VNIVERSIDAD NACIONAL AVTNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

LICENCIATURA EN DERECHO

TRABAJO POR ESCRITO QUE PRESENTA:

ARMANDO BENITEZ MOLINA

TEMA DEL TRABAJO:

“PROPUESTA DEL DELITO DE ROBO INFORMÁTICO”

EN LA MODALIDAD DE “SEMINARIO DE TITULACIÓN COLECTIVA”

PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

MÉXICO, ARAGON, DICIEMBRE DE 2009

A MIS PADRES:

AGUSTIN BENITEZ FLORES Y ANDREA MOLINA PINEDA, con el profundo cariño y amor, por el gran esfuerzo de apoyo que hicieron para lograr la formación de mi profesión.

A MI HERMANO:

EDGAR BENITEZ MOLINA, por el soporte moral e impulsarme en mis estudios.

A MIS MAESTROS:

Le doy gracia a *LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, FES ARAGÓN* que fue mi segunda casa y maestros, que me impartieron los conocimientos adecuados en el transcurso de mi carrera.

ÍNDICE.

Pág.

CAPÍTULO III.
SUJETOS EN LA FIGURA DE ROBO INFORMÁTICO.

INTRODUCCIÓN.

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación; por tanto, abordar el estudio de las implicaciones de la informática en el fenómeno delictivo resulta una cuestión apasionante para quien observa el impacto de las nuevas tecnologías en el ámbito social; efectivamente, el desarrollo y masificación de las nuevas tecnologías de la información han dado lugar a cuestiones tales como el análisis de la insuficiencia del sistema jurídico actual para regular las nuevas posiciones, escenarios, en donde se debaten los problemas del uso y abuso de la actividad informática y su repercusión en el mundo contemporáneo; es por esta razón, que paralelamente al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamientos sin validez antes impensables y en algunos casos de difícil tipificación en las normas penales tradicionales. Donde tenemos a *la informática,* que estudia el tratamiento automatizado de las fuentes del conocimiento jurídico con sistemas de documentación legislativa, jurisprudencial y doctrinal, formando diariamente actividades en la humanidad y en el propio Estado, en el cual se realizan tareas sencillas hasta consultar información en base de datos permitidos, a través de nuevos medios informáticos que se conocen; es así, los delitos que tradicionalmente conocemos en el mundo se reproducen en el mundo virtual y cada vez lo vemos con más existencia y mayor rapidez.

Lo que se analiza en el Derecho Penal con referencia al fenómeno del *Delito Robo Informático* a diferentes tecnologías, modalidades delictivas que presenta en la informática y, aunado a ello la insuficiencia de la Legislación Penal actual; en la cual; plasma la figura de los accesos ilícitos a sistemas y equipos informáticos, donde se requiere un repaso de las situaciones y de las normas penales, tanto de la Legislación Penal como el Código procesal penal para constatar si las mismas se hayan en adelantos de la tecnología actual, nadie escapa de la enorme influencia que ha

alcanzado la informática en la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etcétera, son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática. Junto al avance de la tecnología informática y su dominio en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados de manera genérica *delitos informáticos;* debido a lo anterior, se desarrolla el presente documento que contiene una investigación sobre la temática de los delitos informáticos, de manera que al final pueda establecerse una relación con la auditoría informática. Para lograr una investigación completa de la asunto se establece la conceptualización respectiva del tema, generalidades asociadas al fenómeno sobre el robo informático, el efecto de éstos en diferentes áreas, como poder minimizar la amenaza de los delitos a través de la seguridad, aspectos de legislación informática y se busca unificar la investigación realizada para poder establecer el papel de informática frente a los delitos informáticos; tomando en cuenta, se hará desde un punto y enfoque dogmático, sugiriendo en cada caso las reformas que a nuestros juicios son necesarios para enfrentar el fenómeno del *delito* cometido con medios tecnológicos, ello implica no dejar de lado el aspecto criminológico, imprescindible a nuestro entender, para poder caracterizar en forma completa al fenómeno de la criminalidad informática.

Por ultimo, es difícil escoger un método como el ideal y único camino para realizar una investigación, pues muchos de ellos se complementan y relacionan entre si; a mi consideración los métodos mas completo son el deductivo, inductivo, comparativo, exegético, analítico y jurídico, ya que en estos se plantea una hipótesis que se puede basar en diferencias entre distintos campos de estudio, fundamentar los principios admitidos como ciertos, los cuales se proyectan la a practica jurídica, apoyándose en textos positivos, que se originen en la observancia de los fenómenos jurídicos para llegar a los principios que rigen una institución; en estas operaciones existen e independientes una de la otra, es tener análisis de un objeto que se realiza

a partir de la relación que existe entre los elementos que conforman dicho objeto como un todo; y a su vez , la síntesis se produce sobre la base de los resultados previos del análisis; es decir que se busca que la parte teórica no pierda su sentido, por ello la teoría se relaciona posteriormente con la realidad. Tomando en cuenta las características de estos métodos en esta investigación, que incluye otros métodos entrelazados con lo inductivo o el deductivo y el experimental, que también es opcional; es mencionar las fortalezas que denotan en cada uno de estos submétodos, finalmente la reunión de todas estas fortalezas conformaran los argumentos de mi elección sobre los métodos.

CAPÍTULO I.
EL DELITO.

1.1.- DELITO.

Crimen y delito son términos equivalentes, su diferencia radica en que delito es genérico y por crimen se entiende un delito más grave o específicamente un delito ofensivo en contra de las personas, tanto el delito como el crimen son categorías presentadas habitualmente como universales; sin embargo, los delitos y los crímenes son definidos por los distintos gobiernos que aplican su criterio en un territorio o en un intervalo de tiempo. La idea del delito toma su origen en la ley penal, entre la ley penal y el delito existe un nexo indisoluble, pues el delito es propiamente la violación de la ley penal o, para ser más exactos, la infracción de una orden o prohibición impuesta por la ley; en consecuencia, delito será todo hecho al cual el ordenamiento jurídico penal le adscribe como una pena impuesta por la autoridad judicial en medio de un proceso.[1]

En el delito para su existencia, deben de incidir dos sujetos: el sujeto activo y el pasivo, en ocasiones intervienen otros en conjunción con el activo, ya sea antes o después de la comisión o realización del delito, el sujeto activo del delito será toda persona que en términos generales infrinja la ley penal, ya sea por su propia voluntad o sin ella; es decir, el delito puede ser cometido por el sujeto activo con pleno conocimiento de la acción que va a realizar, esperando el resultado de ése o en caso contrario sin la voluntad de ese sujeto, cuando la acción que da origen al delito, no es deseada y se comete por imprudencia o sucede por un accidente; no obstante, este sujeto será el que realice la acción de la conducta o la omisión de la misma que están previstas y sancionadas por la ley penal. En el caso del sujeto pasivo del delito será toda persona que resienta el daño que ocasiona la comisión del delito, la consecuencia de la conducta delictiva, ya se trate de su persona en sus derechos o en sus bienes, quien se le afecta en su esfera personal de derechos e intereses.

[1] Cfr. http://www.monografias.com/trabajos35/el-delito/el-delito.shtml#nocion.

Por otro lado, el delito se perfecciona con una simple acción u omisión, haciendo abstracción de la verificación del resultado de lesión y de peligro según el objeto o fin que persiguen, la perturbación, daño, disminución o destrucción del bien jurídicamente protegido; en virtud, como toda definición del delito es siempre o casi el resultado de un silogismo que plantea el problema pero que nada nuevo descubre, señalar del delito que es un acto penado por la ley como lo dispone el Código Penal Federal en su artículo 7º y añadir que es la negación del derecho, supone hacer un juicio a *posteriori,* por eso es exacto, es una tautología (decir dos veces), institución que en materia penal están reguladas en el precepto invocado, que en lo conducente estatuye lo siguiente:

Articulo 7. "Delito es el acto u omisión que sancionan las leyes penales.

En los delitos de resultado material también será atribuible el resultado típico producido al que omita impedirlo, si éste tenía el deber jurídico de evitarlo. En estos casos se considerará que el resultado es consecuencia de una conducta omisiva, cuando se determine que el que omite impedirlo tenía el deber de actuar para ello, derivado de una ley, de un contrato o de su propio actuar precedente.

I. Instantáneo, cuando la consumación se agota en el mismo momento en que se han realizado todos sus elementos constitutivos;
II. Permanente o continuo, cuando la consumación se prolonga en el tiempo; y
III. Continuado, cuando con unidad propósito delictivo, pluralidad de conductas y unidad de sujeto pasivo, se viola el mismo precepto legal".

Por lo que respecta con la descripción el término delito, relacionándolo con la informática, computadoras, web, internet, se define como cualquier comportamiento antijurídico, no ético o no autorizado, respectivo con el robo procesado automático de datos y/o transmisiones 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. En la actualidad la informatización se ha implantado en casi todos los países, tanto en la organización y administración de empresas y administraciones públicas

como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente; pero junto a las incuestionables ventajas que presenta, comienzan a surgir algunas facetas, como por ejemplo, lo que ya se conoce como *criminalidad informática*.

1.2.- CONCEPTO JURÍDICO.

Es delito natural o social, la lesión de aquélla parte del sentido moral que consiste en los sentimientos altruistas fundamentales (piedad y probidad), según la medida media en que se encuentran en las razas humanas superiores, cuya medida es necesaria para la adaptación del individuo a la sociedad.[2] El delito debe ser, naturalmente formulada desde el punto de vista del Derecho, *Debe ser una fórmula simple y concisa, que lleve consigo lo material y lo formal del delito y permita un desarrollo conceptual por el estudio analítico de cada uno de los elementos;* en lugar de hablar de violación de la ley como una referencia formal de antijuricidad o concretarse a buscar los sentimientos o intereses protegidos que se vulneran como contenido material de aquella violación de la ley, podrá citarse simplemente la antijuricidad como elemento que lleve consigo sus dos aspectos, formal y material y dejando a un lado la voluntad como expresión formal y como criterio material sobre culpabilidad, tomar esta última como verdadero elemento del delito, a reserva de desarrollar por su análisis todos sus aspectos o especies.[3]

Se halla, que es la acción típica antijurídica, culpable, sometida a una adecuada sanción penal y que lleva las condiciones objetivas de penalidad; de lo anterior se deduce, que para ser delito se necesita reunir estos requisitos, acción descrita objetivamente por la ley decir, tipicidad, contraria al derecho; esto es, que exista antijuricidad dolosa o culposa; es hablar, que medie culpabilidad sancionada con una pena; o sea, que tenga fijada una penalidad y que se den las condiciones objetivas de punibilidad, es definir el

[2] Vid. http://www.derecho.unam.mx/papime/TeoriadelDelitoVol.II/uno.htm
[3] Vid. CASTELLANOS, Fernando. Lineamientos Elementales de Derecho Penal. 10ª ed. Editorial Porrúa México, 1976. Pág. 128.

delito como acontecimiento típico antijurídico e imputable, es emplea la palabra imputable en el amplio sentido de culpabilidad; en resultado, la definición nos ha sugerido la necesidad de intercalar un nuevo carácter de las infracciones penales, la imputabilidad en todo su esplendor corresponde a las partes del delincuente más que a la consagrada al delito, pero es indispensable aludir a ella en una construcción técnico-jurídica del crimen.

Sin embargo, existen diversas concepciones formales del delito, todas aquellas coinciden en que el delito es aquella conducta legalmente imputable; esto quiere decir que dicha acción se encuentra tipificada (descrita), en los distintos ordenamientos de la ley penal; *una vez, admitido como axioma inconcuso que sin la ley no hay delito y que las conductas que quedan fuera de las leyes son impunes, solo se puede asegurar lo que el delito es, interrogando la ley misma*.[4]

Aun más, la concepción formal del delito se considera la única posible por ser producto de la metodología del derecho, debido a que la acción punible, es aquella que se encuentra sancionando por las normas de derecho al prevalecer el método jurídico, aumento la tendencia a concebir la definición formal como única posible, pues las acciones punibles son las castigadas por la ley, en términos del axioma *nullum crimen nulla poena sine lege*; y a su vez cabe replicar tautologicamente que las acciones castigadas son las punibles, cayendo en una contradicción que no aporta solución alguna. Aunque existe una notable similitud entre una concepción formal de delito y el principio de legalidad nullum crimen nulla poena sine lege, el principal problema del concepto formal del delito consiste en la tarea de concretar el concepto de delito en los ordenamientos legales; aunado a ello, buscar una definición que atienda a toda clase de generalidad aun por encima de todos las concepciones que se tienen del Código Penal Federal.

---

[4] Ob. cit. MEDINA PEÑALOSA Sergio J. Teoría del Delito; Casualismo, Finalismo e Imputación objetiva, 2ª Ed. Editorial Ángel, México 2001, pag.29

Por ende, ésta noción entraña una referencia del concepto de delito sustancial con el principio de legalidad, cuya consecuencia más importante estriba en el hecho de someter el concepto de delito a la ley, en ese sentido expresa el código penal Federal, que el delito es el acto u omisión que castigan las normas penales, conjunto de comportamiento que sancionará las leyes penales, no están tipificadas por meros caprichos por parte de los legisladores y no son productos del azar o la casualidad, si no que son erigidos en un código penal con el objeto de defender los distintos valores éticos, morales y sociales del hombre en compañía de sus semejantes, a los cuales también se les puede llamar bienes jurídicos, éstos bienes deben de estar protegidos y las normas tipificadas en los distintos ordenamientos legales con la convicción de que de esa forma se va a asegurar la paz y la sana convivencia ciber-social, esta convicción se ve reforzada con la idea de una pena que impone el Estado mediante un intervención, aunque sea ejecutada por el Estado tiene sus limites punitivos, por esta razón se encuentran contenidas de forma escrita.

1.3.- EL ROBO INFORMÁTICO.

Podemos decir que es llamado como un robo ordinario, al que no se ejecuta con violencia física o moral, llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos mismos; relativamente, el lugar en que se cometa el delito se menciona, que se hace en el ciber-espacio, web, red, internet, que cierta cualidades tiene el ladrón.[5]

En otra palabras, son todos aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático, cibernético y tecnológico; ello implica, actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera, todos estos de origen

[5] Vid. http://www.portaley.com/delitos-informaticos/codigo-penal.shtml

informático; sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho, dado que la seguridad completa no existe al margen para un nuevo incidente de seguridad; por tanto, cuando éste se presenta, se verifica en un alto porcentaje que las organizaciones no se encuentran preparadas para enfrentar la realidad de una intrusión o incidente.

Es ahí, que el incidente representa un reto para demostrar la diligencia de su organización para enfrentar el hecho, tomar el control, recoger y analizar la evidencia y finalmente generar el reporte sobre lo ocurrido, que incluye las recomendaciones de seguridad hechas por la policía cibernética y conceptos sobre los hechos del incidente.

Hernández Guerrero define al Delito informático como, 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[6]; mientras tanto, Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y por las segundas actitudes ilícitas en que se tienen a las computadoras como instrumento o fin.

Como ya se señalo anteriormente, determinados enfoques doctrinales subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas de algún modo con los computadores; a esto señalo que el término Delito de robo Informático debe usarse en su forma plural, en atención a que se utiliza para designar una multiplicidad de conductas ilícitas y no una sola de carácter general, que se hable del delito informático cuando nos estemos refiriendo a una de estas modalidades en particular.

[6] Vid. HERNÁNDEZ GUERRERO, Francisco. Delitos Informáticos, Edición PDF/Adobe Acrobat, México 1997. Pág. 158.

1.4.- DERECHO INFORMÁTICO.

Ha sido analizado desde diversas perspectivas, por un lado el Derecho Informático se define como un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la Informática; por otro lado, hay definiciones que establecen que es una rama del derecho especializado en el tema de la informática sus usos y aplicaciones y sus implicaciones legales;[7] Por lo que es importante señalar la visión que considera que el Derecho Informático es un punto de inflexión del Derecho, puesto que todas las áreas del derecho se han visto afectadas por la aparición de la denominada Sociedad de la Información, cambiando de este modo los procesos sociales y por tanto los procesos políticos y jurídicos, es aquí donde hace su aparición el Derecho Informático, no tanto como una rama sino como un cambio.

Pero no es un término unívoco, pues también se han buscado una serie de términos para el Derecho Informático como: Derecho Telemático, Derecho de las Nuevas Tecnologías, Derecho de la Sociedad de la Información juscibernética, Derecho Tecnológico, Derecho del Ciberespacio, Derecho de Internet, etc.[8]

Es el sector normativo de los sistemas, dirigido a la regulación de las nuevas tecnologías de la información y la comunicación; es decir, la informática y la telemática también integran el derecho informático; por ende, los razonamientos de los teóricos del Derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática, la telemática, las fuentes y estructura temática del Derecho Informático y afectan las ramas del Derecho Tradicional; asimismo, se inscriben en el ámbito del Derecho Publico, el problema de la regulación del flujo internacional de datos informatizados, que interesa al derecho internacional público, la libertad informática o defensa de las libertades frente a eventuales agresiones perpetradas por las tecnologías de la información y

[7] Vid. TELLEZ VALDÉS, Julio. Los Delitos informáticos. ed. Adobe PDF, Editorial Mc Grill, México, 1998, pág, 103, 104.
[8] Cfr. http://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico

la comunicación, objeto de especial atención por parte del Derecho Constitucional y Administrativos o los delitos informáticos, que inciden directamente en el ámbito del Derecho Privado Penal actual.

Ese mismo carácter interdisciplinario o transversal que distingue al derecho informático, ha suscitado un debate teórico sobre si se trata de un sector de normas dispersas pertenecientes a diferentes disciplinas jurídicas o constituye un conjunto unitario de normas (fuentes), dirigidas a regular un objeto bien delimitado, que se enfoca desde una mitología propia, en cuyo supuesto entraría una disciplina jurídica autónoma.

Es indudable que si una computadora se presenta a modo de una herramienta muy favorable para la sociedad, también se puede constituir en un instrumento u objeto en la comisión de verdaderos actos ilícitos.[9] Este tipo de actitudes concebidas por el ciber-delincuente y no por la maquina como algunos pudieran suponer, encuentran sus orígenes desde el mismo surgimiento de la tecnología informática, ya que es lógico pensar que de no existir las computadoras estas acciones no existieran; por otra parte, la misma facilidad de labores que traen consigo dichos aparatos proporcionan que en un momento dado, el usuario se encuentre ante una situación de ocio, la cual canaliza a través de las computadoras, cometiendo una serie de ilícitos. Por el egoísmo humano se establece una especie de duelo entre el hombre y la maquina lo cual, en última existencia provoca el surgimiento de ilícitos, en su mayoría no intencionados por ese deseo del hombre de demostrar su prioridad frente a las maquinas y en este caso especifico las computadoras; de esta forma podemos decir que estas acciones, que más que resultado de una situación socioeconómica, se derivan de una actitud antro psíquica, aunque en el terreno de los hechos son una realidad sicológica bien determinada y que requiere de un tratamiento jurídico especifico.

[9] Op. Cit. TELLEZ VALDÉS, Julio. Derecho Informático. pág. 81.

Por lo antes expuesto, existen infinidades de sitios en el internet, ligas, enlaces externos, campos, donde se puede llevar a cabo algunos de los actos ilícitos, uno de ellos el *Robo Informático,* con el Esquema Basado en la División de Alfa-Redi, podemos ubicar tal como son:

Acceso a la información pública.
Administración de Justicia y Nuevas Tecnologías.
Banca y Dinero Digital.
Com.mx.
Net.com.
Censura en Internet. Libertad de Expresión *online.*
Comercio Electrónico.
Contratos Informáticos.
Compras públicas mediante el uso de las NTIC.
Correo electrónico.
Defensa del consumidor.
Delitos Informáticos.
Derecho en la Era Digital.
Derecho de las Telecomunicaciones.
Derecho Laboral e Informática. Teletrabajo.
Documento Electrónico, mensajes de datos, EDI y Factura Electrónica.
Editoriales online de Derecho.
E-government.
e-Learning del Derecho y Nuevas Tecnologías.
Firma Electrónica.
Hábeas data.
Impuestos e Internet.
Informática Jurídica.
Manifestación de la Voluntad por Medios Electrónicos.
Medidas Cautelares sobre Equipos Informáticos.
Nombres de Dominio y Direcciones IP.
Notas Bibliográficas y de Eventos.
Notificación por Medios Electrónicos.
Privacidad en Soportes Lógicos.
Profesionales del Derecho en la Era Digital.
Propiedad Intelectual y Propiedad Industrial e Internet.
Programas: Software Jurídico. Bases de datos y Gestión de Bufetes.
Protección de Datos de Carácter Personal.
Publicidad e Internet.
Relación entre el Derecho y la Informática.
Seguridades informáticas.
Sociedad Civil e Internet
Sociedad de la Información.
Software libre .
Telefonía y Voz sobre IP.
Wireless Application Prototocol (WAP).

En propuesta, la informática puede ser el objeto del ataque o el medio para cometer otros delitos, independientemente del robo informático que reúnan características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas en el internet, e- mail), básicamente de la gran cantidad de datos que se acumulan con la consiguiente facilidad de acceso a ellos y relativamente fácil manipulación de esos datos, 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 más allá del valor material de los objetos destruidos, a ello se une ataques que 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 sin ser descubiertos.

El estudio de los distintos métodos de destrucción y/o violación del hardware y software es necesario en orden a determinar cuál será la dirección que deberá seguir la protección jurídica de los sistemas informáticos, ya que sólo conociendo el mecanismo de estos métodos es posible encontrar las similitudes y diferencias que existen entre ellos, de este modo se pueden conocer los problemas que es necesario soslayar para conseguir una protección jurídica eficaz sin caer en el casuismo; en consecuencia, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva legislación penal federal 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 formas tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas y, si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado; se comprenderá

que están en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

CAPÍTULO II.
ELEMENTOS ESENCIALES DEL DELITO (POSITIVOS Y NEGATIVOS).

2.1.- CONDUCTA.

Es el primer elemento básico del delito y se define como el comportamiento humano voluntario positivo o negativo, encaminado a un propósito, lo que significa que sólo los seres humanos pueden cometer conductas positivas o negativas, ya sea por actividad o inactividad respectivamente, es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito ya que tiene una finalidad al realizarse la acción u omisión.

En otro orden, es el actuación humana positiva o negativa que produce un resultado en donde da una acción que consiste en una actividad, en un hacer, mientras la omisión es una inactividad, es cuando la ley espera una conducta de un individuo y éste deja de hacerla.[1] Se dice que acción se define como aquella actividad que realiza el sujeto, produciendo consecuencias en el mundo jurídico, en dicha acción debe de darse un movimiento por parte del sujeto, de esta manera, la conducta de acción tiene tres cosa, Movimiento, resultado y la relación de causalidad.

Por ende, la acción en sentido estricto es la actividad voluntaria realizada por el sujeto, consta de un elemento físico y de un elemento psíquico, el primero es el movimiento y el segundo la voluntad del sujeto, esta actividad voluntaria produce un resultado y existe un nexo causal entre la conducta y el resultado. Dicho resultado de la acción debe ser sancionado por la ley penal; esto es, deberá configurar un delito descrito y penado en la ley, será intrascendente que lesione intereses jurídicos protegidos por la ley o sólo los ponga en peligro según el tipo penal.

Como lo señala nuestro Derecho Positivo Mexicano, en el Código Penal en su artículo séptimo, el delito es el acto u omisión que sancionan las

[1] Vid. PALOMAR DE MIGUEL, Juan. Diccionario para Juristas. Tomo I. 2ª ed. Editorial Porrúa México, 2003. Pag. 351.

leyes penales, de donde se desprende el elemento conducta pudiéndose presentar como una acción u omisión.

Así pues, la omisión es la inactividad voluntaria cuando existe el deber jurídico de obrar; que si lo llevamos a la adecuación del robo informático, donde se lleva a cabo el acto u omisión por medio de un computador tiene estos cuatro puntos:

a) Manifestación de la voluntad.
b) Una conducta pasiva.
c) Deber jurídico de obrar.
d) Resultado típico jurídico.

Por tanto, los delitos se clasifican en delitos de omisión simple o propios y delitos de comisión por omisión o impropios, respondiendo a la naturaleza de la norma, los primeros consisten en omitir la ley, violan una preceptiva, mientras los segundos en realizar la omisión con un resultado prohibido por la ley, los primeros no produce un resultado material, los segundos sí.[2]

Por consecuencia, los delitos de simple omisión, violan una norma preceptiva penal, mientras en los de comisión por omisión se viola una norma preceptiva penal o de otra rama del derecho y una norma prohibitiva penal[3]; mientras que los delitos de omisión simple producen un resultado típico y los de comisión por omisión un resultado típico y uno material.

En conclusión, los delitos de omisión simple, se sanciona la omisión y en los de comisión por omisión, no se sanciona la omisión en sí, sino el resultado producido; ahora bien, el aspecto negativo de la conducta es la ausencia de conducta, la cual abarca la ausencia de acción o de omisión de la misma, en la realización de un ilícito. Nuestro Derecho Positivo Mexicano, en el artículo 15 del Código Penal Federal, en su fracción primera, determina como causa de exclusión del delito: "el hecho se realice sin intervención de la

[2] Vid. GONZÁLEZ DE LA VEGA, Francisco. Derecho penal mexicano. 14ª ed. Editorial, Porrúa, México 1977. Pág. 166
[3] Ibid. Pág. 185

voluntad del agente", esto es la afirmación de que no puede constituir una conducta delictiva cuando no se presenta la voluntad del agente. El artículo 12 del Código Penal del Estado, menciona como causas excluyentes de incriminación, en su facción I "el violar la ley penal por fuerza física irresistible o cuando haya ausencia de voluntad del agente…".

2.2.- TIPICIDAD.

Es toda conducta que conlleva una acción u omisión que se ajusta a los presupuestos detalladamente establecidos como delito o falta dentro de un cuerpo legal; nos referimos, para que una conducta sea típica debe constar específica y detalladamente como delito o falta dentro de un código[4].

En virtud que en algunos países que adoptan un derecho penal moderno, no es aplicable la analogía, por lo tanto, la conducta debe ser específicamente detallada en la orientación teleológico funcionalista del Derecho penal fundamentada en la prevención general positiva, se extraen importantes consecuencias para toda la Teoría General del delito, resultados que a partir de la norma primaria considerada como norma de conducta y de la subsiguiente introducción en el concepto de la acción supone la revisión de conceptos tradicionales e incluso de toda la estructura del concepto de delito, pero conservando todavía los elementos tradicionales de tipicidad, antijuridicidad (o tipo de injusto) y culpabilidad y, cuando se intenta romper con dicha estructura no acaba de configurarse algo realmente distinto, sino más bien un aglomerado en el que elementos propios de la culpabilidad vuelven a formar parte del concepto de acción que tiende a engullir la tipicidad y la antijuridicidad para volver a un concepto de delito sintético como la acción culpable.

Efectivamente, en nuestra sociedad actual, surgen nuevas situaciones que exigen respuestas cada vez más valorativas y normativizada (jurídicas, convencionales), los riesgos como expresión normativa del conflicto social

[4] Vid. http://es.wikipedia.org/wiki/Tipicidad

implica una nueva concepción del bien jurídico como criterio de solución al conflicto resuelto en la pauta de conducta contenida en la norma primaria.

En resumen, es la adecuación de la acción que hace el legislador tutelando una norma de cultura y previendo una sanción, con elementos normales de naturaleza descriptiva, referencias a personas, cosas y modos de obrar, refiriéndose a determinar el propósito o fin de la acción o a un ánimo específico con que debe cometerse, lo cual, hacen referencia a un juicio de valor remitiendo a otras disposiciones del ordenamiento jurídico (ajenidad en el robo) u obligan al juez a hacer un juicio de valor.

2.3.- ANTIJURICIDAD.

Es elemento esencial para la existencia de los tipos penales y subsecuentemente para la posibilidad de la existencia del delito ya que la acción delictiva no viola la ley la cual es meramente prescriptiva, sino que se ajusta a ella (tipicidad), lo que resulta violado es la norma de cultura que el legislador reconoce a través de la tipificación. El Derecho es un orden prominentemente normativo y cultural; entendiendo por cultura, de un interés común y de la situación que resulta de tal cuidado, situación que siempre está vinculada a un valor, a través de las normas de cultura ordena y prohíbe ciertas acciones correspondiendo a sus intereses valorativos y sólo cuando el Estado las privilegia con su tutela al reconocerlas en la ley, adquieren el rango de jurídicas.[5]

Aunado a formal y material, el primero nos estriba en la colisión que se da entre la acción delictiva y la norma de cultura legislada, una acción es formalmente antijurídica, cuando infringe una norma que el Estado ha incorporado al orden jurídico y el segundo, a la protección de bienes jurídicos, la acción será sustancialmente antijurídica sólo cuando lesione, ponga en peligro o sea idónea para poner en peligro un bien jurídico.

[5] Vid. http://www.tribunalmmm.gob.mx/bibliotyeca/almadelia/Cop2.htm

Aun más, la simple adecuación de una acción a un tipo legal, no comporta la afirmación de su carácter antijurídico, es necesario que se compruebe la ausencia de toda causa de justificación, por lo que es de matizar la afirmación de que la tipicidad no es sino un indicio de antijuricidad, en el sentido de que también es un fundamento, porque un acto antijurídico es penalmente relevante sólo cuando se adecua a un tipo legal, correcto es decir que esto último no prueba el carácter antijurídico del acto, ya que puede presentarse alguna causa de justificación[6].

2.4.- IMPUTABILIDAD.

Para poder hacer un juicio de reproche sobre una persona que ha cometido una acción antijurídica y típica, es necesario atribuírselo mediante el análisis de su posibilidad de comprenderla; en esto, se han detenido los teóricos para establecer si el sujeto tiene libre albedrío y por lo tanto hay que distinguir entre imputables e inimputables o si, por el contrario, todos estamos determinados y somos en todo caso socialmente responsables. Este es el problema de la imputabilidad, la cual es innegable cuando se ha esclarecido que hay factores de la conciencia y la inconsciencia que intervienen en la comisión de un delito.[7]

El incapaz, realizador del hecho descripto en el tipo no es considerado desde el punto de vista de si actuó con dolo o culpa, entre la plena salud mental o la consciencia plena que sustentan la imputabilidad y la locura o la inconsciencia que la excluyen es simplemente inimputable, existiendo grados que se da en imputabilidad disminuida frente al estado peligroso como conceptos contradictorios en función de la punibilidad, si se atiende a la imputabilidad atenuada, la responsabilidad y la pena se deben atenuar, pero si se toma en cuenta a la peligrosidad, frente al llamado *delincuente ciber-espacioso peligroso* no es correcto disminuir la pena en atención de la defensa del orden público, pues resulta más peligroso.

[6] Vid. http://www.unifr.ch/ddp1/derechopenal/obras/mdp/mdpdel4.htm#92
[7] Vid. http://www.comceoccte.org.mx/images/boletines/ponencia%20delitos%20fiscales.ppt

Por otro lado, la ausencia de imputabilidad (inimputabilidad), es cuando falta el desarrollo de la salud mental o cuando se presentan trastornos transitorios en las facultades mentales, el sujeto no es capaz de conocer el deber jurídico ni de querer las consecuencias de su violación; por lo tanto, es inimputable por:

1. Minoría de edad.- Al considerar que no se ha desarrollado su mente.
2. Enajenación.- Cuando la enfermedad de la mente o el estado de inconsciencia, privan de la consciencia de cometer un delito o de obrar conforme a Derecho.
3. Estados de inconsciencia.- Por el empleo de sustancias tóxicas, embriagantes o estupefacientes por toxico-infecciones o por trastornos mentales.

En concreto, tenemos que es la capacidad de una persona para ser alcanzada por la aplicación del Derecho penal, es lo que determina si es necesario seguir adelante con el estudio de su conducta para llegar a una definición de su suerte final con respecto a su punibilidad, ello acorde con pensar en la imputabilidad como un elemento exigible para poder analizar a otros necesarios que lleven a considerar el hecho como reprimible penalmente, tenida como requisito ineludible, su falta o inimputabilidad cerraría todo el proceso de averiguación de la culpabilidad y la imposibilidad de aplicación de la pena, careciendo de capacidad penal no es posible la actuación de la ley penal castigadora, aunque sí lo es la aplicación de una medida de seguridad.

2.5.- CULPABILIDAD.

Se lleva a cavo, cuando el sujeto imputable consiguiendo haber cometido el delito movido por la voluntad, consiente de ejecutar la acción que estaba tipificada o causarlo por imprudencia o negligencia, de esto depende el reproche que se le haga y la pena que se le imponga, estando ante la culpabilidad que nos lleva al resultado del juicio de valor que da origen al reproche, el sujeto de la acción delictiva por la relación psicológica entre él y

su resultado, siempre que en la misma fuere posible exigírsele proceder conforme a las normas.[8]

En otro orden de ideas, el autor de un hecho calificado como delito es estudiada y valorizada por la culpabilidad como otro elemento integrante, actuando dolosa o culposamente, que se encuentre frente a tales circunstancias anímicas; con respecto a su acción, ésta aparece como expresión jurídicamente desaprobada de su personalidad.

En la culpabilidad deben apreciarse los aspectos síquicos y valorativos de la conducta humana y la diferencia entre el dolo y la culpa, considerados de manera amplia estaría entre lo querido y lo no querido; por lo cual, en el dolo el hecho ilícito que es querido por su autor, con su resultado dañoso y en la culpa, aunque no querido, también es punible su autor. Actúa dolosamente quien sabe lo que hace; Según Luis Jiménez de Asúa, la acción dolosa hace suponer en su autor el conocimiento y dominio previo del acontecer causal y por ello el dominio de los hechos en el caso concreto y en la culpa consiste en la representación de un resultado típicamente antijurídico que se confía en evitar, obrando.

Empero, para que pueda afirmarse que un sujeto es culpable, se hace preciso que un hecho por él cometido sea valorado por el derecho como algo ilícito y que el sujeto que lo comete participe de ese orden jurídico como sujeto capaz y haya definido el significado de su acción como negación; por lo que hace al conocimiento y previsión de un resultado que se sabe injusto, así como la contemplación de las consecuencias objetivas de la acción se tiene en directo e indirecto el primero, que el resultado coincide con el que se propuso el sujeto activo y el segundo, cuando el agente se propone el fin delictivo, sabe que con certeza causará otros tales como:

- EVENTUAL: Se prevén posibles resultados antijurídicos colaterales al fin propuesto, que no se quieren.

[8]Vid. JIMÉNEZ DE ASÚA, Luis. Lecciones de Derecho Penal. Tomo III, Editorial Oxford México, 2003. Pág. 235.

- EMOCIONAL: Voluntad viciada de causar el resultado.

Al estar fundada la culpabilidad en la posibilidad de hacer un reproche al autor de una acción antijurídica y típica siendo imputable, cuando dicha acción está irregularmente motivada porque el sujeto estaba en el invencible error de actuar conforme a Derecho o por hallarse en una especial situación de necesidad o por la presencia de algún otro, motivo suficiente para poder exigírsele una acción conforme al ordenamiento jurídico; por faltar en el agente, el conocimiento o la voluntad que serían el motivo del juicio en que consiste la culpabilidad, si faltará este elemento será incriminable.

Resumiendo, el principio de la culpabilidad como uno de los más complicados para su definición, el cual, se le relaciona y se le incluye como elemento de este principio con la responsabilidad, que son las condiciones que se dan para atribuir a quien de manera voluntaria ejecuta un hecho punible.

De manera, que si tomamos encuentra todos los conceptos antes mencionados, llegamos a la conclusión de que la culpabilidad, *es la perdida del valor de un culpable (juicio de valor sobre el autor, que trae como consecuencia una acción criminal, conciencia de la antijuricidad de la acción por parte del autor, en la cual se incluye su responsabilidad.*

2.6.- PUNIBILIDAD.

A pesar de que muchos autores consideran a la punibilidad simplemente como consecuencia del delito, excluyéndola de entre los elementos que la integran, parecen confundir a la pena verdadera consecuencia del delito y pretensión del Derecho Penal, pero la punibilidad es un concepto abstracto que caracteriza a la acción delictiva y constituye en efecto un elemento del delito, la pena es el contenido de la pretensión punitiva del Estado, mientras que la acción punible es su presupuesto.

Para que sea incriminable la acción antijurídica y típica realizada por un sujeto imputable, ha de estar acompañada por la amenaza legal de la

imposición de una pena, esta culminación prevista en la ley; en virtud, la cualidad de punible, es decir aquella conducta a la que se tiene la posibilidad de aplicar una pena (dependiendo de ciertas circunstancias), en el terreno de la coerción materialmente penal, no es una característica del delito sino el resultado de la existencia de una conducta típica, antijurídica y culpable que cumple determinadas condiciones; tocante a la punibilidad, tiene dos sentidos primero, puede significar merecimiento de pena, en este sentido todo delito es punible y segundo, también puede significar posibilidad de aplicar penas, en esta vista no a cualquier delito se le puede aplicar pena.

Por lo que hace a las medidas de seguridad, tradicionalmente sólo era concebible que la consecuencia fuera una pena; es mencionar, un mal jurídicamente infringido al autor del delito como manifestación del reproche social, con una finalidad ya sea retributiva (se aplica el mal que se merece), intimidatoria (al implicar sufrimiento la finalidad de la pena es evitar los delitos por medio del temor) o de enmienda (la finalidad es mejorar al reo para que no reincida al reinsertarlo a sociedad); sin embargo, con el surgimiento de la idea de la peligrosidad como elemento para determinar la imposición de una consecuencia jurídica al infractor de una norma penalmente protegida y de la defensa social surgieron las medidas de seguridad aplicables a los delincuentes anormales (las curativas a los alienados o las reeducativas a los menores) o a los normales señaladamente peligrosos (las eliminatorias a los habituales), como complementos de la pena en la búsqueda de la prevención y represión del delito.

En la punibilidad, en algunos casos el legislador además de la realización de una acción determinada con que se viola la norma de cultura, hace depender la aplicación de la pena de la presencia de circunstancias extrínsecas e independientes del acto punible; tambien, se haya medidas de seguridad como lo son las pecuniarias, van en perjuicio del patrimonio del delincuente y puede ser la multa (obligación de entregar al Estado una cantidad de dinero legalmente determinada o determinable generalmente establecida para los delitos cometidos por personas que gozan de cierta fortuna o como sustitución a las penas privativas de libertad cortas), la

reparación del daño (atento al derecho de la víctima a que el daño que se le causó le sea resarcido, restituyendo la cosa o pagando su precio si aquel fue material o indemnizando si fue de naturaleza moral teniendo aquí cabida también la publicación especial de sentencia) o la pérdida de los instrumentos del delito, confiscación o destrucción de cosas peligrosas.[9]

2.6.1.- FALTA DE ACCIÓN.

Si la falta de algunos de los elementos esenciales del delito, éste no se integrará; en consecuencia, si la conducta esta ausente, evidentemente no habrá delito a pesar de las apariencias, pues la ausencia de conducta uno de los aspectos negativos o mejor dicho, impeditivos de la formación de la figura delictiva,[10] por ser la actuación humana, positiva o negativa, la base indispensable del delito como de todo problema jurídico, una de las causas de la integración del delito por alejamiento de conducta fuerza física exterior a lo que se refiere el artículo 15 del Código Penal Federal.

2.6.2 AUSENCIA DE TIPO.

Esta se constituye en el aspecto negativo de la tipicidad, es un impedimento de la integración del delito, mas no equivale a la ausencia del tipo. Hay atipicidad, cuando el comportamiento humano es correcto, previsto legalmente en forma abstracta, no encuentra perfecta adecuación en el precepto por estar ausente alguno o algunos de los requisitos constitutivos del tipo, es la ausencia de adecuación típica.[11]

Seguido su curso, cuando no se integran todos los elementos descritos en el tipo legal, se presenta el aspecto negativo del delito llamado atipicidad; en esencia, es la abandono de adecuación de la conducta al tipo, si la conducta no es típica jamás podrá ser delictuosa, cual suele distinguirse entre ausencia del tipo y de Tipicidad, se presenta cuando el legislador,

[9] Vid. http://www.derecho.unam.mx/papime/TeoriadelDelitoVol.II/cinco.htm
[10] Cfr. CASTELLANOS, Fernando. Lineamientos Elementales de Derecho Penal 10ª ed. Editorial Porrúa México, 1976. Pág.162,
[11] Vid. http://www.universidadabierta.edu.mx/Biblio/V/Velazquez%20Julio-Homicidio.htm

deliberada o inadvertidamente no describe una conducta, que según el sentir general, debería ser incluida en el catalogo de los delitos. [12]

2.6.3-. CAUSAS DE JUSTIFICACIÓN.

Todas las causas de justificación confieren un derecho para obrar, otorgan un permiso, sea dejando sin efecto una prohibición o liberando del cumplimiento de un mandato, pueden ser, Error de Prohibición; Concurre cuando el sujeto, pese a conocer completamente la situación o supuesto de hecho injusto, no sabe que su actuación no está permitida, no pertenece para nada a la tipicidad ni se vincula con ella, sino que es un puro problema de culpabilidad; cuando es invencible con la debida diligencia el sujeto no hubiese podido comprender la antijuricidad de su injusto, tiene el efecto de eliminar la culpabilidad; cuando es vencible, para nada afecta a la tipicidad dolosa o culposa que ya está afirmada al nivel correspondiente, teniendo sólo el efecto de disminuir la culpabilidad, lo que se traduce a la cuantía de la pena, que puede disminuirse hasta donde la ley autoriza. La diferencia entre error de tipo y de prohibición reside en que en el primero, el sujeto cree que hace otra cosa; en el segundo, sabe lo que hace, pero no puede motivarse según la norma porque carece de elementos que le posibiliten la comprensión.

Por lo que hace a lo anterior, la causa de justificación es cuando a un hecho presumiblemente delictuoso falta la antijuricidad; podemos manifestar, que no hay delito por la existencia de una causa de justificación, es decir el individuo ha actuado en determinada forma sin la intención de transgredir las normas penales establecidas; de esta manera, que no se le podrá exigir responsabilidad alguna ya sea penal o civil, por que aquella persona que actúa conforme a derecho, no puede lesionar ningún bien jurídico.

2.6.4.- INCULPABILIDAD.

Elemento negativo de la culpabilidad, que se da cuando asisten determinadas causas o circunstancias extrañas a la capacidad de conocer y

[12] Vid. www.comceoccte.org.mx/images/boletines/Ponencia%20delitos%20fiscales.ppt

querer, en la ejecución de un hecho realizado por un sujeto imputable en el cual, opera cuando falta alguno de los elementos esenciales de la culpabilidad, ya sea el conocimiento o la voluntad, tampoco será culpable una conducta si falta alguno de los otros elementos del delito o de la imputabilidad del sujeto. Porque si el delito integra un todo, sólo existirá mediante la unión de todos los elementos constitutivos de su esencia.[13]

En consecuencia, cuando se presenta la inculpabilidad el sujeto no puede ser sancionado, ya que para que exista el delito se necesita la presencia de sus cuatro elementos; primero, se efectúe la conducta; segundo, haya tipicidad, que se adecue la conducta a un tipo penal; tercero, el acto sea antijurídico y por último esta sea culpable.

2.6.5.- EXCUSAS ABSOLUTORIAS.

Aunque una acción u omisión sea típica, antijurídica y culpable, no se castiga cuando concurre una excusa absolutoria. Las excusas absolutorias obedecen al igual que las Condiciones Objetivas Punibles a consideraciones de política criminal, de conveniencia u oportunidad, un ejemplo es el art. 68 del Código Penal Federal Vigente, que establece excusa absolutoria por los delitos contra el patrimonio que cometieran entre sí, siempre que no concurra violencia o intimidación.[14]

Son condiciones objetivas de la punibilidad pero redactadas de forma negativa, decir con causa de exclusión de la pena, aunque concurra un hecho típico, antijurídico y culpable, no se impone sanción si hay una cláusula que impida la punibilidad, si existe una excusa absolutoria para ese caso; en consecuencia, el sujeto no será responsable penalmente.

Estas no se apoyan en que el acto sea en sí mismo legítimo, como sucede en las causas de justificación, ni tampoco en que no aparezca un sujeto en condiciones de capacidad para responder como acontece en las

[13]Vid. http://www.universidadabierta.edu.mx/Biblio/V/Velazquez%20Julio-Homicidio.htm
[14] Vid. http://html.rincondelvago.com/punibilidad.html

causas de no imputabilidad, sino mas bien aparece fundada en motivos transitorios y de convivencia. Considera el legislador, más útil tolerar el delito que castigarle aún conociendo que existe delito y que hay personas que de él pueden responder estas son auténticas condiciones personales capaces de excluir la aplicación efectiva de la pena frente a un hecho típico antijurídico y culpable por razones de conveniencia político criminal.

En concreto, la diferencia radica en la naturaleza del factor condicionante, que en las excusas son siempre motivos de índole personal como de parentesco, carácter personal, de estas aparece como un criterio cierto para diferenciarlas de las condiciones objetivas de punibilidad, constituyen un núcleo relativamente reducido que surgen en relación a la materia misma del injusto, en consideraciones ligadas a los desvalores del acto y del resultado.

CAPÍTULO III.
SUJETOS EN LA FIGURA DE ROBO INFORMÁTICO.

En el estudio teórico en el delito de robo informático que se encuentra dentro de los delito informático y ante el volumen de definiciones que se han venido planteando, la intención inicial es lograr una explicación que se mantenga dentro de los cánones y principios establecidos por del Derecho Penal, informático, a la vista de que no todas ellas se ajustan de manera correcta, la mayoría de autores que han tratado el tema los han descrito; *todos aquellos en que una computadora es utilizada como medio o como fin para la comisión de una acción típica*, en una primera aproximación lo ideal es ver en qué punto esta definición se mantiene dentro de las bases preestablecidas por el Derecho Penal.

En este punto, el bien jurídico que se protege es la integridad física y lógica de los equipos informáticos en su caso y la capacidad de transmisión o recepción y el procesamiento a distancia en el otro, es absolutamente necesario en el primero que el sujeto pasivo cuente con un equipo informático y en el segundo, que este equipo tenga la posibilidad de conectarse a redes a fin de operar el teleprocesamiento. Como por regla general hoy en día todos los equipos cuentan con esta capacidad, a través del uso de módem o de tarjeta red, podemos decir que, al menos una gran mayoría de los posibles sujetos pasivos del primer grupo lo son también del segundo, razón por la cual, las similitudes que une a ambos grupos.[1]

Como sabemos algunas Legislaciones en México han recogido una parte de los tipos penales que nos ocupan pero en contrapartida, en la mayoría de los casos han dejado la cuestión probatoria en materia de pruebas electrónicas sin modificaciones que permitan una correcta persecución de estas conductas.

[1] Cfr. CAMPOLI, Gabriel. Delitos Informáticos en la Legislación Mexicana. Editorial INACIPE. México, 2005 Pág. 61

3.1.- SUJETO ACTIVO Y PASIVO.

El sujeto activo del delito será toda persona que, en términos generales infrinja la ley penal, ya sea por su propia voluntad o sin ella; es decir, el delito puede ser cometido, por el sujeto activo, con pleno conocimiento de la acción que va a realizar, esperando el resultado de ése o en caso contrario, sin la voluntad de ese sujeto, cuando la acción que da origen al delito no es deseada y se comete por imprudencia o sucede por un accidente, este sujeto será el que realice la acción de la conducta o la omisión de la misma que están previstas y sancionadas por la ley penal.

En el caso del sujeto pasivo del delito, éste será toda persona que resienta el daño que ocasiona la comisión del delito, la consecuencia de la conducta delictiva ya se trate de su persona en sus derechos o en sus bienes, persona a quien se le afecta en su esfera personal de derechos e intereses; muchas de las personas que cometen los delitos informáticos o electrónicos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible, en casos la motivación del delito de robo informático no es económica sino que se relaciona con el deseo de ejercitar y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.[2]

El sujeto pasivo en el caso del robo informáticos, pueden ser individuos, instituciones crediticias, órganos estatales, que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos; para la labor de prevención de estos delitos es importante el aporte de los dominios públicos que puede ayudar en la determinación del *modus operandi*, esto es de las maniobras usadas por los delincuentes informáticos.

[2] Vid. http://www.jalisco.gob.mx/PoliciaCibernetica.nsf/CapturaProtegeteWeb?OpenForm

En resumen aquellos individuos que poseen ciertas características que no presentan el denominador común de los delincuentes; esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible o bien son hábiles en el uso de los sistemas informatizados, aún cuando en muchos de los casos no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos; de esta forma, la persona que entra en un sistema Informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes; en consiguiente, el nivel típico de aptitudes del delincuente Informático es tema de controversia ya que para algunos dicho nivel no es indicador de delincuencia informática, en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Tocante al sujeto pasivo o víctima del delito, tenemos que distinguir es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo y en el caso de los delitos informáticos, mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi.

3.2.- OBJETO DEL DELITO

Desde luego, la naturaleza y tipo de delito de que se trate influirá en la calidad, tipo y numero de los sujetos activos y las consecuencias de eso son los pasivos; por otra parte, el objeto del delito es muy importante no solamente en la teoría del mismo, sino para la existencia y vida del mismo, incluyendo su comisión o realización; esto es, el objeto jurídico del delito es el bien protegido por el derecho y que precisamente por esa razón se

denomina bien jurídico, es decir el quid de la norma, con la amenaza de la sanción, trata de proteger contra posibles agresiones.

A mayor abundamiento, el objeto del delito es sobre lo que debe recaer la acción del agente según la descripción legal respectiva y por otra parte, el bien tutelado por las particulares normas penales y ofendidas por el delito, de tal enunció aparecen dos conceptos completamente diferentes, el de objeto material y el de objeto jurídico del delito que solo coinciden cuando la ofensa de un bien tutelado por el derecho penal consiste en la modificación de aquello sobre lo cual precisamente se verifica el resultado.

Por ende, el objeto material del delito éste puede ser la formulación que antecede, que la descripción legal respectiva tiene por tal de donde se infiere que no constituye objeto material; en sentido jurídico, las cosas materiales con que se cometió el delito o constituyen su producto o son huellas de su perpetración, pues ellas conciernen al episodio delictivo concreto y no a su abstracta previsión legal; entonces, el objeto material del delito puede ser tanto una persona como una cosa. El estado protege determinados bienes porque ello es necesario para asegurar las condiciones de la vida en común, el resguardar el interés en la observancia de los preceptos legales, se preserva por la norma penal, el derecho del particular ya que no puede considerarse lógicamente que la norma Jurídica o sea, el objeto de la protección, pues la norma no puede proteger el interés en la protección, ser en definitiva, no puede protegerse así misma.

Por lo antes expuesto, se conviene que el bien jurídico penalmente protegido que el delito ofende, es una relación entre personas y cosas; entre estos bienes hay algunos que, por ser vitales para la colectividad y el individuo, reciben protección jurídica por su significación social y a los cuales el derecho acuerda su especial tutela erigiendo en tipos delictivos algunas formas especialmente criminosas de atentar contra ellos, por tanto, como

objetos de interés jurídico vienen a constituir el objeto jurídico que se halla tras cada delito[3].

El robo informático es un hecho jurídico tiene importancia jurídica, por cuanto el derecho le atribuye consecuencias jurídicas, el nacimiento de derechos para el agraviado y para el Estado, como el persecutor de los delitos y pérdida de derechos para el delincuente; como el delito es un hecho jurídico voluntario, supone que él es ante todo un hecho humano y no un hecho natural, es una acción, un obrar con efectos comprobables en el mundo exterior y no una simple declaración de voluntad y es además, una acción voluntaria y consciente y por tanto imputable, referible al sujeto activo como suya.

3.3.- OTROS SUJETOS.

En la sociedad informatizada en nuestro país se pretende alcanzar una gran mayoría de los quehaceres de nuestra vida cotidiana que se encuentra relacionado con la informática, desde su centro laboral, su tarjeta de crédito, su correo electrónico, sus datos personales fichados en los registros y archivos nacionales, en la actividad tributaria, entre otros; las ventajas que ofrece el empleo de esta nueva tecnología en la optimización de los servicios que se brinden en estas esferas mencionadas y en muchas mas son incuestionables, pero como casi todo tiene su lado oscuro, nuestra posición en estas tecnologías es neutral en un porciento mayoritario comparado con aquellos que se dedican por razones laborales o de entretenimiento a hacer robos, modificaciones constantes en dichos sistemas computarizados, por lo que estamos expensas a ser víctima de las acciones antijurídicas que se lleven contra estos medios informáticos, los cuales pueden ser manejados o plenamente afectados quiénes pretenden saciar necesidades con su uso. Esta dimensión transgresora y abusiva del empleo de las nuevas tecnologías, debe ser enfrentada por el Derecho

[3] Cfr. REYNOSO DÁVILA, Roberto, Teoría General del Delito, 6ª ed. Editorial Porrúa, México, 2006, pág.25

Penal como disciplina garante de la convivencia pacifica e instrumento ultimo de control social; así que, estamos en presencia de una acción u omisión socialmente peligrosa prohibida por ley bajo la conminación de una sanción penal a la que es considerada delito informático, pues de forma expresa se manifiesta como la acción típica, antijurídica y dolosa cometido mediante el uso normal de la informática o sea, un elemento informático o telemático contra el soporte lógico o software de un sistema de tratamiento autorizado de la información.

Al igual que en el resto de los delitos existen otro sujetos activos, estamos hablando de delincuentes peligrosos comunes, el hecho de que sean considerados activos, el delincuente común está determinado por el mecanismo y medio de acción que utilice para llevar producir el daño, quiénes en la mayoría de los supuestos en que se manifiestan y las funciones que desempeñan pueden ser catalogados sujetos especiales; el reconocimiento de varios tipos de conductas antijurídicas que puede manifestar los sujetos, expresadas en el presente capítulo, es preciso para conocer las posibles formas de comisión delictiva y obviamente profundizar en las posibles formas de prevención y detención de estas conductas.

3.3.1.- HACKER.

Es una persona muy interesada en el funcionamiento de sistemas operativos, curioso que simplemente le gusta husmear por todas partes, llegar a conocer el funcionamiento de cualquier sistema informático mejor que quiénes lo inventaron; esa palabra es un término ingles que caracteriza al delincuente silencioso o tecnológico, son capaces de crear sus propios softwares para entrar a los sistemas, tomando su actividad como un reto intelectual[4].

Esta visión de ellos se ajusta a la realidad, que hay una fina línea entre actuar así y producir un daño o caer en la tentación de *robar información,* por no hablar que en numerosas legislaciones, el mero hecho

[4] Vid. http://es.wikipedia.org/wiki/Dark_heats#Dark_hats_o_hackers_negros

de colocarse en un sistema ya es delito, a pesar de ello hay quiénes opinan que el acceso a sí mismo a un sistema, no puede ser considerado a priori como delito, si no se dan los requisitos, objetivos y subjetivos que configuran los tipos penales correspondientes; por ende, los Hackers deberán ser juzgados por sus hechos, no por criterios sin sentido como calificaciones académicas, edad, raza o posición social.

Estos suelen ser verdaderos expertos en el uso de las computadoras y por lo general hacen un uso delictivo de sus conocimientos, aunque no tienen reparo en intentar acceder a cualquier máquina conectada a la red o incluso penetrar a una Intranet privada, siempre con el declarado fin de investigar las defensas de estos sistemas, sus lados débiles y anotarse el mérito de haber logrado burlar a sus administradores, muchos de ellos dan a conocer a sus víctimas los huecos encontrados en la seguridad e incluso sugieren cómo corregirlos, otros llegan a publicar sus hallazgos en revistas o páginas Web de poder hacerlo.

En otro orden de ideas, el hacking puede clasificarse en directo e indirecto en 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 el desciframiento de los códigos de acceso o password, no causando daños inmediatos y tangibles en la victima o bien por la mera voluntad de curiosear o divertirse de su victima. La voluntad de divertirse generalmente se traducen por paseos por el sistema haciendo alarde de su intromisión, es lo que se ha llamado *joyriding o paseos de diversión,* caracterizando a esta clase de hacking: el Hacker es una persona experta en materias informáticas y con edad fluctuante entre los 15 y 25 años de edad es por ello que esta delincuencia se ha denominado, pantalones cortos, su motivación no es la de causar daños sino de obtener personales satisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad, ésta burla ellos lo toman como diversión, más no se dan cuenta que están cometiendo un delito.

3.3.2.- CRACKER.

Persona que se introduce en sistemas remotos con la intención de destruir, robar datos, denegar el servicio a usuarios legítimos y en general a causar problemas, mejor llamado *El Pirata informático*; utilizando variantes el primero, penetra en un sistema informático y roba información o produce destrozos en el mismo y en segundo, se dedica a desproteger todo tipo de programas para hacerlas plenamente operativas, como de programas completos comerciales que presentan protecciones anti-copia.

Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas; para los grandes fabricantes de sistemas y la prensa este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección, pero el problema no radica ahí, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware, así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica[5]; como su nombre indica se dedican a romper, por supuesto las protecciones y otros elementos de seguridad de los programas comerciales, en su mayoría con el fin confeso de sacar provecho de los mismos del mercado negro, crean códigos para utilizarlos en la copia de archivos, sus acciones pueden ir desde la destrucción de información ya sea a través de virus u otros medios, hasta el robo de datos y venta de ellos; por ejemplo, de su actuar ilegal son los millones de CDs con software pirata que circulan por el mundo entero y de hecho, muchas personas no llegan a sospechar que parte del software tienen en sus máquinas, incluso con certificados de garantía de procedencia, sucede sobre todo en los países del tercer mundo; se agrupan en pequeñas compañías y contratan especialistas de alto nivel.

[5] Cfr. http://es.wikipedia.org/wiki/Dark_heats#Dark_hats_o_hackers_negros

Aunque tratan de cubrirse con el ropaje de la aventura y el desafío tecnológico, los miles y millones de perdidas y los cientos de casos que conocen anualmente la policía y fiscales de todo el mundo, hablan de un interés pecuniario y delictivo científico, con herramientas de este espécimen suelen ser potentes editores hexadecimales y debuger's (depurador) mediante los cuales desmontan los programas, lo que se conoce como ingeniería inversa hasta llegar a las protecciones que son generalmente utilidades de tiempo que se representan en el reloj interno de la máquina o en el sistema operativo para desencadenar una cuenta regresiva que descontará los días posibles a usar el software hasta que el mismo caduque y el usuario este obligado a pagarlo o renunciar a él.

3.3.3.- PHREAKER.

Especialista en telefonía(Cracker de teléfono), inviste conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles, en la actualidad también poseen nociones de tarjetas prepago, ya que la telefonía celular las emplea habitualmente; sin embargo, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralistas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

Buscan burlar la protección de las redes públicas y corporativas de telefonía, con el declarado fin de poner a prueba conocimientos y habilidades, en la actualidad casi todas estas redes de comunicaciones son soportadas y administradas desde sistemas de computación e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de *hacking* a sus servidores.[6] Estos tipos con conocimientos de telefonía insuperables conocen a fondo los sistemas telefónicos incluso más que los propios técnicos de las compañías telefónicas, ellos han sabido crear todo

[6] Vid. http://es.wikipedia.org/wiki/Phreaker

tipo de cajas de sistemas fraudulentas con una función determinada; actualmente se preocupan mas de las tarjetas prepago que de estas cajas, ya que suelen operar desde cabinas telefónicas o móviles, con capacidad de captar los números de abonado en el aire, de esta forma es posible crear clones de tarjetas telefónicas para larga distancia.

Dentro de las actuales manifestaciones de phreaking podríamos distinguir:

a) Shoulder-surfing: Esta conducta se realiza por el agente mediante la observación del código secreto de acceso telefónico que pertenece a su potencial víctima, el cual lo obtiene al momento en que ella lo utiliza sin que la víctima pueda percatarse de que está siendo observada por este sujeto quien, posteriormente aprovechará esa información para beneficiarse con el uso del servicio telefónico ajeno.

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

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

3.3.4.- LAMMERS Y BUCANEROS.

El primero son los que aprovechan el conocimiento adquirido y publicado por los expertos, si el sitio web que intentan vulnerar los detiene, su capacidad no les permite continuar mas allá, generalmente son despreciados por los verdaderos hackers que los miran en menos por su falta de conocimientos y herramientas propias, muchos de los jóvenes que hoy en día se entretienen en este asunto forman parte de esta categoría y el segundo se trata de comerciantes, los bucaneros venden los productos

crackeados como tarjetas de control de acceso de canales de pago; por ello, los bucaneros no existen en la Red, solo se dedican a explotar este tipo de tarjetas para canales de pago que los Hardware Crackers crean, suelen ser personas sin ningún tipo de conocimientos ni de electrónica ni de informática pero si de negocios, el bucanero compra al CopyHacker y revende el producto bajo un nombre comercial, realidad que es un empresario con mucha afición a ganar dinero rápido y de forma sucia[7].

3.3.5.- GURUS y NEWBIE.

Los gurus, son maestros y enseñan a los futuros Hackers, normalmente se trata se personas adultas, porque la mayoría de Hackers son personas jóvenes que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma para enseñar a sacar de cualquier duda al joven iniciativo al tema. Es como una especie de profesor que tiene a sus espaldas unas cuantas medallitas que lo identifican como el mejor de su serie. El guru no esta activo, pero absorbe conocimientos ya que sigue practicando, pero para conocimientos propios y solo enseña las técnicas más básicas; en siguiente, traducción literal de newbie, alguien que empieza a partir de una WEB basada en Hacking, inicialmente es un novato, no hace nada y aprende lentamente, a veces se introduce en un sistema fácil y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la pagina WEB para seguir las instrucciones de nuevo, típico tipo simple y nada peligroso[8].

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

[7] Vid. http://www.telepolis.com/cgi-bin/web/DISTRITODOCVIEW?url=/1578/doc/hacking/Personas.htm

[8] Vid. http://www.segu-info.com.ar/amenazashumanas/otros.htm

tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada, esta minuciosa distinción de sujetos según su actuar no son útiles para tipificar el delito pues son sujetos indeterminados que no requieren condición especial; mas vale realizar dicha diferenciación para ubicarnos en el marco en que se desenvuelven y las características de su actuar, favoreciendo con ello el procedimiento penal que se deberá llevar a cabo luego de producirse el delito.

La gran mayoría de los hackers, en sentido general, copian herramientas que desarrollaron otros, actualmente existen alrededor de 60 mil páginas que explican con todo detalle muchos de los trucos para piratear, sólo basta con bajar un programa y comenzar a bombardear un sitio para lograr las primeras experiencias incluso, hay algunas páginas que ofrecen laboratorios de virus, donde la persona puede crearlos a su medida, siguiendo instrucciones básicas además, por medio de estos programas van aprendiendo a desarrollar sus propias herramientas.

Entre los métodos preferidos por estos delincuentes para desarrollar su actuar son: **1)** Puertas falsas: entradas que sirven para hacer la revisión o la recuperación de información en caso de errores en el sistema consiste en aprovechar los accesos. **2)** Llave maestra(superzapping): El uso no autorizado de programas para modificar, destruir, *robar*, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático, el nombre proviene de un programa de utilidad que se llama superzap, que permite abrir cualquier archivo de una computadora aunque se halle protegido por medidas de seguridad. **3)** Pinchado de líneas: Se realiza a través de la interferencia de las líneas telefónicas o telemáticas a través de las cuales se transmiten las informaciones procesadas en las bases de datos informáticas.

Un aspecto a diferenciar entre un hacker y un cracker puede ser que el primero crea sus propios programas, ya que tiene muchos conocimientos

en programación y además en varios lenguajes de programación, mientras que el segundo se basa en programas ya creados que puede adquirir normalmente vía Internet. Otro aspecto de interés de un cracker es destrozar la máquina que hay al otro lado, vender información al mejor postor, destruyen datos, roban información, modifican ficheros, introducir en los programas códigos malignos que crean problemas en el sistema donde se ejecutan o sea, lo único que hacen es crear problemas en la red, no es constructivo como un hacker, que trata de mejorar la red dando a conocer sus incursiones y los fallos que ha encontrado.

En referencia, el sujeto pasivo seguirá siendo la víctima del delito, el propietario legítimo del bien jurídico protegido; es decir, su información en base de datos sobre quien recae la conducta de acción u omisión que realiza el sujeto activo; en el caso de estos delitos, los sujetos pueden ser persona natural o jurídica que usan sistemas automatizados de información, generalmente conectados a otros. Mediante el sujeto pasivo podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, aunque estos generalmente no son descubiertos o no son denunciados a las autoridades responsables; tal vez la razón de ello es la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática o bien el temor a su empresa y las consecuentes pérdidas económicas u otros motivos.

En resumen, la especial naturaleza de la persona que tratamos nos permite considerarla además sujetos activos del derecho penal en la medida de su constitución o funcionamiento (capacidad legal) así lo demuestren. El artículo 16 Código Penal Federal vigente y sus acápites correspondientes al mismo, define esta figura y ratifica la responsabilidad penal que la misma posee ante el ordenamiento legal que le da vida; adoptar ésta condición de Hacker resultaría por otro lado muy complejo detectar su actividad; pues el hecho de entrar a un programa, sólo le permitiría conocer de las informaciones de otros, pero que sería inútil que las utilizara sino forma parte de su contenido de trabajo referido en su escritura de constitución; de aquí

que, remotamente pudiese sólo tener conocimiento de la información y prevenirse ella misma de cualquier acción que contra ella se tramara o poner en práctica medidas estratégicas para su autoprotección en lo que a ella pudiese afectar, primordialmente en el mercado internacional donde se juegan los roles principales.

El uso del www, llamado World Wide Web, la Web o Red Global Mundial con fines publicitarios hace que se trasladen a Internet, eslogan y mensajes publicitarios que se difunden en la vida real, ello hace posible la aplicación de la ley a las infracciones que se produzcan en el ciberespacio y que puedan causar un perjuicio grave a los consumidores, inclusive apreciaremos aquí conductas delictivas provocadas por usos comerciales pocos éticos, pese a cualquier obstáculo que pueda interferir en su actuar con intenciones de obtener beneficios en el mercado. Dichos delitos convencionales se encuentran en el capítulo referido a los delitos contra el honor donde podemos apreciar acciones tipificadas y que tienen una gran asociación con la nueva figura que aparece en el mundo digital y que intentamos que se reconozca en nuestro ordenamiento legal; podríamos presumir además, que la persona jurídica sea el sujeto activo de esta acción que se produzca con fines de competencia o ser el sujeto pasivo siendo afectada con dicha acción.

Como sujeto pasivo tomemos como referencia un ejemplo muy sencillo que evidencia su amenaza, que puede ser víctima en el campo de las comunicaciones en específico; podemos tomar como ejemplificación que en una empresa telefónica, banco, etcétera, puede darse el caso del robo informático y traer disímiles afectaciones, similar al robo de línea mediante acceso remoto nos encontramos el robo desde la misma central de información, desde donde se manipulará el software y se facilitaran las llamadas y actos ilícitos; la afectación muestra que delitos informáticos de esta modalidad será de doble sentido, económico, porque no se factura y existen pérdidas para la empresa y de peligro al realizar uso del software pues pudiera traer consecuencias mayores que el objetivo con que fue

utilizado, como alguna alteración del mismo con relación a su funcionamiento habitual.

En conclusión, éstos sujetos especiales por su modo de actuar y los medios que utilizan para ello trascienden por su relevancia en la historia de la humanidad y más aun en la historia del derecho. Realmente su presencia en la comisión de un hecho delictivo es sumamente importante, pues en una gran mayoría son individuos que comienzan a forjarse dentro del mundo de las acciones antijurídicas y otra parte son los responsables directos de mantener en pie dentro de este mundo que lucha por el pleno y total desarrollo de los sistemas computarizados y entre estos últimos están inmiscluidos tanto los que llevan a cabo la acción como aquellos que se niegan a denunciar las acciones negativas que han sido realizadas en su contra. Nuestro Código Penal Federal en los artículos del 16 al 18 de manera muy generalizada acorde con el capítulo, encierra la responsabilidad y las categorías de los sujetos de la acción penal; el autor y el cómplices, en el presente tema no se precisa determinar las categorías que pudieran trascender de estas acciones, mas si fuese conveniente hablar de una legislación especial que enmarque un supuesto patrón de conductas que posibilite identificar ante cual figura delictiva nos encontramos; por ende, al menos poder hacer un estudio determinando de campos de acción y los requisitos para su desenvolvimiento garantizando la efectividad de los órganos encargados de hacer justicia y la inmediatez de las sanciones adecuadas en cada situación que se presente en su jurisdicción, incluso para hacer eficaz la prevención en este sector y; también hablando del procedimiento, acatado por los tribunales en la actualidad es realmente incoherente con la realidad que se impone para las personas jurídicas, pues aun no ha sido detectada una vía eficaz para el enjuiciamiento de la persona tratada. Es de ilógicos pretender que sea juzgada la misma en un proceso vinculado con la informática cuando aun por el procedimiento convencional del ordenamiento, aun más sencillo ha sido imposible llevarse a cabo; Mas tampoco existe un ciber-tribunal para juzgar, ni un personal altamente preparado para enjuiciar a un sujeto activo de la acción penal en la esfera de

la informática, por dichas razones es imprescindible llevar a cabo la formación de juristas en esta esfera.

3.4.- POLICIA CIBERNÉTICA.

Unidad que comienza a funcionar en el mes de octubre del 2002, con la finalidad de detectar por medio del patrullaje en la red los sitios, procesos y responsables de las diferentes conductas delictivas tales como, la pornografía infantil, fraudes, robos, incitación al suicidio y las adicciones además de cualquier otro ilícito donde se emplean medios informáticos y electrónicos; a su vez, tiene como fin trabajar en coordinación con las instancias federales, locales, municipales y organizaciones que contribuyan al combate y prevención de las conductas y actos criminales que atacan o utilizan los medios señalados.

Desde entonces se ha mantenido al frente en el combate de este tipo de conductas, aportando metodologías y tecnología al combate frontal contra la delincuencia, al utilizar las herramientas más modernas por personal capacitado y actualizado continuamente en sus funciones; la Policía Cibernética, actualmente establecido en grupos multidisciplinario de profesionistas cuya actividad se centra principalmente en monitorear la red de Internet y se complementan sus actividades con el trabajo de campo, con el objetivo, misión y visión de identificar y desarticulación de organizaciones criminales que promueven conductas ilícitas empleando medios tecnológicos, además de prevenir a la sociedad Jalisciense de estas conductas delictivas, coadyuvando con la autoridad correspondiente en sus tres niveles de gobierno, contribuir a la seguridad y protección de la sociedad en general y de la población infantil en particular contra grupos o individuos que les dañan con el empleo de recursos tecnológicos, establecer un sistema de vigilancia permanente, desarrollar la investigación sistemática y continua[9].

[9] Vid. http://www.noroeste.com.mx/publicaciones.php?id=420868

Cabe señalar, que si entre sus funciones está la de combatir la pornografía infantil vía Internet, la Policía Cibernética también busca prevenir otros delitos que se cometen en y a través de una computadora, principalmente aquellos que atentan contra las instituciones y la población vulnerable, de acuerdo con la dirección de Inteligencia de la Policía Federal Preventiva (PFP), dicha Policía trabaja actualmente en la conformación de un banco de datos sobre pedofilia y agresiones sexuales, esa base de datos servirá para identificar patrones, rangos, preferencias y modus operandi de los casos reportados en México, para lo cual se intercambia información con organizaciones no gubernamentales nacionales.

El objetivo es conformar el primer banco de datos de bandas mexicanas dedicadas al tráfico de prostitución infantil y que utilizan la Internet para promover este delito; además, se intercambian datos con organizaciones internacionales como el National Center For Missing and Exploited Children de Estados Unidos, que ha ayudado identificar grupos de pedófilos en el estado de California.

La Policía Cibernética opera a través de patrullajes antihacker por el ciberespacio a través de computadoras, con lo que han comprobado el alarmante crecimiento de organizaciones de pedófilos que transmiten pornografía y promueven la corrupción de menores vía Internet; dicho ciber-patrullaje sirve también para atrapar a los delincuentes que cometen fraudes, robos, intrusiones, secuestros y organizan sus actividades delictivas en la red, sin que necesariamente se dediquen a la pornografía infantil. Según datos de la Policía Federal Preventiva (PFP);[10] luego, del ciber-patrullaje se analiza la información recolectada para combatir los delitos que tienen lugar en Internet y que son cometidos de manera particular contra menores; también de manera encubierta, se realizan operativos en la denominada súper carretera de la Información para detectar sitios donde se transmite pornografía infantil y donde un menor puede ser contactado por los delincuentes para conducirlo a actos inmorales.

[10] Vid. http://www.belt.es/noticias/2004/julio/23/poli_ciber.htm

Estas operaciones tuvieron sus máximo fruto en 2002, cuando la Policía Cibernética identificó en Acapulco a la organización pedófila más importante a nivel mundial y que encabezaba Robert Decker, quien fue detenido y expulsado a Estados Unidos, gracias a la colaboración con otras policías cibernéticos del planeta se ha logrado que con cada detención hecha en otros países se pueda detectar las conexiones que tienen los delincuentes en México; de igual manera, la Policía Cibernética recibe la colaboración de organismos no gubernamentales quienes por su cuenta realizan ciber-patrullajes en la Red, que han localizado sectas satánicas que utilizan menores y animales en sus sacrificios; de acuerdo con la información de la Dirección de Inteligencia de la Policía Federal Preventiva (PFP), ello demuestra que los delitos cometidos en contra de menores a través de una computadora y otros medios han tenido un incremento sin precedentes en México y todo el mundo.

La multicitada Policía Cibernética está adscrita a la Coordinación General de Inteligencia para la Prevención de la Secretaria de Seguridad Pública (SSP) y patrulla Internet mediante software convencional para rastreo de hackers y sitios de Internet, comunidades y chat en los que promueven la pornografía y el turismo sexual infantil; Con ello, se busca hacer de Internet en México un lugar seguro para el intercambio de información además de analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciberespacio, así como su modus operandi.

En lo que respecta al mercado informático, todo lo relacionado con hardware y software ha evolucionado muchísimo en lo que se refiere a seguridad, en cuanto a la seguridad en las redes todavía falta un camino grande, pero ya han empezado a aparecer productos muy sólidos en lo que se refiere a la administración de la seguridad informática en las redes multiplataforma.

3.5.- LEGISLACIÓN SOBRE DELITOS INFORMÁTICOS (COMENTARIO).

La legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, basándose en 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, previsionales y de identificación de las personas y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar 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 podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico institucional debe proteger.

No 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 conscientes e irresponsables de los datos que dichos sistemas que contiene la humanidad, no esta 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 puede conferirles, la utilicen para satisfacer sus propios intereses a expensas de las libertades individuales y en detrimento de las personas; asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas, la protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial e incluso de derecho administrativo, estas distintas medidas de protección no tienen porque ser excluyentes unas de otras sino que por el contrario, éstas deben estar estrechamente vinculadas; por eso, dada las características de esta problemática sólo a través de una protección global desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Un estudio de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras, desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos en la mayoría de las naciones occidentales existen normas similares a los países europeos; todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

También, las personas que cometen los Delitos Informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes; esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos, con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos; de esta forma, la persona que ingresa en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

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

3.6.- COMO FIN U OBJETIVO.

Es Promover la cultura de la legalidad y de la seguridad informática en todos los sectores del país como elemento fundamental para el desarrollo de los negocios y las nuevas tecnologías, lograr que en México el Internet y las telecomunicaciones en general sean medios seguros y confiables para la información y los negocios;[11] probar que la delincuencia informática en México es una realidad palpable, y como tal debe dársele la importancia necesaria en todos los ámbitos para combatir eficazmente esta actividad ilícita y perjudicial para toda la comunidad informática y de negocios del país; lanzar una campaña nacional para fomentar la cultura de la seguridad informática en los sectores público y privado; fomentar en las universidades, particularmente en las carreras tecnológicas, los valores éticos en el desempeño del profesional de la informática; también deberá fomentarse entre los directivos de escuelas y universidades el cumplimiento del Estado de Derecho, para que denuncien a los estudiantes que sean sorprendidos llevando a cabo delitos informáticos y colaboren con las autoridades competentes; capacitar a nuestras autoridades para que puedan investigar y perseguir de manera eficaz este tipo de delitos; en la actual Unidad de Policía Cibernética de la Policía Federal Preventiva, dependiente de la Secretaría de Seguridad Pública, dedica la mayor parte de sus esfuerzos a rastrear y detener pedófilos en internet; sabiendo lo delicado de este tipo de delitos y la debida atención policiaca que merecen; sin embargo, la pedofilia por internet no es el único ni el más relevante de los delitos informáticos; haciendo la modificación del Código Penal Federal, que sólo menciona a unos cuantos en materia de *Acceso Ilícito a Sistemas y Equipos de Informática* y aún no contempla muchos tipos de ataques informáticos como delitos.

En comento, hay categorías que se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

[11] Vid. http://www.delitosinformaticos.com.mx/mision.htm

a. Programación de instrucciones que producen un bloqueo total al sistema.
b. Destrucción de programas por cualquier método.
c. Daño a la memoria.
d. Robo de información.
e. Manipulación de maquinas.
f. Atentado físico contra la máquina o sus accesorios.
g. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
h. Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

a. Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
b. Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
c. Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
d. Otros delitos: Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

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

3.7.- CÓDIGO PENAL FEDERAL.

El Código Penal Federal en vigor, regula el acceso no autorizado a sistemas o servicios y destrucción de programas o datos, esta conducta se

encuentra regulada en los artículos 211 bis 1 al 211 bis 7, que determinan lo siguiente:

"TÍTULO NOVENO.
REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA.
CAPÍTULO I.
REVELACIÓN DE SECRETOS…

CAPÍTULO II.
ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA.

Artículo 211 bis 1. Al que sin autorización modifique, destruya o provoque perdida 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 perdida 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 perdida 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 de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4. Al que sin autorización modifique, destruya o provoque perdida 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 perdida 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 incrementaran 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 capitulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno".

Ahora bien, haciendo un análisis en los artículos citados, podremos hacer la modificación para la regulación de este Titulo Noveno quedando lo siguiente:

"TITULO NOVENO
REVELACIÓN DE SECRETOS Y DELITOS INFORMÁTICOS.
CAPITULO I.
REVELACIÓN DE SECRETOS…
CAPÍTULO II.
DELITOS INFORMÁTICOS.

Artículo 211 bis 1.- *para efectos de este título se entenderá por:*

I.- Computadoras: máquinas, aparatos, dispositivos, sistemas o equipos de informática, ya sean electrónicos, óptico, magnético o de cualquier tecnología, que sea apta para funciones lógicas, aritméticas,

transmisión, almacenamientos de datos, así como para el tratamiento sistemático de la información mediante el procedimiento automático de datos electrónicos, de cualquier otra tecnología. Este término también incluye las redes públicas o privadas de computadoras.

II.- Programas de computo: la expresión original en cualquier forma, tipo, lenguaje o código de mecanismo, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo de almacenamiento masivo realice una tarea o función especifica.

III.- Daño: deterioro o menoscabo a la integridad confidencial y disponibilidad de datos públicos, privados, información programas de cómputo.

IV.- Mecanismo de seguridad: dispositivo de almacenamiento masivo físico o electrónico, contraseña, palabra clave, código de acceso, programas de cómputo, equipo informático y/o información contenida en una computadora, sistemas o equipos informáticos:

a) Acceso interno o externos no autorizados;
b) Robo, ataque, alteración, borrado de información de cualquier índole.
c) Repudio del emisor o receptor de la información.

También de entenderá por mecanismo de seguridad, cualquier dispositivo técnico utilizado para protección de programas de cómputo contra su robo, copiado y distribución o uso ilícito.

V.- Datos, información personal: cualquier información relacionada a una persona física o moral, identificada. Los datos personales usualmente contienen información que directa, indirecta puede ser relacionada o ligada a una persona física o moral en particular.

***Artículo 211 bis 2.-** Comete el delito informático, la persona que con intención y sin derecho:*

I.- Robe información a una computadora pública, privada, dentro o no de la red de internet sin autorización;

II.- Accese, intercepte, modifique, altere, borre, destruya, provoque daños, perdida de información contenida en computadoras y programas de cómputo;

III.- Conozca, copie, divulgue o distribuya a terceros información o comunicaciones no dirigidas a él, contenidas en computadoras;

IV.- Diseñe, introduzca, programe, distribuya o provoque la transmisión o ejecución de programas de cómputo, datos, información, códigos, conjuntos de instrucciones, comandos informáticos que tengan por objeto:

a) Impedir el uso, funcionamiento apropiado o causar daños a información, computadoras o programas de computación;
b) Alterar la información, programas de cómputo contenidos en una computadora;
c) Causar la negación de servicios de naturaleza informática realizados por una o red de computadora;

V.- Diseñe, programe, comercialice, trafique, transmita, haga disponibles o distribuya programas de cómputo, números de serie o registros, palabras clave, códigos de acceso o información de cualquier naturaleza que sirva para violar mecanismos de seguridad;

VI.- Amenace, hostigue, intimide, aceche o cause temor a personas físicas o morales, mediante mensajes electrónicos, el uso de computadoras u otros mecanismos tecnológicos similares.

VII.- Comercialice, trafique, trasmita, difunda, distribuya o haga disponibles a través de redes de computadoras y/o dispositivos de almacenamiento masivo, magnéticos, ópticos, electrónicos o de cualquier tecnología:

a) Pornografía infantil;
b) Información xenofóbica, racista, discriminatoria de cualquier naturaleza;
c) Incitaciones, provocaciones para cometer delitos informáticos de cualquier índole;

VIII.- Obtenga sin consentimiento y mediante engaños datos o información personal de individuos para usarla con fines comerciales, obtenga un lucro directo, indirecto de dicha información, la use o provoque para cometer cualquier actividad ilícita;

IX.- transmita, publicite, distribuya o haga disposiciones a través de computadoras en red de internet o redes de computadoras datas o información personal de terceros sin su consentimiento o que la haya obtenido mediante engaños;

X.- Inserte, altere, borre, elimine información contenida en una computadora o programas de cómputo, lo cual resulte en información auténtica, independientemente de si la información sea directamente legible o accesible para su consulta.

A quien comete los delitos previstos en las fracciones III, VI, VII, VIII y IX, se le impondrá una pena de seis meses a tres años y de doscientos a seiscientos días multa.

A quien comete los delitos previstos en las fracciones I, II, IV, V y X, se le impondrá la pena de prisión de tres a diez años y de cuatrocientos a mil días multa.

Artículo 211 bis 3.- *las penas previstas en este capítulo se aumentaran hasta en una mitad:*

I.- Para los casos previstos en las fracciones I, II, y V de artículo 211 bis 2, cuando la información obtenida se utilice en provecho propio o ajeno;

II.- Para los casos previstos en la fracción IV del articulo 211 bis 2, cuando el daño se haya propagado masivamente, afectando a computadoras localizadas en varios Estados de la República Mexicana.

III.- Para cualquiera de los casos previstos en el artículo 211 bis 2:

a) *Cuando las conductas sean cometidas por funcionarios, empleados o personas que presten sus servicios en las instituciones, organizaciones , empresas a la que se le haya causado el daño;*
b) *Cuando el delito informático se haya cometido en contra de computadoras de de gobierno o del sistema financiero;*
c) *Cuando dos o más individuos hayan actuado coordinadamente para penetrar alguno de los delitos de este título;*
d) *Cuando para cometer el delito informático haya violado algún mecanismo de seguridad;*
e) *Cundo con el fin de disimular su identidad y/o ubicación, se haya aprovechado de la computadora y/o datos o información personal de un tercero o haya usado falsos para realizar cualquiera de las conductas tipificadas en este capítulo;*
f) *Cuando bajo engaños o aprovechándose del error en que se encuentra una persona, obtiene de éste información, códigos o claves de acceso o logra instalar en su computadora programas de cómputo, que le permitan realizar cualquiera de las conductas tipificadas en este capítulo.*

Artículo 211 bis 4.- *Las penas previstas en este capítulo se aumentan hasta el doble:*

a) *Cuando se hayan dado dos o más agravantes de las mencionadas en e l artículo 211 bis 3.*
b) *Cuando el delito informático haya sido motivado por cuestiones políticas, activistas, terroristas o haya tenido cualquiera de los fines contemplados en el Libro Segundo, Título Primero "Delitos de la Seguridad de la Nación" de éste Código.*

En respuesta, algunos de los defectos en esta área se contempla que el mismo Código dice que constituye el delito si se accesa a un sistema informático protegido por el mecanismo de seguridad; esto es erróneo pues, no define que debe entenderse por mecanismo de seguridad; es decir, ¿Qué es un mecanismo de seguridad de un sistema informático? ¿un

password? ¿Candado contra robo (físico)? ¿Tener la computadora encerrada en un cuarto bajo llave?, es como compararlo si se diera el delito de allanamiento de morada, es necesario que la casa habitación cuente con candado, llave o que cuente con una agente a lado, esta vaga redacción traerá problemas de interpretación a la hora de juzgar o analizar un caso concreto; también, no contempla todo los tipos de ataques informáticos más comunes; en consecuencia, el Código Penal Federal sufre en ese por los avances de la tecnología.

CONCLUSIONES.

PRIMERA.- En los últimos años, las tecnologías de la información y la Comunicación han revolucionado la vida social en numerosos aspectos: científicos, comerciales, laborales, profesionales, escolares, etcétera; la tecnología avanza a una velocidad vertiginosa y el Derecho, en especial el Derecho Mexicano, se ha quedado con mucho rezagado en la regulación de una materia que lo ha rebasado, el desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables, como la manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos, acceso, utilización y robo indebido 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 o morales, pero no sólo la cuantía de los perjuicios así ocasionados es a menudo superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse, se trata de una delincuencia de especialistas capaces de borrar toda huella de los hechos; en consecuencia, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que las peculiaridades del objeto de protección.

SEGUNDA.- Dar un concepto sobre delito de robo informáticos no es una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de *delitos* en el sentido de acciones tipificadas o contempladas en textos jurídico-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 aún; sin embargo, muchos especialistas en derecho informático emplean esta alusión a los efectos de una mejor conceptualización, de esta manera, el autor mexicano Julio Téllez Valdez

señala 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); por otro lado, se sostiene que los delitos informáticos son cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo.

TERCERA.- Es así, que el Derecho informático surge como un medio efectivo para regular la conducta del hombre en sociedad, pero la sociedad no es la misma en cada uno de los lugares del planeta e incluso en su ciber-especio electrónico, ni es la misma en cada momento de la historia; la sociedad evoluciona, se ha dado con el tiempo los avance de la ciencia y de la tecnología; el Derecho regula la conducta y los fenómenos sociales a través de leyes y entre esas legislaciones nos encontramos algunas de las leyes informáticas, el proceso de creación e inserción de estas leyes a la vida de una comunidad caber-jurídica determinada (en el caso de México, municipio, estado, país) es larga y lenta, sobre todo en el Sistema Jurídico Latino.

CUARTA.- En los últimos años, las Tecnologías de la Información y la Comunicación (TIC), han revolucionado la vida social en numerosos aspectos e incluso han cambiado los hábitos de entretenimiento y de interrelación de las personas al interior de la vida familiar; ciertamente resulta imposible que el Derecho vaya a la par con la tecnología en cuanto al fenómeno o conducta ilícita que infiere en el ámbito ciber-jurídico, empezando porque es evidente que estos fenómenos y/o conductas informáticas tienen que manifestarse primero, ya que las leyes no pueden regular lo que aún sigue cambiando; Si a esto le sumamos el carácter formal, escrito de nuestro sistema ciber-jurídico, las particularidades del proceso legislativo, la necesidad de que personas con formación de abogados comprendan lo necesario sobre tópicos técnicos, tecnológicos y las injerencias de intereses políticos, resulta que el Derecho y en especial, el Derecho Mexicano que es el que nos ocupa e interesa, se ha quedado con

mucho rezago en la regulación de una materia que lo ha rebasado y que exige atención inmediata y efectiva.

QUINTA.- Desde el punto de vista social es conveniente, educar y enseñar la correcta utilización de todas las herramientas informáticas, impartiendo conocimientos específicos acerca de las conductas prohibidas, algunas reseñadas en ésta investigación que no deben ejecutarse, no solo con el afán de protegerse, sino para evitar convertirse en un agente de dispersión que contribuya a que un delito informático siga extendiéndose y alcance una computadora en la que, debido a su entorno crítico, produzca un daño realmente grave e irreparable; con todo ello, se han llevado a cabo esfuerzos por legislar en la materia y algunos de éstos han fructificado, en las siguientes líneas trataré de dar un listado general sobre la situación actual de la legislación informática en México; para hacerlo de una manera ordenada, enunciemos los tópicos más importantes que ameritan una regulación especial, para analizar el caso de cada uno de ellos, donde la óptica legal y ante la inexistencia de normas que tipifiquen los delitos cometidos a través de la computadora, es necesario legislar:

- La instigación del robo informático cometido a través de la computadora.

- El tipo culposo para aquellos que, por imprudencia, negligencia, impericia causaren daños, introduzcan virus u otros, con capacidad de dañar a través de la computadora, considerando culposa la conducta de quien a través de la computadora daña los controles de un enfermo o paciente.
- Firma digital/electrónica y contratos electrónicos.
- Protección ạ correo electrónico (privacidad, spam).
- Protección a bases de datos.
- Cómputo forense (evidencias electrónicas).
- Protección de propiedad.

Expresándonos en términos no legales, al hablar de delitos informáticos, uno de ellos el robo informático, nos referimos a aquellas conductas que teniendo como instrumento o fin computadoras u otros bienes informáticos, lesionan o dañan bienes, intereses o derechos de personas físicas o morales, en términos jurídicos, para que exista delito es necesario

un acto u omisión que sancionen las leyes penales, por que una de las características indispensables del delito es la tipicidad; es decir, que la conducta esté descrita en un tipo penal en una ley penal, además de ser antijurídica, culpable y punible.

SEXTA.- En la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos electrónicos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas; además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación, tenerse en cuenta hasta que punto el derecho penal se extiende con criterios importantes, teniendo presente la situación actual en referencia con los delitos informáticos; considero que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema; en consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a cada país o región; la delincuencia informática, se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio, por eso puede señalarse que la prevención de los delitos electrónicos constituye un reto considerable tanto para los sectores afectados del país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales, por lo que es importante reforzar tanto las leyes que sancionan estos tipos de delitos como enseñar e informar a la comunidad; al respecto, debido a la naturaleza virtual de estos delitos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área; desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados

esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

SÉPTIMA.- De las características que acabo de enunciar, es importante señalar que se debe de actuar de la manera más eficaz para evitar este tipo de delitos y que no se sigan cometiendo con tanta impunidad, se debe de legislar de una manera seria y honesta, recurriendo a las diferentes personalidades que tiene el conocimiento, tanto técnico en materia de computación como en lo legal, ya que si no se conoce de la materia, difícilmente se podrán aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular. Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área; desde el punto de vista de la Legislatura es difícil la clasificación de éstos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática, la falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

BIBLIOGRAFÍA.

ANDRÉS CAMPOLI, Gabriel. Derecho Penal Informático en México. Edición e impresión por Instituto Nacional de ciencias penales. INACIPE, México 2004.

ANDRÉS CAMPOLI, Gabriel. Delitos informáticos en la legislación mexicana. Edición e impresión por Instituto nacional de ciencias penales. INACIPE, México 2005.

CASTELLANOS, Fernando. Lineamientos elementales de Derecho Penal. Editorial Porrúa, México, 1976.

GONZÁLEZ DE LA VEGA, Francisco. Derecho penal mexicano Editorial, Porrúa, 1977.

MEDINA PEÑALOSA, Sergio J. Teoría del Delito; Casualismo, Finalismo e Imputación objetiva, 2ª.Ed. Editorial Ángel, México 2001.

REYNOSO DÁVILA, Roberto, Teoría General del Delito, 6ª ed. Editorial Porrúa, México, 2006.

TELLEZ VALDÉS, Julio. Los Delitos informáticos. Edición Adobe PDF, Editorial McGraw-Hill/Interamericana editores, S.A. de C.V. México, 1998.

OBRAS GENERALES.

JIMÉNEZ DE ASÚA, Luis. Biblioteca de Clásicos del derecho Penal lecciones. Tomo III Oxford, 1999

PALOMAR DE MIGUEL, Juan. Diccionario para Juristas. Tomo I. Editorial Porrúa, 2003.

PALOMAR DE MIGUEL, Juan. Diccionario para Juristas. Tomo II. Editorial Porrúa, 2003.

LEGISLACIONES.

Código Penal Federal.

Ley Orgánica del Poder Judicial de la Federación.

Código Penal del Estado de Nuevo León.

INTERNET.

http://html.rincondelvago.com/punibilidad.html
www.comceoccte.org.mx/images/boletines/Ponencia%20delitos%20fiscales.ppt
http://www.derecho.unam.mx/papime/TeoriadelDelitoVol.II/cinco.htm
http://www.tribunalmmm.gob.mx/bibliotyeca/almadelia/Cop2.htm
htt://derecho. Uman.mx/TeoriadelDelitoVol.II/cinco.htm
http://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico
http://www.portaley.com/delitos-informaticos/codigo-penal.shtml
http://www.derecho.unam.mx/papime/TeoriadelDelitoVol.II/uno.htm
http://www.delitosinformaticos.com.mx/mision.htm
http://www.segu-info.com.ar/amenazashumanas/otros.htmhttp://www.telepolis.com/cgibin/web/DISTRITODOCVIEW?url=/1578/doc/hacking/Personas.htm
http://es.wikipedia.org/wiki/Phreakerhttp://es.wikipedia.org/wiki/Dark_heats#Dark_hats_o_hackers_negros
http://www.delitosinformaticos.com.mx/mision.htm