económicas no es bueno. A menudo existen fugas de información; ya que muchos usuarios de la red ponen su número de tarjeta de crédito para hacer compras y estos números son captados por otras personas que los reutilizan para hacer más compras sin ser los titulares de la tarjeta.

En otras ocasiones, los delincuentes informáticos que llevan a cabo este tipo de conducta, generan números válidos de tarjetas de crédito a través de procedimientos digitales para usarlos posteriormente en compras a distancia.

Otro inconveniente con que cuentan las tarjetas de crédito, es que las empresas que otorgan tarjetas numeradas a sus usuarios lo hacen a través de un sistema automatizado de creación de números aleatorios; dicho sistema es muy susceptible de ser vulnerado ya que cualquier persona con conocimientos en la materia puede hacer un sistema de cálculo de números aleatorios y por tanto, puede crear números válidos para efectuar transacciones fraudulentas.

Con el análisis realizado a las conductas delictivas típicas en los delitos informáticos, se puede apreciar la relevancia jurídica que dichas conductas han adquirido en la actualidad en virtud de la gran cantidad de delitos informáticos que diariamente se realizan a través de las mismas, lo que hace cada vez más importante su tipificación y

sanción a través de la creación de sistemas jurídicos aplicables a los mismos.

CAPITULO V.
PROTECCION PENAL DE LA PROPIEDAD INTELECTUAL EN INTERNET.

5.1 ALGUNAS CONSIDERACIONES PRELIMINARES.

La propiedad intelectual, desde el punto de vista de la tradición continental europea y de buena parte de los países latinoamericanos, "supone el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano"[43].

En los términos de la Declaración Mundial sobre la Propiedad Intelectual (votada por la Comisión Asesora de las políticas de la Organización Mundial de la Propiedad Intelectual (OMPI), el 26 de junio del año 2000, es entendida similarmente como "cualquier propiedad que, de común acuerdo, se considere de naturaleza intelectual y merecedora de protección, incluidas las invenciones

[43] http://es.wikipedia.org/wiki/Propiedad_intelectual (Consultada el 29/XII/08).

científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Existe además una corriente, especialmente la que proviene del movimiento de *Software Libre*, que considera que el término "Propiedad Intelectual" es engañoso y reúne bajo un mismo concepto diferentes regímenes jurídicos no equiparables entre sí, como las patentes, el derecho de autor, las marcas, las denominaciones de orígen, entre otros.

Dicho lo anterior y estudiando de lleno el tema que nos compete, tenemos que señalar que uno de los mas grandes errores que se puede cometer al desarrollar un tema de derecho penal es circunscribirse a un ordenamiento en especifico, con mayor razón cuando se habla de Derecho Penal Informático, dada la natural trasnacionalidad de los actos dañosos que esta nueva tecnología implica.

Es cierto que, como primera medida, debe siempre tenerse en cuenta esta trasnacionalidad a fin de realizar una aproximación coherente con las conductas de los posibles transgresores de los derechos ajenos.

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

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

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

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

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

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

protección de los derechos involucrados, es claro que en poco tiempo los autores se negaran a exponer sus creaciones en la red por el riesgo que ello implica para sus derecho patrimoniales.

Estos pequeños ejemplos surgen, por cierto, de las experiencias recientes en algunos casos de otros delitos en la red, como el sonado del virus I LOVE YOU que como fue introducido desde Filipinas por un natural de ese país resultó impune cuando los daños causados a la administración y al gobierno de Estados Unidos resultaron cuantiosos.[44]

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

Para los efectos prácticos del estudio de esta problemática, dividiré en forma totalmente arbitraria y personal las áreas de estudio, a fin de simplificar la solución de los temas planteados.

5.2 LA LEY APLICABLE

Es un principio generalmente aceptado la territorialidad estricta del Derecho Penal, lo cual refleja, el principio de juez natural reconocido en los tratados internacionales de derechos humanos, pero, como todo principio, éste admite algunas excepciones. Dentro de éstas,

[44] Campolli. Gabriel Andrés. Principios de Derecho Penal Informático. Editorial Ángel. Primera Edición. México 2004. Pág. 58.

podemos hablar de aquella que permite la extraterritoraliedad del Derecho Penal en aquellos casos en que los efectos del delito se produzcan dentro del territorio que se arroga la aplicación de su derecho o la que implica que se hace extensiva la aplicación del Derecho Penal de un Estado cuando los efectos del delito afecten en forma directa los intereses del mismo.

Estos dos casos son recogidos expresamente por el PC de la Republica Argentina, y en forma general, en mayor o menor medida, por casi todos los ordenamientos del mundo.

Según estos principios podemos decir que en casi todos los casos resultaría aplicable la ley penal del lugar donde se produzcan los efectos del delito.

Pero claro, volvemos al punto de partida, ¿Dónde se producen los efectos? ¿En el lugar donde se asienta el servidor que sostiene la página, o donde el damnificado por las violaciones de propiedad intelectual pierde en forma ilegítima sus derechos o sufre un menoscabo en su patrimonio?

Cualquiera de esas dos opciones parece razonable, pero si recordamos que siempre en forma anexa a la demanda penal por violación de propiedad intelectual existe un reclamo por vía civil, sería lo mas lógico que independientemente de en que locación o territorio se encuentre asentado el servidor que soporta la pagina *web* o la base de datos que es objeto del delito, corresponde la aplicación de las leyes del territorio en el cual el sujeto pasivo se menoscabados sus derechos patrimoniales, morales, o ambos, toda vez que estos derechos son en definitiva el bien jurídico protegido.

El único inconveniente se puede plantear en los casos en que los daños se produjeron de forma simultanea en varios Estados, por lo cual se pueden tener soluciones alternativas, por ejemplo, la aplicación de ley del país en que el delito fuera mas grave, aunque en verdad y *prima facie* pueda decirse que esto entraría en conflicto con el principio de ley penal más benigna, lo cual no es así dado el que este hace referencia a las leyes de un mismo ordenamiento, cosa que no sucede en casos como el planteado.

En aquellos casos en que hablaremos de delitos o daños de igual magnitud (ya que la entidad de los daños causados puede ser así mismo un criterio de aplicabilidad de la ley), podríamos decir que correspondería por ejemplo, la *lex fori* de aquel estado que hubiese iniciado las actuaciones, y en caso de persistir, aún nos queda el criterio de la aplicación de la ley del lugar en que el sujeto activo fuere detenido, con lo cual siempre encontraríamos, en diversos rangos una solución para poder evitar la superposición de dos o mas ordenamientos aplicables.

5.3 LA COMPETENCIA JURISDICCIONAL

Una vez resuelto el problema de la ley aplicable, corresponde al ordenamiento interno de cada país según las normas de Derecho Penal Internacional la determinación del juez competente en cada caso, pero con la salvedad de que si no ha sido esta determinada por el ordenamiento interno, debe siempre estarse a los jueces de competencia nacional o federal, según se denomine en cada situación, dada la internacionalidad de las cuestiones planteadas, a la casi seguridad de que deberá imputarse a ciudadanos extranjeros, empresas, o ambos, con asiento extranjero, y además debemos tener

en cuenta que, por regla general, las cuestiones referentes a las telecomunicaciones (y no debemos olvidar que Internet es en gran parte telecomunicación), corresponden a los ordenamientos federales o nacionales, según se denominen en casa Estado.

5.4 LA EXTRADICION

Un capitulo aparte merece el tema de la extradición, ya que ésta implícita la interacción de, al menos, dos estados, y ello supone algunas condiciones de coincidencia mínimas entre ambos ordenamientos.

Una de esas coincidencias es la que se funda en el hecho de que el acto perseguido debe ser delito en ambas jurisdicciones, lo cual, a la altura del desarrollo del Derecho Penal Informático que hoy nos encontramos, supone en la práctica un obstáculo casi infranqueable, ya que la mayoría de los delitos electrónicos o informáticos no se encuentran legislados casi en ningún país del planeta, lo cual implica una casi imposibilidad fáctica de la misma.

Por otra parte debe de tomarse en cuenta también el hecho de que si se trata de delitos menores, correccionales o como sea que la legislación interna denomine a los que poseen penas privativas de la libertad menores a dos o tres años, según el caso, los mismos resultan para casi todas las legislaciones como extraditables, razón que impone una nueva restricción a los casos que nos ocupan si esto no se prevé en forma adecuada al momento de realizar la legislación de cada Estado.

Lo cierto a modo de reflexión, es que a la fecha, estos delitos contra la propiedad intelectual en la red, rara vez pueden ser llevados a juicio, si los mismos son cometidos fuera del territorio en el cual reproduce el daño o lesión al bien jurídico.

Por poco que se medite, la solución es casi única: Establecer un tratado internacional especifico para regular las cuestiones planteadas, y sobre todo la extradición, pero con el claro inconveniente de que cualquier país o grupo de países que no firmen y ratifiquen el tratado, ponen en peligro, en forma directa, la efectividad de éste, toda vez que cuando los sujetos activos se encuentren en su territorio resultara imposible la extradición para su juzgamiento.

Como solución alternativa, hasta tanto se logre un marco internacional adecuado, podría preverse que la investigación de los hechos y la captura de los sujetos involucrados quede a cargo de la INTERPOL, por ejemplo, dado su carácter trasnacional, a otro organismo similar que pueda cumplir sus funciones en la mayoría de los Estados posiblemente afectados por conductas de los tipos descritos en el presente trabajo.

Como ultima consideración, pero no por ello menos importante, debe también tenerse en cuenta el hecho de que la casi totalidad de los países impide la extradición pasiva de sus propios nacionales en tanto y en cuanto ellos se encuentren dentro del territorio del cual ostenta esa calidad, cuestión a debatir seriamente, ya que este límite crearía una barrera que impediría casi totalmente la aplicación de norma penal alguna, ya que dentro de la red es muy fácil cometer cualquier tipo de delitos si abandonar el propio territorio, los cuales

quedarían impunes en casi todos los casos, toda vez que si el país de origen no autoriza la extradición de sus nacionales, cualquier ordenamiento resultaría ineficaz para aplicar sus procedimientos penales en ausencia del sujeto activo, al cual resulta imposible hacer comparecer a juicio.

En este punto creo que al menos para los delitos cometidos a través de la red y en virtud de ka defensa de intereses comunes, deberían los Estados reflexionar la postura, ya que son los mismos estados quienes pueden ser victimas de las acciones ilegítimas por la red.

5.5 EL BIEN JURIDICO PROTEGIDO

Si hacemos referencia a cuál es el bien que esta normativa debe proteger, debemos de remitirnos a las clasificaciones habituales de los delitos, colocando a éstos dentro del ámbito de los delitos contra el patrimonio.

Tenemos, de esta manera, en realidad dos bienes jurídicos integrantes de la protección: *a)* Los derechos patrimoniales del autor, y *b)* Los derechos morales del autor.

Es claro que cualquier norma que pretenda una protección adecuada de la propiedad intelectual en Internet debe contemplar al menos esos dos aspectos.

De estos dos tipos de bienes jurídicos, resulta mas fácil la protección de los derechos patrimoniales, ya que es evidente que los efectos de cualquier violación que se produzca sobre este tipo de

derechos siempre será mucho más notoria que la que se produzca a los derechos morales, la cual puede permanecer oculta o disimulada durante varios periodos sin que el sujeto pasivo note la comisión del delito.

Por otra parte, debemos tener en cuenta también que no todos los derechos morales pueden ser protegidos en forma eficiente y eficaz, sino que en general se tiende en la mayoría de las legislaciones a su protección civil por considerarse mas adecuada a esos efectos.

Asimismo se debe recordar el hecho de que las legislaciones de origen anglosajón no reconocen siquiera la existencia de estos derechos, razón por la cual debe suponerse que en forma alguna los mismos podrían ser protegidos por la legislación penal, lo cual, en caso de realizarse tratados internacionales, puede, como ya lo ha sucedido en materia civil, producir escollos insalvables que lleven a un claro desperdicio de esfuerzos, ya que las posiciones se vuelven infranqueables en lo que a la existencia y protección de derechos morales de autor se refiere.

En algunos casos, pues, la doble protección puede resultar ineficaz o incluso conflictiva, razón por la que sería recomendable que en los casos en que el legislador considere necesaria la protección penal de los derechos morales del autor, debe siempre tenerse en cuenta que para los tratados internacionales de la materia, ésta posiblemente se dejada de lado en pos de arribar al acuerdo sobre los temas de mayor jerarquía, como los son aquellos que implican además la violación patrimonial, es decir, que en un solo acto se violentarían los dos bienes jurídicos protegibles.

5.6 LOS DERECHOS DE PROPIEDAD INTELECTUAL E INTERNET

Como primera medida, debe comprenderse cual es la necesidad real de una protección penal de estos derechos en Internet y su alcance normativo y aplicativo, ya que los tipos penales son los que en definitiva incluyen o excluyen una determinada conducta del espectro penal.

Como en todo tema de Derecho, es cierto que existen al menos tres posturas, la desincriminatoria, la netamente proteccionista y la ecléctica, En este caso, como casi siempre sucede, los extremos terminan resultando viciosos, y por ello siempre se tiende a la postura intermedia o ecléctica.

En este caso no podemos decir que deben penarse algunas conductas y otras no. En rigor de verdad deben penarse aquellas que impliquen un desmedro del patrimonio del sujeto activo, con los agravantes o atenuantes que el legislador considere necesarios.

El esquema planteado por la legislación española puede ser considerado como una alternativa posible, aunque quizás pueda mejorarse en algunos aspectos. Por eso se hace necesario enunciar qué actos resultarán punibles y cuáles no.

Para ello resulta entonces importante *a contrario sensu* definir cual es la función de las páginas de Internet o de las bases de datos puestas a disposición del público en esa red.

Es claro, por ejemplo, que las páginas *web* han sido creadas por sus autores con la expresa finalidad de ser visitadas por los

navegantes, razón por la cual la carga de las mismas en la mayoría RAM del ordenador del navegante jamás puede ser ilícita ya que es su función real.

Por otra parte, las mismas páginas no se trasmiten por la red, sino que, en mérito al rigor científico, debemos reconocer que lo que se envía por Internet al navegador es una serie de instrucciones en lenguaje HTML, por lo cual esas instrucciones parten desde el autor como para el libre acceso del usuario, a lo que debemos agregar que las computadoras graban esa información de la página en forma temporal para evitar tener que recuperarla cada vez que el usuario ordena un adelante o atrás en el navegador.

De todo este se desprende que el uso y el almacenamiento de las páginas *web* en el. ordenador propio no pueden ser considerados delitos en ningún caso, ya que responden al uso normal de la obra puesta a disposición por el creador.

Pues bien, en general se tiene por aceptada la postura de que las ideas no se protegen, cuestión que, en lo personal, y para algunos casos específicos no comparto, pero éste en particular no es uno de ellos, aunque sostengo que deben protegerse algunas ideas como en el caso del *know how* del sistema anglosajón; podemos decir entonces que, por regla general, tampoco pueden protegerse los botones, iconos, diseños de *links* u otros objetos de HTML o JAVA que se incluyan en la página.

Otro punto distinto es el caso de la impresión de las páginas para el uso del navegante, pero si asumimos que absolutamente todos los navegadores poseen un menú de impresión podemos decir

que el mismo tampoco resultaría ilegítimo desde que el autor al colocar la página conocía esta posibilidad y él consintió que la página presentada en la red pueda ser impresa por el navegante. Alguna peculiaridad presentarían en este caso aquellas páginas que mediante códigos especiales han bloqueado esta posibilidad, en cuyo caso en realidad el delito podría configurarse por el salteo, craqueo o violación de los códigos más que por la propiedad intelectual en sí.

Pues bien, si ninguna de estas conductas puede ser considerada ilegítima y en virtud de ellos no pueden ser protegidas penalmente, ¿qué conductas si pueden protegerse? La respuesta surge, pues, del análisis precio: todas aquellas que no correspondan con el uso normal de las páginas *web* o de los contenidos presentados en las mismas.

Para iniciar el desglose de esas conductas, me remito, pues, a la legislación civil de la materia que es la que describe cuáles son los derechos de los autores en el ámbito patrimonial para descubrir así qué conductas pueden ser ilícitas en virtud del alcance de esos derechos.

5.7 DERECHO DE EXPLOTACION

En el caso de las violaciones a este derecho en particular, es claro que puede protegerse en forma penal la explotación ilegítima de las páginas *web* y de sus contenidos, mediante tipos penales que eviten conductas lesivas como la desviación de tráfico, el *deep linking* y cualquier otra que produzca un menoscabo en el rendimiento económico esperado de la página o del contenido de la misma.

Es claro que al cubrirse este derecho genérico deben considerarse incluidos en la protección los derechos de reproducción, distribución, comunicación pública, puesta a disposición del público, transformación o cualquier otro que se considere como parte de la explotación de una obra o su fijación en el caso de los derechos de los intérpretes.

5.8 PERFILANDO EL TIPO PENAL ESPECIFICO

Luego de toda esta introducción de consideraciones generales de los delitos en la red y de la propiedad intelectual y tipos delictivos, por resumen, estamos ahora en condiciones de realizar o dar forma al tipo penal específico para la protección de los derechos intelectuales en la red.

Queda claro que la protección penal para la propiedad intelectual en Internet debe remitirse en forma expresa a los derechos económicos de los titulares de las páginas *web* o de sus contenidos, ya que resulta casi imposible la protección de los derechos morales de autor en este ámbito tan efímero y trasnacional en el que nos movemos, con implicancias de distintos ordenamientos que pueden o no otorgar alguna protección mayor en materia civil pero que, por regla general, clasifican a estos delitos dentro del grupo de delitos económicos.

Si bien expresé que la norma prevista en el ordenamiento español me parece correcta en cuanto al tipo penal, hice en su momento algunas reservas, las cuales me permito explayar en este momento de resumen del tipo.

La primera objeción surge en el hecho de que la norma requiere para la configuración del tipo penal el ánimo de lucro en el sujeto activo, cuestión que no considero correcta ni necesaria, ya que en función de la propiedad del bien jurídico y de los posibles daños económicos que pudiere sufrir el sujeto pasivo, tal condición resulta innecesaria, ya que una acción con los mismos efectos podría quedar impune si el órgano acusador no pudiere demostrar el ánimo de lucro en el sujeto activo, resultaría fuera de tipo penal y por ello impune de haber producido daños efectivos.

La segunda objeción tiene que ver con el tipo de normas que deben aplicarse en Derecho Penal a fin de evitar constantes actualizaciones de la legislación vigente.

Con esto me refiero a que si bien el articulo trascrito considera todas las posibles violaciones a los derechos de propiedad hoy existentes, ello no implica que una modificación en la legislación o un nuevo avance en la tecnología no conviertan a la norma penal en letra muerta, y un buen ejemplo de ello pueden resultar los recientes *e-books* que no se encontrarían protegidos toda vez que pueden no ser considerados por algunos como verdaderas obras en virtud de la novedad de su *corpus mecanicus*, lo cual podría acarrear serios problemas en un futuro cercano, como también el hecho de cuáles son los límites de la reproducción para el uso personal que, como ya dijimos, no puede ser considerada delito.

Se dice, y no sin razón, que siempre los tipos penales deben ser específicos en virtud de la finalidad protectiva del Derecho Penal, lo cual no implica que en gran medida, los mismos puedan ser abiertos, y un claro ejemplo de ello es el tipo penal del homicidio, que

en la mayoría de las legislaciones se presenta como un tipo penal abierto, con una redacción que implica más o menos que “aquel que matare quitare la vida o expresiones similares a otro sin distinción de sexo o edad, sufrirá la pena de... según el caso puede hasta ser pena de muerte”, pero en ningún caso se especifica los miedos por los cuales se produce la muerte, con la salvedad de aquellos sistemas que en algunos casos prevén el medio apara producirla como agravante de la pena.

¿Pues bien, si en un bien jurídico tan caro al ser humano como lo es la vida, se permite sin restricciones la formula “por cualquier medio” en forma implícita o explícita, porque no podemos utilizar ese tipo de formulaciones en algo tan vinculado a la cambiante tecnología a fin de evitar constantes revisiones y modificaciones de la legislación penal que en definitiva sólo resultan en detrimento de los sujetos activos y del mismo pueblo en virtud de la innecesaria pérdida de tiempo legislativo?

5.9 EL TIPO PENAL BASICO

Luego de las salvedades expuestas, me permito delinear el tipo penal básico para la protección penal de la propiedad intelectual en Internet.

Plagio simple: “El que usurpare la calidad de autor, o indujere a un tercero a error sobre la misma en una creación intelectual de cualquier tipo, o de otra manera, cualesquiera que esta fuere, desplazare de esa calidad al verdadero autor por cualquier medio que no implique la voluntad expresa y no viciada del mismo, se esta

conducta realizada en forma presencial o por medios telemáticos de cualquier tipo, sufrirá la pena de…"[45]

Plagio agravado por la finalidad o los medios: "El que cometiere el delito previsto en el articulo anterior, con fines de lucro, o bien el detrimento de los derechos patrimoniales del verdadero autor, dentro del territorio en el cual este reside o en territorio extranjero, a través de la utilización de medios telemáticos o su aplicación, aunque no obtuviese beneficio económico propio o para un tercero, pero habiendo producido una disminución o frustración absoluta de los derechos del autor en forma real o potencial, sufrirá la pena de…"[46]

Plagio agravado por los resultados: "El que hubiere cometido alguno de los delitos de los artículos anteriores, y de ello hubiere obtenido un lucro, sea este de forma directa o indirecta, sufrirá la pena de…"[47]

Plagio agravado por la condición personal: "Se agravara la pena de los artículos anteriores en un tercio de la escala si el sujeto activo del delito fuere funcionario publico o perteneciere a una entidad de derechos intelectuales publica o privada, con o sin fines de lucro, o en los casos en que la obra hubiere llegado a su poder en virtud de una relación contractual, laboral, educativa o de otra especie que indique en algún termino relación de subordinación entre el sujeto activo o sujeto pasivo"[48]

En virtud de la amplitud de los tipos propuestos, los indicados cumplirían los presupuestos previstos y desarrollados en el presente

[45] Ibidem. p. 71.
[46] Idem.
[47] Idem.
[48] Idem.

trabajo a los efectos de proteger debidamente la propiedad intelectual en la red de Internet, sin necesidad de ser, en un futuro, modificados, por los sucesivos cambios tecnológicos que pudieren ocurrir en la red.

Para evitar confusiones sobre la calidad de obra de un determinado objeto, como por ejemplo las paginas web en si mismas, correspondería en todo caso la aclaración en un artículo supletorio que podría tener la siguiente redacción:

Articulo complementario: "Se consideran a los efectos del presente (titulo, capitulo, apartado o la denominación que corresponda según el caso), expresamente incluidas dentro de obras protegidas a las paginas web, la información en ellas contenidas, los artículos periodísticos publicados en papel o en la red, las bases de datos on line y off line y cualquier otra que la legislación civil considere como obra intelectual a los efectos de la protección de derechos de autor."

Deberá pues advertirse, de cualquier manera, el presente artículo es contemplado como norma abierta, ya que remite en forma expresa a la legislación civil, y cualquier cambio en los criterios fundantes de la misma en referencia al concepto de obra producirá en forma automática la modificación necesaria en la legislación penal.

5.10 ALGUNAS SOLUCIONES FUERA DEL TIPO PENAL.

Como ya anticipe, se hace necesarias para evitar futuras imposibilidades practicas en la aplicación de la norma, algunas consideraciones especiales en cuanto a la Ley Aplicables y

Competencia de los Tribunales, cuestión que puede dificultar o impedir la correcta aplicación de las normas previstas y de esa manera no permitir la verdadera protección penal de los derechos intelectuales en Internet.

Estas previsiones debieran ser generales a efectos civiles y penales, ya que no son, los que hoy nos ocupan, los únicos delitos posibles en Internet ni las únicas discusiones posibles respecto a la competencia Ley Aplicable, por lo que considero que en realidad las siguientes deberían ser adoptadas dentro de la parte General de los códigos penales, civiles, o ambas, a efectos de evitar futuros conflictos de leyes o incompetencias que nada aportan a la seguridad jurídica de los desarrollos intelectuales o comerciales de la red.

5.11 SOBRE LA LEY APLICABLE, LA COMPETENCIA E INTERNET

Como ya se expuso, se considera conveniente la aplicación de la Ley en el lugar en el cual los efectos se producen, ya sea esta de tipo penal o civil, y a modo explicativo, se integra al presente a cápite u ejemplo en forma previa a la formulación legal especifica relativa a propiedad intelectual.

Supongamos una obra publicada en la pagina web con dominio en la Republica Argentina, soportada en un *Server* que reside en Miami, y que es tomada por un ciudadano español y publicada en una revista italiana como propia, pues bien, ¿ en que lugar se producen realmente los efectos del delito?

Algunos dirían que en Argentina, porque ese es el sitio en que se produce el desbaratamiento de los derechos de autor, ya que ahí

reside el dominio; otros, que en Estados Unidos ya que el articulo esta en forma física en el *Server* de Miami, otros de que en España ya que el sujeto activo reside ahí.

Pues bien, en realidad los efectos del delito se producen en Italia, ya que es ahí donde el autor pierde sus derechos por el accionar del plagiario, y es ahí donde, en definitiva, dejara de percibir lo que le corresponde por regalías en concepto de derecho de autor.

Es claro, entonces, que se debe considerar como sitio de producción de los efectos a aquel en el cual el autor deja de percibir los beneficios que le corresponden según la ley de ese lugar.

Es por ello que corresponderá en definitiva la aplicación de la Ley Italiana a todos los efectos con independencia del lugar de residencia del sujeto activo o sujeto pasivo, aun del lugar en que se desarrolle el juicio.

Respecto a la competencia de los Tribunales en el enjuiciamiento, la materia civil puede separarse de la penal, ya que podría ser validamente aceptada una demanda interpuesta en Argentina en Italia o en España, con las consecuencias que ello implica para la seguridad jurídica.

Creo, por ello, que seria mas prudente igualar ambas competencias toda vez que hay una gran cantidad de ordenamientos procesales penales que permiten en forma conjunta ambas acciones. Como ya se dijo, se sostiene que debería remitirse a los Tribunales

competentes según la ley aplicable pero ello puede tener algunos inconvenientes que deberían ser cubiertos de alguna manera.

Si se acepta como posible la aplicación extraterritorial de la ley penal en función del lugar de cumplimiento de los efectos del delito, y los tribunales admiten el juzgamiento de delitos cometidos en forma extraterritorial(dada al amplitud de Internet, este es un criterio que se torna necesario) validamente se podría, por ejemplo aceptar que según la ley italiana se designe como competente a un tribunal español para el enjuiciamiento del delito cometido pero con la aplicación de la ley italiana de fondo y la española de forma.

Esta posición evitaría violar la garantía universal del juez natural para el sujeto activo y mantendría incólumes los derechos del sujeto pasivo sin necesidad de producir la extradición la cual como se dijo en muchas casos resultaría menos que imposible.

Por otra parte, tampoco considero que pueda violar los principios del Derecho Penal en general, ya que como sabemos, los delitos que nos ocupan pertenecen al grupo de los de acción publica(o de atención por los ministerios fiscales o procuraduría según el caso), razón por la cual es innecesaria la presencia del sujeto pasivo en el desarrollo del juicio penal.

En cuanto a los reclamos civiles anexos que pudieran surgir, los cuales dependen de la acción directa del damnificado, se pueden presentar soluciones alternativas que salvaguarden sin necesidad de su presencia.

A fin de evitar posibles conflictos de leyes aplicables y competencia, lo ideal seria agregar como norma de conexión internacional la siguiente:

Sobre la ley aplicable y la competencia de los delitos: *"A los efectos de los presentes delito, será aplicable la ley del territorio en el cual se produzcan los efectos del mismo, sea el plagio o sui manifestación económica, debiendo entenderse como tal aquel en que el autor deja de percibir sus regalías por la acción del sujeto activo. Será competente a esos efectos el juez del lugar en que se encuentre el autor del hecho pero en todos los casos deberá aplicar la ley de fondo correspondiente y será de uso la ley procesal del lugar de asiento del procedimiento."*[49]

[49] Ibidem. p. 75.

CONCLUSIONES

PRIMERA.- Como toda enunciación teórica, la presente puede ser vista desde muchos ángulos en los cuales algunos podrán o no coincidir, pero adelanto que la finalidad del presente trabajo a sido tratar de analizar la situación a la fecha de la protección penal de la propiedad intelectual en Internet, tratando de adaptar los conceptos generales de la misma en tanto las normas originales no tenían prevista la explosión de información que ha producido la red y las posibles consecuencias que ello implica en el ámbito internacional.

SEGUNDA.- Por regla general, las normas penales, por su territorialidad son pensadas solo en función de propio territorio, pero para el caso de Internet y su aplicación en el *ciberespacio*, deben preverse los efectos internacionales que seguro van a surgir.

TERCERA.- Es por ello que se ha intentado cubrir, en forma expresa, ese tipo de implicaciones mediante la modificación de los

tipos penales y el agregado de algunas normas alternas que den sentido a la aplicación extraterritorial de las normas penales.

Creo, en definitiva, haber dejado cubierto no solo los aspectos de fondo penal si no también los aspectos procesales que pudieren impedir la normal aplicación del derecho sustantivo.

CUARTA.- Dejo claro en esta conclusión que con toda norma penal, las formulaciones realizadas son orientativas y, en definitiva, deben ser adaptadas a cada ordenamiento en particular, pero el fin es un desarrollo teórico de normas penales que siempre dependen para su aplicación de la política criminal de cada Estado.

QUINTA.- Por lo demás, en cuanto mas se aproximen las normas finales a las presentes en su conjunto, menores problemas practicas habrán de producirse en su aplicación y en el intento de unificar las legislaciones a efectos de logara un tratado internacional que prevea las normas penales a aplicar en Internet y sus implicaciones procesales.

SEXTA.- En definitiva, lo ideal es lograr el acuerdo internacional que permita la persecución penal internacional de todos los delitos cometidos en la red, pero hasta que ello ocurra, seria recomendable la adopción de normas similares alas descritas a efectos de mitigar las posibles violaciones de derechos intelectuales en Internet que hoy se hallan tan en boga y que, en definitiva, no hacen otra cosa que día a día disminuir la creatividad por la falta de incentivos reales y por la gran sensación de desprotección que sienten los autores y creadores.

SEPTIMA.- No dejaremos que red sucumba por falta de protección adecuada, contamos con las soluciones reales, solo debemos ponerla en practica de manera urgente y efectiva.

BIBLIOGRAFIA

BIDART Campos, Germán José, “Teoría General de los Derechos Humanos”, 1° Ed., 1991.

CAMPOLI, Gabriel Andrés. Principios de Derecho Penal Informático. Editorial Ángel. Primera Edición. México 2004.

CAPPELLETTI Mauro, “Access to Justice”; Milan, Italia. 4° Ed., 1979.

CASTELLANOS Tena, Fernando. “Lineamientos Elementales del Derecho Penal” (Parte General). Trigésima Cuarta Edición. Editorial Porrúa., México, D.F., 1994.

DE CABO, Filosofía del Derecho y Filosofía de la Cultura. 3° Ed., 1982.

FIX-ZAMUDIO, Héctor y Ovalle Favela, José; “Derecho Procesal”; 1° Ed. 1991, México.

HANSE, Oliver. Suzan Dionea Balz. “Leyes y negocios de Internet”. Traducción: Jasmín Juárez Parra. Revisión Técnica: Gabriel Barrios Garrido. Ed. Mcgraw Hill (Sociedad Internet de México). México, 1996. Traducido de la primera edición en Inglés de Business and Law on the Internet.

MEJÁN, Luís Manuel C. “El Derecho a la Intimidad y la Informática”. Editorial Porrúa. 2° Edición. México, 1996.

MIR Puig, S. “Delincuencia informática. Promociones y Publicaciones Universitarias”. Librería Babara de Bragaza, 8. Oficinas y Revistas Tamayo y Baus, 728004. Barcelona, 1992.

ICONOGRAFIA

http://www.cddhcu.gob.mx/camdip/foro/, “Foro de Consulta Sobre Derecho e Informática (Memorias)”, ponencia: “Mecanismos Existente con Ausencia de Estructuras, el Derecho Informático, el Delito Electrónico”, Autor: Dra. Luz Maria del Pozo y Contreras, Poder Legislativo Federal, Biblioteca del H. Congreso de la Unión, Guadalajara, Jalisco., Septiembre 1996.

http://www.jose_cuervo.lettera.net

Http: //www.jose cuervo.lettera.net, Pagina de José Cuervo Álvarez, “Delitos Informáticos Protección Penal de la Intimidad”, España, 29 de mayo de 1997.

www.vlex.com, Perú: el Bien Jurídico en el Delito Informático, Luís Miguel Reyna Alfaro, Doctrina-análisis y Artículos.

www.vlex.com.mx, México: El Derecho a la Intimidad y el Derecho a la Información: ¿Garantías encontradas?, Favio Rubén Troncazo Auld, Doctrina-análisis y artículos.

http://www.cddhcu.gob.mx/candip/foro/.

www.vlex.com.mx , Argentina.

http://www.monografias.com/trabajos6/delin/delin.shtm

www.vlex.com.mx, Argentina: "Presupuestos Para la Incriminación del Hacking", Autor Hugo Daniel Carrión. Buenos Aires, Argentina.

http://www.monografias.com/trabajos6/delin/delin.shtm, delitos informáticos y computacionales cuyos efectos se producen en el extranjero. (Bolivia).

www.vlex.com, España: "legislación al Respecto Sobre Delitos Informáticos", (Doctrina-artículos y análisis), Marcelo Manson, 07/06/2001.

LEGISGRAFIA

Código Penal Federal.

Código Penal Del Estado de Veracruz.