UNIVERSIDAD LATINA, S.C.

INCORPORADA A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

"LA AUSENCIA DEL TIPO PENAL EN EL CÓDIGO PENAL FEDERAL DE LAS CONDUCTAS ANTISOCIALES QUE GENERA EL USO DE LOS SISTEMAS INFORMÁTICOS".

T E S I S

QUE PARA OPTAR POR EL TITULO DE
LICENCIADA EN DERECHO

P R E S E N T A

JOANA ALVAREZ DE LOERA

ASESOR DE TESIS:

JOSÉ FERNANDO CERVANTES MERINO.

MÉXICO, D.F. 2005.

Febrero 7 del 2005

LIC. GUILLERMINA OLGUÍN VARGAS
Directora Técnica de la Licenciatura en Derecho
Universidad Latina S.C., Campus Centro
P r e s e n t e.

Apreciable Directora, con la presente me permito informar a usted, que la alumna JOANA ALVAREZ DE LOERA ha concluido, bajo la dirección y asesoría del suscrito, la tesis denominada **"La ausencia del tipo penal en el Código Penal Federal de las conductas antisociales que genera el uso de los sistemas informáticos".**

El trabajo de investigación anteriormente referido, pone en contexto que si bien el avance científico-tecnológico en la sociedad moderna trae beneficios para la cultura humana, también es verdad que provoca lagunas legales que conllevan a la impunidad de los individuos que aprovechando sus conocimientos informáticos sacan provecho lesionando el interés de los demás.

Ciertamente, el presente trabajo de investigación, además de ser novedoso propone que dentro del Código Penal Federal se incluyan determinadas figuras delictivas inherentes a los delitos informáticos.

Me permito hacer notar a usted, que la señorita Alvarez de Loera durante el desarrollo de la presente investigación demostró responsabilidad e interés encomiable y siempre apegada a los lineamientos académicos requeridos por nuestra Institución, **lo cual me permite expresar mi conformidad con el trabajo realizado y desde este momento emito mi voto aprobatorio para los efectos conducentes académicos a que haya lugar.**

Aprovecho la ocasión para reiterarle mi más alta consideración y enviarle un saludo cordial.

Atentamente
"LUX VIA SAPIENTAS"

LIC. JOSÉ FERNANDO CERVANTES MERINO.

AGRADECIMIENTOS:

A DIOS:

Primordialmente por darme la vida, por darme lo mas valioso en este mundo que son mis padres y finalmente por permitirme vivir la alegría de terminar con esta faceta de mi vida, que es tan importante para mi, y por prestarme a los dos ángeles que me guían.

A MI PADRE:

Por que desde pequeña ha sido para mi un hombre grande y maravilloso y que siempre he admirado; gracias por guiar mi vida con energía, esto es lo que ha hecho de mi y lo que soy, gracias por todo lo que me has dado.

A MI MADRE:

Con la mayor gratitud por todos tus esfuerzos, tus desvelos, tus sacrificios para que pudiera terminar mi carrera profesional; por haberme dado todo y por enseñarme a luchar por lo que se quiere.

Gracias por guiar mi camino y por estar siempre junto a mí en los momentos difíciles.

Mi triunfo es tuyo.

A MI HERMANO JORGE ALVAREZ DE LOERA:

Por compartir todos los años de nuestras vidas juntos y por el gran apoyo brindado durante los años más difíciles y más felices de mi vida, en los cuales he logrado terminar mi carrera profesional, la cual constituye un aliciente para continuar con mi superación.

A NOÉ CUEVAS OCAMPO:

Por que gracias a su apoyo, consejos, comprensión y tolerancia, he llegado a realizar las más grandes de mis metas, y con la promesa de seguir siempre adelante juntos.

JUEZ AMADO CHIÑAS FUENTES:

Mil gracias por la confianza depositada, y por haber creído en mí, por permitirme empezar con el primer paso de uno de mis más grandes metas que es realizar la carrera judicial, con admiración, gracias.

LICENCIADO CERVANTES MERINO:

Principalmente por aceptar asesorarme en la realización de esta tesis y por la enseñanza de sus conocimientos, que son muchos.

LICENCIADOS INTEGRANTES DEL PODER JUDICIAL FEDERAL:

Calzada Caldera Agripina; Aguilar Moreno Ricardo; Silvia Guadalupe Palazuelos; José Díaz De León, Anaya Robles José Antonio; Luis Mora Hernández; Jorge Salas Pérez; Javier Flores Del Río; Enrique Frías Medina; Enrique Velásquez, Daniel Dámaso Castro Vera, en testimonio de gratitud ilimitada por su apoyo, aliento y estimulo, mismos que posibilitaron la conquista de esta meta.

Mi formación profesional.

A MIS COMPAÑEROS DEL JUZGADO CUARTO DE DISTRITO "A" DE AMPARO EN MATERIA PENAL:

Claudia Hernández; Ángel, Cristóbal, Edwin, Elizabeth, Ricardo, Hatziri, Armando, señora Vicky, Isaac, Julio y Claudia Mercado por que al término de esta etapa de mi vida, quiero expresar un profundo agradecimiento a quienes con su ayuda, apoyo y comprensión me alentaron a lograr esta hermosa realidad y por tener un gran ambiente de trabajo.

A LA UNIVERSIDAD LATINA Y A TODOS MIS PROFESORES DE LA LICENCIATURA EN DERECHO:

Les dedico esta tesis como agradecimiento al apoyo brindado durante cinco años de estudio y como reconocimiento de gratitud al haber finalizado esta carrera.

A todas las personas que siguen a mi lado y a las que ya se fueron a un mejor lugar de la vida, que a lo largo de mi vida han estado junto a mí, como un testimonio de cariño y eterno agradecimiento por mi existencia, valores morales y formación profesional.

ÍNDICE:

Prólogo ---------- 4

Introducción ---------- 9

CAPITULO I

1.1 El derecho penal y su concepto ---------- 13

1.2 El derecho penal en sentido subjetivo y objetivo ---------- 14

1.3 La evolución histórica de las ideas penales ---------- 16

1.4 Concepción moderna del derecho penal con el surgimiento de las escuelas penales ---------- 21

1.5 Escuela clásica ---------- 21

1.6 Escuela positivista ---------- 24

1.7 Escuela ecléctica ---------- 26

CAPITULO II.

2.1 Evolución doctrinal de las diversas teoría elaboradas para el estudio del delito ---------- 28

2.2 Teoría Causalista ---------- 28

2.3 Teoría Finalista ---------- 36

2.4 Conclusión y diferencias de la teoría Causalista y Finalista de la acción. ---------- 42

2.5 Principales diferencias entre la teoría Causalista y Finalista de la acción. ---------- 47

2.6 Dualidad entre la teoría Causalista y Finalista de la acción -------- 48

2.7 Teoría del funcionalismo Social ---------- 48

2.8 Teoría psicologista de la culpabilidad ---------- 49

2.9 Teoría normativista de la culpabilidad. ---------- 51

2.10 Teoría sociologista. ---------- 52

2.11 El delito, definición legal y doctrinaria. ---------- 52
2.12 Elementos del delito ---------- 55
2.13 La conducta ---------- 59
2.14 La ausencia de conducta ---------- 64
2.15 La tipicidad ---------- 65
2.16 La ausencia de tipicidad ---------- 66
2.17 La antijucididad ---------- 68
2.18 Las causas de justificación ---------- 69
2.19 La imputabilidad ---------- 76
2.20 La inimputabilidad ---------- 77
2.21 La culpabilidad ---------- 78
2.22 Formas de comisión del delito ---------- 80
2.23 La inculpabilidad ---------- 82
2.24 Las condiciones objetivas de punibilidad ---------- 84
2.25 La falta de condiciones objetivas ---------- 85
2.26 La punibilidad ---------- 85
2.27 Las excusas absolutorias ---------- 86

CAPITULO III

3.1 Antecedentes históricos de los delitos informáticos ---------- 89
3.2 Estructura de las computadoras. ---------- 99
3.3 Lenguajes de programación de las computadoras. ---------- 100
3.4 Principales lenguajes de programación. ---------- 100
3.5 Tratamiento internacional y nacional. ---------- 108
3.6 Postura de diversos organismos internacionales en materia de regulación informática ---------- 112
3.7 Legislación comparada de los delitos informáticos. ---------- 118
3.8 Legislación nacional. ---------- 130
3.9 Tratado del libre comercio de Américo ---------- 132

3.10 Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio, e incluso con el comercio de mercancías falsificadas. ---------- 133
3.11 Código penal del estado de Sinaloa. ---------- 134
3.12 Ley federal de derechos de autor y código penal federal. ---------- 136

CAPITULO IV.

4.1 Concepto de los delitos informáticos. ---------- 142
4.2 Sujeto activo ---------- 143
4.3 Sujeto pasivo ---------- 145
4.4 Principales características ---------- 147
4.5 Conductas ilegitimas más comunes ---------- 152
4.6 Tipo delitos informáticos. ---------- 154
4.7 Conductas que se cometen a través de la computadora y del Internet . ---------- 174
4.8 Casos verídicos ---------- 175
4.9 Estadísticas sobre los delitos informáticos. ---------- 180

CAPITULO V.

5.1 Fundamentos para la tipificación de los delitos informáticos en el código penal federal. ---------- 191

Conclusión ---------- 209
Bibliografía. ---------- 213.

PRÓLOGO

En la actualidad las computadoras se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación fundado en la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios.

Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee, un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados.

En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder a casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Este es el panorama del este nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la informática es hoy una forma de poder social. Las facultades que el fenómeno pone a disposición de gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícitos e ilícitos, en donde es necesario el derecho para regular los múltiples efectos de una situación nueva y de tantas potencialidades en el medio social.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los microprocesadores de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información".

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso, sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad. Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la Organización de Cooperación y Desarrollo Económico (OCDE) a Paris, Francia, en mayo de 1983, el término delitos relacionados con las computadoras se define como

"cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesador 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. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como criminalidad informática.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, fraudes, entre

otros). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, se han 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 que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

El estudio de los distintos métodos de destrucción y/o violación del hardware y el software es necesario en orden para 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 regulación sólo en aquellos aspectos en los que, en base a las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos pueden proporcionar datos e informaciones sobre miles de personas, físicas y morales, 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, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares, se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

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

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, dadas 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.

INTRODUCCIÓN

La principal problemática que se analiza en este tema de tesis es la falta de tipificación de las conductas ilícitas generadas a través de la informática, las cuales se pretende que lleven el nombre de Delitos Informáticos, por tal motivo dichas conductas no son sancionadas por el Código Penal Federal; por lo que se trata de crear conciencia social de la responsabilidad; para dotar al país, de las legislaciones adecuadas ya que en la actualidad en nuestro país no son castigadas las conductas delictivas generadas por el gran avance tecnológico de las computadoras, sobre todo en el campo de la informática, implica actividades criminales, que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional.

Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del derecho, para que esas conductas ilícitas deban ser sancionadas por el derecho penal.

Dado a lo anterior, ha sido imposible conocer la verdadera magnitud de los Delitos Informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados por no ser consideradas como delito en nuestra legislación mexicana.

Por lo que, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar este tipo de conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática que cada dia tiende a

expandirse mas, ya que el desarrollo tan amplio de la tecnología ofrece un aspecto negativo ya que ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de forma que hasta hora no era posible imaginar.

Los beneficios que los medios tecnológicos y el uso de la informática en particular aportan a la sociedad actual. Es indudable que la vertiginosidad del progreso no se presentaría si no intervinieran de manera directa los elementos electrónicos con los que contamos hoy en día. Sin embargo, la utilización de dichos medios informáticos, al ser destinados al servicio de la sociedad, requieren de una inminente regulación jurídica con respecto a su utilización. El objetivo de esta tesis es analizar las conductas delictivas que puede generar el gran avance tecnológico, sobre todo en el campo de la informática.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades, sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquélla. En ese entendido, la presente tesis se dirige al análisis de las posibles medidas preventivas penal que deben ser tomadas en cuenta para evitar que la comisión de este tipo de delitos alcance en México los niveles de peligrosidad que se han registrado en otros países.

Durante la etapa de investigación se encontró que no existe un consenso en cuanto al concepto de delito informático, y que estudiosos del tema lo han definido desde diferentes puntos de vista como son el criminógeno, formal, típico y atípico, dando lugar a que la denominación de esta conducta haya sufrido diferentes interpretaciones, que ya han sido analizadas en este trabajo, por lo que creí adecuado hacer un estudio minucioso sobre la teoría del delito y las diferentes maneras en que ha evolucionado, para tener un mejor panorama del delito, para una mejor forma de analizar las conductas generadas por las computadoras. Además se han señalado los sujetos activos y pasivos, clasificación y los tipos de delitos informáticos considerados tanto en la doctrina como en la legislación de diferentes países.

Seguidamente, se presenta un estudio comparativo de la problemática de los delitos informáticos en países tanto de Europa como de América, donde mayor incidencia ha tenido este fenómeno, el tratamiento penal que algunos gobiernos le han dado, y la parcial inercia que otros han mantenido sobre el tema, lo que se ha traducido en proyectos que hasta el momento no han fructificado.

A continuación se analiza la regulación que han tenido en la legislación mexicana las conductas ilícitas relacionadas con la informática. Para ello se estudian los antecedentes que han tenido las regulaciones vigentes en esta materia: Acuerdos celebrados en el marco del Acuerdo General de Aranceles Aduaneros y Comercio (GATT) y El Tratado de Libre Comercio de América del Norte (TLC).

Seguidamente se enuncia el tratamiento administrativo que se realiza a través de la Ley Federal del Derecho de Autor, y en el penal. Sobre el particular, debe aclararse que esta ley no regula delitos informáticos ya que su competencia es la de sancionar administrativamente conductas ilícitas cuyo bien jurídico a tutelar es la propiedad intelectual.

Para finalizar se incluye una propuesta, sustentada en el estudio comparativo antes mencionado, que trata de adecuar a la realidad existente en México, pero previendo que nuestro país no está exento de la velocidad del desarrollo tecnológico y de los vicios que éste genera.

En ese sentido, esta tesis se dirige al análisis de las posibles medidas preventivas de carácter penal que deben ser tomadas en cuenta para evitar que este tipo de delitos, alcancen en México los niveles de peligrosidad que se han dado en otros países.

Como objetivo especifico, proponer la solución de dichas problemática considero que es necesario que el Código Penal Federal incluya figuras delictivas que contengan a los Delitos Informáticos, por tal motivo propongo la iniciativa de Reforma al Código Penal Federal.

Como objetivo general combatir todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informativo, a través de la regulación en las Leyes Penales Federales de aquellas actitudes antijurídicas para evitar su impunidad adminiculada, ya que considero que es una forma de control preventivo y correctivo de las conductas criminógenas que están dirigidas en contra de las computadoras.

CAPITULO I

1.1 El derecho penal y su concepto

1.2 El derecho penal en sentido subjetivo y objetivo

1.3 La evolución histórica de las ideas penales

1.4 Concepción moderna del derecho penal con el surgimiento de las escuelas penales

1.5 Escuela clásica

1.6 Escuela positivista

1.7 Escuela ecléctica

CAPITULO I

1.1 EL DERECHO PENAL Y SU CONCEPTO

La sociedad es, sabidamente, una forma de vida natural y necesaria al hombre, en la cual se requiere un ajuste de las funciones y de las actividades de cada individuo, que haga posible la convivencia evitando choques, resolviendo conflictos y fomentando la cooperación.

En consecuencia, si el hombre ha de vivir en sociedad para su conservación y desarrollo, es claro que en esa sociedad, organizada con tales fines, ha de tener posibilidad de hacer todo aquello que sea medio adecuado para llenar sus propias necesidades, hallándose obligado a respetar el ejercicio de iguales facultades en los demás y aun a contribuir con su esfuerzo para la satisfacción de las exigencias colectivas, constituyéndo así el orden jurídico por el conjunto de normas que regulan y hacen posible y benéfica la vida en común.

El derecho penal, también llamado derecho criminal, derecho punitivo o derecho de castigar, "es el conjunto de normas jurídicas del estado que versan sobre el delito y las consecuencias que este acarrea, ello es la pena y las medidas de seguridad."[1]

Así y de acuerdo a lo estimado por Ignacio Villalobos, en su obra "Derecho Penal Mexicano", define al Derecho Penal como:

"Aquella rama del Derecho Público Interno, cuyas disposiciones tienden a mantener el orden político-social de una comunidad, combatiendo por medio de penas y otras medidas adecuadas aquellas conductas que le dañan o ponen en peligro."[2]

[1] Diccionario Jurídico Mexicano, Instituto de Investigaciones Jurídicas, Ed, Porrúa, p. 1023, México 2003.
[2] VILLALOBOS, Ignacio. DERECHO PENAL MEXICANO. Editorial Porrúa. S.A. México 1975. pp. 650.

La expresión Derecho Penal como certeramente afirma Maggiore, se aplica para designar tanto al conjunto de normas penales (ordenamiento jurídico penal), cuanto a la Ciencia del Derecho Penal, estimada como una rama del conocimiento humano compuesta de un acervo de nociones jurídicas de naturaleza intelectual , por lo que define al derecho penal como "la rama del derecho público interno relativa a los delitos, a las penas y a las medidas de seguridad, que tiene por objeto inmediato la creación y la conservación del orden social."[3]

En consecuencia podemos definir al Derecho Penal como la rama del derecho público interno relativo a los delitos, a las penas y a las medidas de seguridad que se aplican para lograr y conservar el orden social.

La anterior definición obedece que entendemos por Derecho público, como el conjunto de normas que rigen relaciones, en donde el estado interviene y tiene la capacidad para establecer los delitos y señalar las penas, imponer estas y ejecutarlas; asimismo normar relaciones entre el poder y los gobernados, ya que la potestad punitiva compete exclusivamente al estado.

1.2 EL DERECHO PENAL EN SENTIDO SUBJETIVO Y OBJETIVO.

El derecho penal subjetivo es el atributo de la soberanía por el cual a todo Estado corresponde reprimir los delitos por medio de las penas; en tanto que objetivamente se forma por el conjunto de normas y de disposiciones que reglamentan el ejercicio de ese atributo: el Estado, como organización política de la Sociedad, tiene como fines primordiales la creación y el mantenimiento del orden jurídico; por tanto, su esencia misma supone el uso de los medios adecuados para tal fin.

[3] MAGGIORE, DERECHO PENAL I, Editorial Temis, Bogotá, 1954, p.3.

Define al Derecho Penal Sustantivo José Arturo González Quintanilla, en su obra intitulada "Derecho Penal Mexicano", de la siguiente forma: " El Derecho Penal es el poder punitivo del Estado, constituyendo, desde luego, la expresión más enérgica del poder. Mediante este fenómeno se establecen los delitos y las penas como su legítima consecuencia. Los representantes y órganos correspondientes del Estado captan los valores medios que se requieren para la convivencia en común de la colectividad; así también, llevan a cabo la imposición de los valores propios que aseguran la subsistencia y desarrollo del Estado como tal, incorporando los de mayor envergadura en el Código o Leyes Penales."[4]

Cuello Calón lo define el derecho Penal en Sentido Objetivo como "el conjunto de normas jurídicas establecidas por el estado que determinan los delitos, las penas y las medidas de seguridad con que aquéllos son sancionados."[5]

Por otra parte, Pessina define al derecho Penal en Sentido Objetivo como "el conjunto de principios relativos al castigo del delito."[6]

Para Raúl Carrancá y Trujillo estima que el derecho penal, objetivamente considerado, es "el conjunto de leyes mediante las cuales el estado define los delitos, determina las penas imponibles a los delincuentes y regula la aplicación concreta de las mismas a los casos de incriminación."[7]

Entre las diversas concepciones del Derecho Penal, Jiménez de Asúa, citando a varios autores, nos menciona: "Hay definiciones subjetivas en que se alude al fundamento del derecho de castigar, considerándolo como la ciencia que funda y determina el ejercicio del poder punitivo del Estado.

En su sentido objetivo lo define como: " conjunto de normas que regulan el Derecho Punitivo."[8]

El Derecho Penal, es el complejo de las normas del derecho positivo destinadas a la definición de los delitos y fijación de las sanciones.

---

[4] GONZÁLEZ Quintanilla, José Arturo. DERECHO PENAL MEXICANO. (PARTE GENERAL) Editorial Porrúa .S.A. México1993. pp.503.
[5] CUELLO, Calón Eugenio, DERECHO PENAL I, 8ª EDICIÓN, P.8.
[6] PESSINA, ELEMENTOS DEL RERECHO PENAL, Madrid 1892, p.1.
[7] RAÚL, Carrancá y Trujillo, TRATADO DE DERECHO PENAL, TITULO I, P. 27-28.
[8] JIMÉNES DE ASÚA, Luis, DERECHO CRIMINAL, Alemania, 1892.

Por otra parte, Adolfo de Miguel Garcilópez, considera que "el Derecho Penal Subjetivo, se identifica con el *jus puniendi,* es el derecho a castigar."[9]

Finalmente, podemos concluir que el Derecho Penal Objetivo es el conjunto de normas jurídicas establecidas por el estado que determinan los delitos, las penas y las medidas de seguridad para la conservación del orden social; asimismo por Derecho Penal Subjetivo es el conjunto de atribuciones del estado, emanadas de normas, para determinar los casos en que deben imponerse las penas y medidas de seguridad o bien la facultad que tiene el estado de castigar al autor o autores de una conducta delictiva.

1.3 LA EVOLUCIÒN HISTORICA DE LAS IDEAS PENALES

A lo largo del tiempo, la función represiva se ha orientado hacia diversas rutas según los distintos pueblos; ya que desde que la sociedad existe como tal, desde las primeras agrupaciones humanas, el hombre conoce el fenómeno de la criminalidad. Esta se manifiesta en todas las sociedades. Constituye uno de los aspectos constantes de la vida social, hasta el punto que hoy no se considera la criminalidad como un fenómeno anormal del grupo social, sino como algo connatural a toda sociedad organizada, siendo sólo lo anormal los bruscos crecimientos o decrecimientos de las tasas de delito. Con base a ello, se han señalado como características del fenómeno criminal su permanencia y su actualidad.

El manejo que en forma común han transmitido los juristas de la historia del Derecho Penal es la siguiente: Venganza Privada; Venganza Divina; Venganza Pública; Defensa del Poder Absoluto; período Humanitario y Etapa Científica.

VENGANZA PRIVADA.- En esta etapa a esta etapa suele llamársele también venganza de la sangre o época bárbara que fue el impulso de la defensa o la venganza la *ratio essendi* (razón de ser) de todas las actividades provocadas por un ataque injusto. Durante esta época, la función punitiva la ejercían los particulares,

[9] GARCILÓPEZ, Adolfo de Miguel, DERECHO PENAL, p.7.

pues cada particular, cada familia y cada grupo se protegía y se hacía justicia por si mismo, sin embargo, debido a los excesos cometidos por los ofendidos al realizar su "venganza"."[10]

"La venganza privada se conoce también como venganza de la sangre en ocasiones los vengadores, al ejercitar su reacción, se excedían causando daños mucho mayores que los recibidos, por lo que hubo la necesidad de limitar la venganza y así apareció, surgió lo que se conoce como la ley del talión, que no fue otra cosa, sino una medida moderadora, pues sólo se le reconocía al ofendido el derecho de causar un mal de igual intensidad al sufrido.

Tiempo después de que nació la compensación, mediante la cual "se autorizaba para que ofendido y ofensor, nombrasen representantes que moderaran los reclamos recíprocos y acordaran la cantidad del castigo."[11]

Finalmente podemos considerar que en esta época no era otra cosa que los particulares se hacían justicia por su propia mano, conocida como la ley del talión que se caracterizaba por su muy conocida frase "ojo por ojo y diente por diente", por lo que se surgió la necesidad de que el castigo fuera en proporción al mal sufrido, para que no existiera un castigo mayor al daño causado, ya que esta época se degenero por que el hombre no castigaba conforme al daño que le habían causado, si no que se excedía en el castigo y siempre quería ocasionar mas daño que el hecho.

VENGANZA DIVINA.- "En este período se estima al delito como una de las causas del descontento de los dioses; por eso los jueces y tribunales juzgan en nombre de la divinidad ofendida, pronunciando su sentencia e imponiendo las penas para satisfacer su ira, logrando el desistimiento de su justa indignación, por lo que en esta etapa la justicia represiva era manejada generalmente por la clase sacerdotal."[12]

En conclusión en esta época la religión jugaba un papel muy importante ya que los sacerdotes eran los que impartían justicia y designaban el castigo que merecían

---

[10] VILLALOBOS, Ignacio. DERECHO PENAL MEXICANO. Editorial Porrúa. S.A. México 1975. pp. 24.
[11] SOLER, Sebastián. DERECHO PENAL ARGENTINO. Buenos Aires, p.55.
[12] VILLALOBOS, Op. cit. PP.25.

los delincuentes, este es un claro ejemplo de los judíos que han sido siempre eminentemente religiosos, en esta época había una gran confusión entre los delitos y los pecados y no se contaba con ningún tipo de garantías individuales para el individuo que cometiera cualquier tipo de delito.

VENGANZA PUBLICA.- "Durante esta etapa, se empieza a hacer distinción entre delitos privados y públicos, según el hecho lesione de manera directa los intereses de los particulares o el orden público. Es entonces cuando aparece la etapa llamada "venganza pública" o "concepción política"; los tribunales juzgan en nombre de la colectividad. Este fue una inmensa época, de propósitos retributivos y a lo sumo intimidantes, con fines de prevención general, en que se aspiraba a utilizar al delincuente en provecho del Estado (minas, galeras)."[13]

Carrancá y Trujillo, "aguzó su ingenio para inventar suplicios, para vengarse con refinado encarnizamiento; la tortura era una cuestión preparatoria durante la instrucción y una cuestión previa antes de la ejecución, a fin de obtener revelaciones o confesiones, por o que surgieron los calabozos, las jaulas, de hierro o de madera.[14]

Cuello Calón afirma "que en este periodo nada se respetaba, ni siquiera la tranquilidad de las tumbas, pues se desenterraban los cadáveres y se les procesaba; los jueces y tribunales poseían facultades omnímodas y podían incriminar hechos no previstos como delitos en las leyes.[15]

En esta etapa se pretendía que el dominio que representara a la sociedad fuera de una sola persona, si no por el contrario los tribunales juzgaban al delincuente en representación de la sociedad, definitivamente se trataba de una época totalmente de tortura, sin embargo empieza a surgir el castigo a cargo de los tribunales quienes juzgaban el daño causado y el castigo merecedor a tal ilícito, en esta etapa la sociedad estaba más integrada, pero de igual manera no se contaba con ninguna garantía individual.

---

[13] Op. cit. PP.52
[14] CARRANCÁ, op cit. P60
[15] CUELLO, op cit. 52

PERIODO HUMANITARIO.- "Es una ley física que a toda acción corresponde una reacción de igual intensidad, pero en sentido contrario nació como reacción a la excesiva crueldad imperante en la aplicación de penas. Dentro de esta corriente, se pugna por la exclusión de suplicios y crueldades innecesarios, se propone la certeza contra las atrocidades de las penas, se preconiza la peligrosidad del delincuente como punto de mira para la determinación de las sanciones aplicables y surge por una legalidad de los delitos y de las penas, hasta el extremo de proscribir la interpretación de la ley, por el peligro de que pudiera servir de pretexto para su verdadera alteración."[16]

De entre los puntos más importantes que hace mención **Beccaria** destaca los siguientes:

a) "El derecho a castigar se basa en el contrato social y por tanto la justicia humana y la divina son independientes.

b) Las penas únicamente pueden ser establecidas por las leyes; éstas han de ser generales y sólo los jueces pueden declarar que han sido violadas.

c) Las penas tienen que ser públicas, prontas y necesarias, proporcionadas al delito y las mínimas posibles; nunca deben ser atroces.

d) Los jueces, por no ser legisladores, carecen de la facultad de interpretar la ley.

e) El fin de las penas es evitar que el autor cometa nuevos delitos, así como la ejemplaridad respecto a los demás hombres.

La pena de muerte debe ser proscrita por injusta; el contrato social no la autoriza, dado que el hombre no puede ceder el derecho a ser privado de la vida, de la cual el mismo no puede disponer por no pertenecerle. "[17]

---

[16] BECCARIA. TRATADO DE LOS DELITOS Y DE LAS PENAS. Editorial Porrúa. S.A.México1995. pp.408.
[17] Op.cit. P.409.

Finalmente, en conclusión en esta etapa se empieza a ver la calidad de la norma y es derivada de la venganza pública, donde toda acción tenia una reacción y se empezaba a analizar el grado de peligrosidad del delincuente, para que su castigo fuera en proporción al grado de peligrosidad del delincuente y asimismo juzgar la posibilidad de readaptación, ya que en esta etapa se logro un aspecto muy importante para imponer la sanción justa por delito ocasionado por que se exigía que debía haber una ley en la que se mencione cuales eran las penas que se iban a imponer.

ETAPA CIENTIFICA.- "En esta etapa, el delincuente es el objeto de la máxima preocupación científica de la justicia. El delito es una manifestación de la personalidad del delincuente y hay que readaptar a éste a la sociedad corrigiendo sus inclinaciones viciosas. Tal corrección es el pivote sobre el cual gira este nuevo período. La pena como sufrimiento carece de sentido; lo que importa es su eficacia, dado aquel fin. Las ciencias criminológicas vinieron a iluminar el problema hasta su fondo y a caracterizar el nuevo período en el que la personalidad compleja del sujeto es lo que se destaca en el primer término del panorama penal."[18]

En conclusión esta época se basaba en un sistema carcelario, que existiere una norma más perfeccionada, ya más semejante a lo que se vive en la actualidad donde se pretende readaptar al delincuente, por medio de una pena en la que se encuentra privado de su libertad con la finalidad de readaptar a los delincuentes para que cada vez más sea menos el índice de delincuencia, utilizan como medios para dicha readaptación el trabajo, la escuela entre otras actividades, pero si bien es cierto se trata de readaptar a los delincuentes pero en la mayoría de las veces esto no se logra si no al contrario.

[18] CASTELLANOS, Fernando, LINEAMIENTOS ELEMENTALES DEL DERECHO PENAL, México 2002, Editorial Porrúa. Pp.36-37.

1.4 CONCEPCION MODERNA DEL DERECHO PENAL CON EL SURGIMIENTO DE LAS ESCUELAS PENALES.

En la evolución de lo que hoy conocemos como Derecho Penal, tuvo que pasar a través de diferentes etapas, las cuales se hicieron referencia en párrafos precedentes; de dicho desarrollo se formaron las "Escuelas Penales", las cuales como lo menciona "González Quintanilla" en su obra "Derecho Penal Mexicano", son "el cuerpo orgánico de concepciones contrapuestas sobre la legitimidad del derecho de penar, sobre la naturaleza del delito y sobre el fin de las sanciones"."[19]

1.5 ESCUELA CLASICA.

El máximo exponente fue Francisco Carrancá y Trujillo, famoso maestro de pisa, para el maestro de Pisa el delito es una violación del derecho, que como tal se debe sancionar, y se compone de dos elementos o fuerzas que son una moral y otra física".[20]

En otras palabras podemos hacer mención que en Carrancá aparece el planteamiento de la consideración de que el delito es un ente jurídico que se conforma por presupuestos y elementos que son necesarios para la integración de la figura delictiva, y de dos elementos o fuerzas que son una moral esta se integra por conocimiento de la ley, previsión de sus efectos, libertad de elegir y la voluntad de obrar y la fase subjetiva y otra física o bien fase objetiva, en donde estudia el hecho externo, que nace de un movimiento corporal voluntario o bien de una ausencia voluntaria del movimiento corporal.

Sin embargo, Francisco Carrancá Y Trujillo, donde logran definir que el delito es la inflexión del estado promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre positivo o negativo moralmente imputable y políticamente dañoso.

---

[19] GONZÁLEZ Quintanilla, José Arturo. DERECHO PENAL MEXICANO. (PARTE GENERAL) Editorial Porrúa .S.A. México1993. pp.503.
[20] CARRARA, Francisco. PROGRAMA DEL CURSO DE DERECHO CRIMINAL, parte general, volumen I, Editorial Temis, Bogotá, Colombia, P.43.

La escuela clásica mira preferentemente a la acción criminosa, al delito mismo, con la independencia de la personalidad del autor; esto llega a ser para Francisco Carrancá Y Trujillo una especie de garantía individual al afirmar: el juez competente para conocer de la maldad del hecho, no puede tener en cuenta la maldad del hombre sin rebasar el límite de sus atribuciones.

Dando surgimiento a la Escuela Clásica, siendo sus principales conceptos básicos los siguientes:

1.- "El Punto cardinal es el delito, hecho objetivo, y no el delincuente.

2.- El método es deductivo y especulativo.

3.- Sólo puede ser castigado quien realice un acto previsto por la ley como delito y sancionado con una pena.

4.- La pena sólo puede ser impuesta a los individuos moralmente responsables (libre albedrío).

5.- La represión penal pertenece al Estado exclusivamente, pero en el ejercicio de su función, el Estado debe respetar los Derechos del hombre y garantizarlos procesalmente.

6.- La pena debe ser estrictamente proporcional al delito y señalada en forma fija.

7.- El Juez sólo tiene facultad para aplicar automáticamente la pena señalada en la ley por cada delito. "[21]

---

[21] CASTELLANOS, Fernando, LINEAMIENTOS ELEMENTALES DEL DERECHO PENAL, México 2002, Editorial Porrúa.

Para Francisco Carrancá Y Trujillo el delito consiste en "la infracción del estado promulgada para proteger la seguridad de los ciudadanos, resultantes de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso."[22]

Las principales características de esta escuela son:

- "Todos los hombres son iguales.
- Los hombres son libres y tienen la facultad de decidir sobre lo bueno y lo malo.
- El delito existe independientemente del hombre ya que no forma parte interna de el.
- La responsabilidad es de tipo moral.
- Señala un meto deductivo".[23]

En conclusión podemos decir que escuela clásica del Derecho Penal mira preferentemente a la acción criminosa, al delito mismo, con independencia de la personalidad del autor, esto llega a ser una especie de garantía individual como lo afirma el maestro Francisco Carrancá Y Trujillo, asimismo, siguió preferentemente el método deductivo, por ser la adecuada a las disciplinas relativas a la conducta humana, por que el derecho esta constituido en un conjunto de normas y no puede plegarse a los sistemas de las ciencias naturales por no ser parte de la naturaleza y no someterse a sus leyes, sus principales tendencias comunes fueron la igualdad, el libre albedrío, la entidad del delito, la imputabilidad moral y como ya se menciono anteriormente el método deductivo.

---

[22] CARRANCÁ, op cit. P 60.
[23] GARCÍA LÓPEZ, Adolfo de Miguel, DERECHO PENAL, p.7.

1.6 ESCUELA POSITIVISTA.

La escuela Positivista se presenta igualmente como la negación radical de la Escuela Clásica la cual posteriormente, le cedió el paso a la Escuela Positiva, la cual de manera preponderante, en esta rama del pensamiento se toma en cuenta la personalidad del reo como criterio determinante en las disposiciones y las finalidades del Derecho Penal.

Los principales Fundadores de la Escuela Positivista son César Lombroso, Enrique Ferri y Rafael Garófalo.

Para César Lombroso observa al delito desde el punto de vista biológico o físico, donde "el hombre delincuente es un ser salvaje y el criminal es un ser atávico, con regresión al salvaje; el delincuente es un loco, un epiléptico".[24]

Enrique Ferri modifica la doctrina de Lombroso "al estimar que si bien la conducta humana se encuentra determinada por instintos heredados, también debe tomarse en consideración el empleo de dichos instintos y ese uso esta condicionado por el medio ambiente; en el delito concurre, pues, igualmente causas sociológicas".[25]

De la trilogía de los grandes maestros del positivismo penal, Garófalo es el jurista que "pretende dar contextura jurídica a las concepciones positivas y produce la definición del delito natural".[26]

Las directrices conceptual-básicas de la Escuela Positiva Villalobos las resume de la siguiente manera:

1.- El punto de mira de la justicia penal es el delincuente, pues el delito no es otra cosa que un sistema revelador de un estado peligroso.

---

[24] Castellanos. Op cit.60
[25] Castellanos. Op cit.60
[26] CASTELLANOS. Op cit. 60

2.- La sanción penal, para que derive del principio de la defensa social, debe estar proporcionada y ajustada al "estado peligroso" y no a la gravedad objetiva de la infracción.

3.- El método es el inductivo, experimental.

4.- Todo infractor de la ley penal, responsable moralmente o no, tiene responsabilidad legal. "la voluntad está determinada por influjos de orden físico, psíquico y social.

5.- La pena tiene una eficacia muy restringida; importa más la prevención que la represión de los delitos, y por tanto, las medidas de seguridad importan más que las penas mismas.

6.- El Juez tiene facultad para determinar la naturaleza delictuosa del acto y para establecer la sanción, imponiéndola con duración indefinida para que pueda adecuarse a las necesidades del caso.

7.- La pena, como medida de defensa, tiene por objeto la reforma de los infractores readaptables a la vida social, y la segregación de los incorregibles.

Principales características:

- "La responsabilidad es de tipo social.
- La sanción debe corresponder a la peligrosidad del autor
- Importa más la prevención que la represión de los delitos."[27]

Finalmente, en conclusión en la escuela positivista se observa que para César Lombroso, el delito lo contempla desde el punto de vista biológico o físico donde el hombre delincuente es un ser salvaje, a diferencia de Enrique Ferri, el delito desde

[27] Op cit 61-65

el punto de vista natural, genético y hereditario, todo ello proviene de un aspecto social; Sin embargo, Rafael Garófalo, manifiesta que el delito es la violación de los sentimientos de piedad y probidad por lo que es indispensable la adaptación del individuo por la colectividad, a pesar de las divergencias existentes entre los positivistas, se pueden señalar varias concepciones comunes como son el punto de mira de la justicia penal que es el delincuente; la sanción penal para que derive del principio de la defensa social debe estar proporcionada y ajustada al estado peligroso y no a la gravedad objetiva de la infracción.

El método utilizado es inductivo, experimental; todo infractor de la ley penal responsable moralmente o no, tiene responsabilidad legal; la pena posee una eficacia muy restringida en donde importa más la prevención que la represión de los delitos; el juez tiene la facultad para determinar la naturaleza delictuosa del acto u por ultimo la pena como medida de defensa, tiene por objeto la reforma de los infractores readaptables a la vida social.

1.7 ESCUELA ECLÉCTICA

La Tercera Escuela, es una posición ecléctica entre las dos escuelas anteriores, tomando conceptos fundamentales de los clásicos y también de los positivistas, estimando al delito como un fenómeno individual y social, orientándose al estudio científico del delincuente y de la criminalidad; niega el libre albedrío si éste es considerado en toda su dimensión; acepta el principio de la responsabilidad moral distinguiendo entre imputables e inimputables; sin embargo, "no se estima al delito como un acto realizado por alguien con libertad absoluta, sino que existen motivos que determinan y coaccionan psicológicamente al infractor; se inclina más por estimar la pena como una defensa social."[28]

[28] Op. cit. pp.69-72

Principales características:

- Se admite del positivismo la negación del libre albedrío y concibe al delito como un fenómeno individual y social, se inclina hacia el estudio científico del delincuente.

- De la escuela clásica acepta el principio de la responsabilidad moral y hace la distinción entre el delincuente imputable e inimputable.

En atención a lo anterior podemos decir que la escuela ecléctica es la unión de la escuela clásica y positivista ya que estima al delito como un fenómeno individual y social, ya que se encuentra en el individuo por naturaleza, por tal motivo, se orienta al estudio científico del delincuente y de la criminalidad; para su estudio del grado de criminalita o peligrosidad del delincuente.

En esta etapa, se niega el libre albedrío si éste es considerado en toda su dimensión; asimismo, acepta el principio de la responsabilidad moral distinguiendo entre imputables e inimputables; en donde diferencia entre los delincuentes que pueden ser castigados por tener toda la intención de delinquir y los que delinquen por tener algún mal psicológico, sin embargo, no se estima al delito como un acto realizado por alguien con libertad absoluta, sino que existen motivos que determinan y coaccionan psicológicamente al infractor; se inclina más por estimar la pena como una defensa social, para lograr un menor índice de delincuencia.

CAPITULO II.

2.1 Evolución doctrinal de las diversas teorías elaboradas para el estudio del delito

2.2 Teoría Causalista

2.3 Teoría Finalista

2.4 Conclusión y diferencias de la teoría Causalista y Finalista de la acción.

2.5 Principales diferencias entre la teoría Causalista y Finalista de la acción.

2.6 Dualidad entre la teoría Causalista y Finalista de la acción

2.7 Teoría del funcionalismo Social

2.8 Teoría psicologista de la culpabilidad

2.9 Teoría normativista de la culpabilidad.

2.10 Teoría sociologista.

2.11 El delito defunción legal y doctrinaria.

2.12 Elementos del delito

2.13 La conducta

2.14 La ausencia de conducta

2.15 La tipicidad

2.16 La ausencia de tipicidad

2.17 La antijucididad

2.18 Las causas de justificación

2.19 La imputabilidad

2.20 La inimputabilidad

2.21 La culpabilidad

2.22 Formas de comisión del delito

2.23 La inculpabilidad

2.24 Las condiciones objetivas de punibilidad

2.25 La falta de condiciones objetivas

2.26 La punibilidad

2.27 Las excusas absolutorias

CAPITULO II.

2.1 EVOLUCIÓN DOCTRINAL DE LAS DIVERSAS TEORÍA ELABORADAS PARA EL ESTUDIO DEL DELITO:

Para el estudio del delito y sus elementos, se han creado diversas corrientes doctrinarias, por lo que en este capitulo no se pretende hacer un análisis profundo sobre diversas teorías que han surgido para estudiar al delito, solo mencionare a las teorías del delito conforme al siglo XX que se han considerado de mayor importancia como son la Teoria Causalista, Finalista de la acción y Funcionalista, ya que estamos conscientes que para su análisis es recomendable un estudio profundo como lo sería un tema de tesis unitario, para un estudio completo, como ya lo sabemos han creado mucha polémica, sin embargo esta tesis, no tiene como propósito explicar las numerosas tendencias que los juristas manejan sobre los elementos del delito, sino solo tratar de explicar lo que es el delito y sus elementos para poder entender que las conductas antisociales generadas por las computadoras pueden ser consideradas como delitos informáticos..

2.2 TEORÍA CAUSALISTA

La acción es un aspecto del delito y para **la teoría Causalista** "es un comportamiento humano dependiente de la voluntad (voluntario), que produce una determinada consecuencia en el mundo exterior, que puede consistir en el puro movimiento corporal, seguido del resultado ocasionado por él en el mundo exterior."[29]

El sistema jurídico penal llamado Causalista nace a partir de la obra Franz Von Liszt, quien se apoya en el concepto de acción como "un fenómeno causal natural como punto de partida del delito. La explicación naturalística del acto o acción humana, se basa en relaciones de procesos causal es acción que nace de un

[29] JESCHECK, Hans-Heinrich, TRATADO DE DERECHO PENAL, PARTE GENERAL, Volumen I, 3ª Edición, Ed. Bosch, Barcelona,1998 p292

movimiento corporal que es un proceso, que va a producir un cambio en el mundo exterior, es decir, un efecto, y entre una y otro se da una relación".[30]

El acto o acción humana y su efecto en el mundo material, son un proceso causal; como todo proceso causal natural que parte de una causa, produce une efecto.

Para algunos causalitas el término acción o acto es comprendido del concepto de omisión. Otros autores prefirieron el uso de otros términos, como conducta, hecho, o acontecimiento, que abarcaban los conceptos de acción u omisión. No es el momento de profundizar en esta debatida cuestión conceptual, y por ahora nos limitaremos a hablar de acto o de acción (en sentido lato) como comprensivas tanto de la acción (en sentido estricto) como de la omisión.

Liszt señala que la acción humana debe ser voluntaria, pero que tal voluntariedad está referida únicamente al movimiento corporal que produce un resultado material, donde sólo existe una relación de causalidad entre ese movimiento corporal voluntario y el resultado material.

El movimiento corporal voluntario resulta así un proceso causal "ciego", es decir, en donde no interesa el sentido o fin de la acción.

Desprende Liszt que la voluntad tiene dos caracteres: "uno interno, contenido de la voluntad; y otro externo, la manifestación de la voluntad".[31]

En la teoría Causalista en el estudio del acto, o acción, lo que interesa es la fase externa, la interna corresponde a otro nivel, es decir, a la culpabilidad, donde se analiza si el contenido de la voluntad fue doloso o culposo.

---

[30] ORELLANA, Wiarco Octavio Alberto. TEORÍA DEL DELITO. Ed. Porrúa, 6ª EDICIÓN, México 1998. p. 7-2-4
[31] Op. cit. p 12-14

Asimismo, en el terreno de la acción únicamente debe plantearse lo relativo a la manifestación de la voluntad no el por qué de la misma, o sea, su finalidad.

El maestro Jiménez de Asúa comparte el punto de de Liszt de que la acción no está matizada con la que persigue: que es acromática, y así nos dice: "A nuestro juicio, de acuerdo con Von Liszt, se debe dar a la **acción** personalidad propia. "Es lo natural, que no debe teñirse prematuramente de valor jurídico". [32]

De esta suerte la acción es un factor de orden natural desencadenante de un resultado material, es simple y sencillamente un proceso causal.

A partir de Liszt el sistema Causalista señala que los subelementos que integran a su vez al elemento acto, o acción son:

a) "Manifestación de la voluntad, que consiste en la inervación voluntaria del cuerpo humano que se traduce es un movimiento corporal, o en su inactividad (cuando nos hallamos frente a la omisión).

b) Un resultado, que es la mutación en el mundo exterior, causado por la manifestación de la voluntad, o la no mutación de ese mundo exterior por la acción esperada que el sujeto no realiza, y

c) Un nexo causal, que radica en que el acto, acción o conducta ejecutada por el sujeto, produzca el resultado previsto en la ley, de tal manera que entre uno y otro exista una relación de causa a efecto".[33]

[32] JIMÉNES DE ASÚA, Luis, LA LEY Y EL DELITO, P 213
[33] Op cit. P 215

Esta teoría trata a la acción como factor causal del resultado, sin tomar en cuenta la intención que llevó al sujeto a cometerlo, de "la acción solo importa si el comportamiento movido por la voluntad, causo el resultado y no así, si la voluntad iba dirigida a éste."[34]

Maurach, "considera irrelevante para la acción, debe aparecer en otro lugar de la construcción del delito, en la configuración del dolo, en el sentido propio de un *dolos malus*, será albergado como característica de la culpabilidad".[35]

Por otra parte, Zaffaroni, considera a la acción como "un movimiento voluntario, no reflejo, pero que carece de importancia o se prescinde a que esa voluntad se dirige".[36]

Como reacción al pensamiento del positivismo sociológico y obviamente a su metodología que había llevado al Derecho Penal al campo de la sociología, pero que, a la vez, recoge también la influencia de aquel, se manifestó en Alemania el pensamiento de Franz Von Lizt. Bajo la influencia del positivismo, el concepto del "delito" aparece recogido y estudiado en un plano naturalistico y causal, por lo que ese esquema lo lleva a plantear el análisis del delito bajo el binomio de los elementos objetivo y subjetivo, apareciendo la concepción del delito como un hecho en sentido objetivo y causal, denominado como comportamiento o conducta, conteniendo el resultado y el nexo causal.

Para determinar la existencia del delito se une también, el análisis de la antijuricidad, entendida como un juicio de valor objetivo relativo a la contradicción del hecho con el derecho, con lo que se integra el elemento objetivo del delito.

El elemento subjetivo, está constituido por el nexo de relación psicológica entre el querer del agente y la causación de producción del resultado, que es el ámbito en que se precisa la culpabilidad.

---

[34] BETANCOURT López, Eduardo. TEORIA DEL DELITO. Editorial Porrúa. S.A.México1994 pp.5-11.
[35] MAURACH, Reinhart. TRATADO DEL DERECHO PENAL. Tomo I, Barcelona p. 202.
[36] ZAFFARONI, Eugenio Raúl. MANUAL DEL DERECHO PENAL PARTE GENERAL. Ed. Cárdenas Editor y Distribuidor, México, 1991 pp. 369-370.

En síntesis, la teoría Causalista Von List analizó de manera sistemática al delito, cuyos caracteres esenciales eran los siguientes:

- "El delito siempre es un acto humano; por tanto, actuación voluntaria trascendente en el mundo exterior; es decir, la causa o no impedimento de un cambio en el mundo exterior. Nunca llegarán a constituir un delito los acontecimientos fortuitos, independiente de la voluntad humana.

- El delito es, además, un acto contrario al derecho; es decir un acto que contraviniendo, formalmente, a un mandato o prohibición del orden jurídico, implica, materialmente, la lesión o peligro de un bien jurídico.

- El delito es, por último, un acto culpable; es decir un acto doloso o culposo de un individuo responsable".[37]

Por tal motivo, se valora los elementos positivos y negativos del delito de la siguiente manera:

1.- CONDUCTA: como un movimiento corporal, que es la causa de una modificación en el mundo exterior, cuya percepción se constata a través de los sentidos.

2.- TIPICIDAD: Función significadora y sistematizado de la teoría del delito, que como instrumento técnico garantizara el principio de legalidad, garantía del individuo frente al poder punitivo del estado.

[37] DIAZ, Aranda Enrique, DERECHO PENAL PARTE GENERAL, Ed. Porrúa, Mexico 2003. p.115.

Tipo penal

- Complementados
- Circunstanciados
- subordinados
  - Cualificados
  - privilegiados

3.- ATIPICIDAD: Se presenta en el momento en que falte alguno de los elementos del tipo penal.

"Aquellas conductas que no están descritas en algún tipo penal de denominan atípicas y se consideran irrelevantes pera el derecho penal, conforme a la formula *nullus crimen nulla poena sine lege,* creada por Feuerbach".[38]

También se consideran atípicas las conductas que no reúnen todos los elementos descritos en el tipo.

4.- ANTIJURICIDAD: Es contrario al del derecho o bien el injusto, en otras palabras contrario a la norma.

5.- CULPABILIDAD: Existen dos especies de culpabilidad que son.

- **DOLO**: Es la intención de realizar el elemento previsto, violando un deber jurídico.

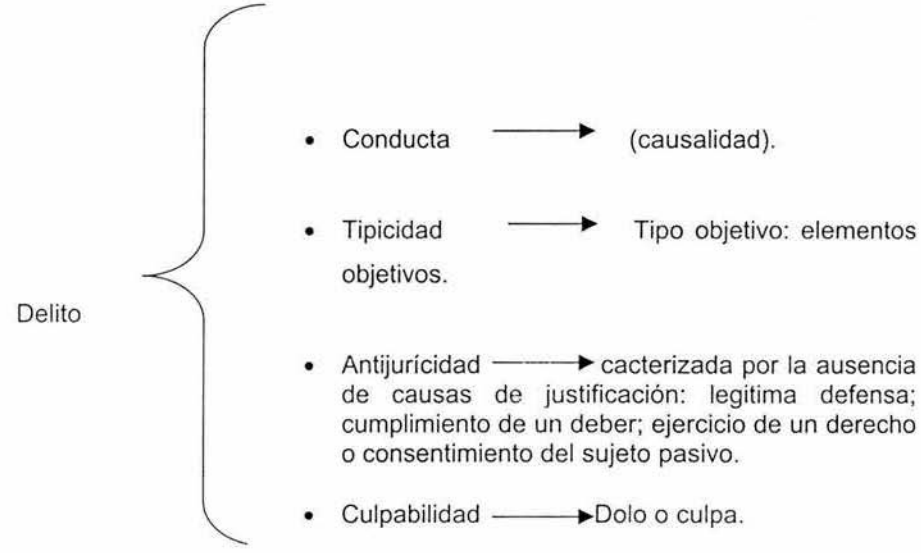
- **CULPA**: Producción de un resultado típicamente antijurídico que pudo y debió ser previsto y que por negligencia, imprudencia o impericia del agente causa un efecto dañoso.

[38] DIAZ, Aranda Enrique, DERECHO PENAL PARTE GENERAL, Ed. Porrúa, México 2003 p 116

Von Liszt esbozó el sustento puramente psicológico de la culpabilidad al manifestar "la relación subjetiva entre el hecho y el autor solo puede ser psicológica".[39]

SISTEMA CLASICO (CAUSALISTA).

A partir de 1907 se pudo desarrollar la teoría del delito conforme a los postulados del sistema clásico (Causalista) sustentado en un presupuesto y tres categorías, cuya estructura es la siguiente:



En la conducta, la tipicidad y la antijuricidad se analizaban exclusivamente la parte objetiva del delito, mientras que se reservaban a la culpabilidad todos los aspectos subjetivos.

[39] DÍAZ, Aranda Enrique. DERECHO PENAL PARTE GENERAL. Ed. Porrúa, México 2003. p.117-119

SISTEMA NEOCLÁSICO (CAUSALISTA-VALORATIVO).

Edmund Mezger modificó los postulados del sistema clásico debido a las múltiples críticas a que fue sometido, sobre todo, por que rechazaba someter a las ciencias del espíritu a los principios de las ciencias naturales, por lo cual reoriento a la dogmática penal a través del empleo de un método propio de las ciencias del espíritu o ciencias culturales, al cual se le denomino "método comprensivo".[40]

Con lo anterior, puso de manifiesto que era erróneo dividir tajantemente el análisis del delito en parte objetiva-material, (conducta, tipicidad y antijuricidad) y parte subjetiva (culpabilidad), motivo por el que Mezger también se "aparto de la concepción positivista afirmando que la ley no es lo único en el derecho, pues la dogmática jurídico-penal, debe atender al ser espiritual del derecho en su búsqueda por la justicia".[41]

La estructura del sistema neoclásico era la siguiente:

Delito

- Conducta ⟶ (causalidad adecuada), ya que se sustentaba un juicio valorativo sobre la idoneidad o la adecuación de la conducta para provocar ese resultado.
- Tipicidad ⟶ Se requería verificar tanto los elementos objetivos del tipo, normativos y subjetivos específicos cuando el tipo así lo requeria.
- Antijuricidad ⟶ cacterizada por la ausencia de causas de justificación: legitima defensa; cumplimiento de un deber; ejercicio de un derecho o consentimiento del sujeto pasivo, por lo que también debia atender a los elementos subjetivos del injusto.
- Culpabilidad ⟶ Imputabilidad, dolo o culpa y ausencia de causas excluyentes de culpabilidad, esto es que se requería tanto la valoración subjetiva como las circunstancias materiales que roderaon al hecho y establecer si podían reprocharle a la persona el habberse comportado contrariamente a derecho.

[40] DIAZ, Aranda Enrique, Op cit p 118.
[41] MEZGER, TRATADO DEL DERECHO PENAL, Madrid, 1995, p.11-20.

En conclusión podemos decir que los causalistas explican la existencia de la acción delictiva como un factor causal del resultado, sin tomar en cuenta la intención que llevó al sujeto a cometerlo y cuando un sujeto tiene la voluntad de realizarla, sin tomar en cuenta necesariamente la finalidad que se proponía al hacerlo, por que ésta no pertenece a la conducta o hecho, por lo que a la acción se le considera como un hacer voluntario, pero en esa voluntad no hay contenido y se concibe a la acción como un proceso causal natural y extrajurídico, libre de valor como simple causación, sin tomar en cuenta la voluntad rectora, contempla la sola producción del acto en el mundo externo y no el actuar lleno de sentido, separan el contenido de la voluntad, es decir, la finalidad, el propósito con que o por que se hace algo, limitando a la acción a aparecer únicamente como función causal.

2.3 LA TEORÍA FINALISTA

Planteada en la tercera década del siglo XX, procuró seguir el análisis científico de la ley penal, intentando superar las contradicciones que se apuntaban en los esquemas precedentes de la dogmática penal.

Surge así, la corriente del finalismo o teoría de la acción final, corresponde a Hans Welzel ser el creador del finalismo y poner las bases de la nueva construcción de esta estructura sistemática penal.

El punto de partid de la teoría finalista como su nombre lo indica, una concepción distinta de la acción de la que maneja la teoría casualista.

Ahora bien, para la teoría finalista de "la *acción humana es el ejercicio de la actividad finalista"*, por lo tanto, un acontecimiento "finalista" y no solamente "causal". La "finalidad" o actividad finalista de la acción se basa en que el hombre, sobre la base de conocimiento causal, puede prever en determinada, por lo que se compone de dos fases".[42]

[42] MUÑOZ, Conde Francisco, TEORIA GENERAL DEL DELITO, P.10

FASE INTERNA:

a) El objetivo que se pretende alcanzar o proposición de fines

b) Los medios que se emplean para su realización.

c) Las posibles consecuencias concomitantes o secundarias que se vinculan con el empleo de los medios, que pueden ser relevantes o irrelevantes para el derecho penal.

FASE EXTERNA:

a) "La puesta en marcha, la ejecución de los medios para cristalizar el objetivo principal.

b) Los resultados previstos y concomitantes.

c) El nexo causal".[43]

En síntesis, la teoría finalista considera como los elementos positivos y negativos del delito los siguientes:

1.- **"CONDUCTA O HECHO:** Es la acción humana es el ejercicio de la actividad finalista.

---

[43] MUÑOZ, Conde Francisco. TEORIA GENERAL DEL DELITO. P 11 Y 12

- Dolo: Voluntad de realizar el hecho tópico.

- Culpa: La voluntad de acción no se dirige al resultado típico, que se proyectan con consecuencias intolerables socialmente, en donde el sujeto confía en que no se producirá o ni siquiera pensó en su producción.

2.- AUSENCIA DE CONDUCTA: Cuando no se presentan las fases en que se puede dar la acción, es decir, cuando el sujeto no se ha planteado la realización de un fin, no ha seleccionado los medios para lograrlo o no ha considerado los efectos concomitantes.

- ✓ **MOVIMIENTOS REFLEJOS**
- ✓ **SUEÑO**
- ✓ **SONAMBULISMO**
- ✓ **HIPNOTISMO**

Estados de inconciencia.

Acciones libres en causa

- **VIS-MAIOR**: Fuerza mayor, es aquella fuerza que no se puede resistir proveniente de la naturaleza.

- **VIS-ABSOLUTA**: Fuerza física exterior irreversible, cuando supera la voluntad del sujeto en tal modo que es incapaz de autodeterminarse.

2.- TIPICIDAD: Es el encuadramiento de la conducta al tipo penal.

3.- ATIPICIDAD: Se presenta en el momento en que falte alguno de los elementos del tipo penal.

- Falta de un bien jurídico tutelado.
- Falta de objeto material
- Inidoneidad en dos medios.

4.- ANTIJURICIDAD: Es contrario al del derecho o bien el injusto, en otras palabras contrario a la norma.

5.- CAUSAS DE JUSTIFICACIÓN: Aquellas causas que excluyen la antijuricidad de una conducta que puede subsumirse en un tipo legal, eso es, aquellos actos u omisiones que revisten un aspecto del delito.

6.- CULPABILIDAD: Existen dos especies de culpabilidad que son:

•**DOLO:** Es la intención de realizar el elemento previsto, violando un deber jurídico.

•**CULPA**: Producción de un resultado típicamente antijurídico que pudo y debió ser previsto y que por negligencia, imprudencia o impericia del agente causa un efecto dañoso.

7.- INCULPABILIDAD: Es la no configuración del dolo y la culpa como son las causas genéricas que excluyen de la culpabilidad las siguientes

- La minoría de edad hasta los 14 años, donde existe incapacidad de inculpabilidad a causa de su inmadurez mental y social.

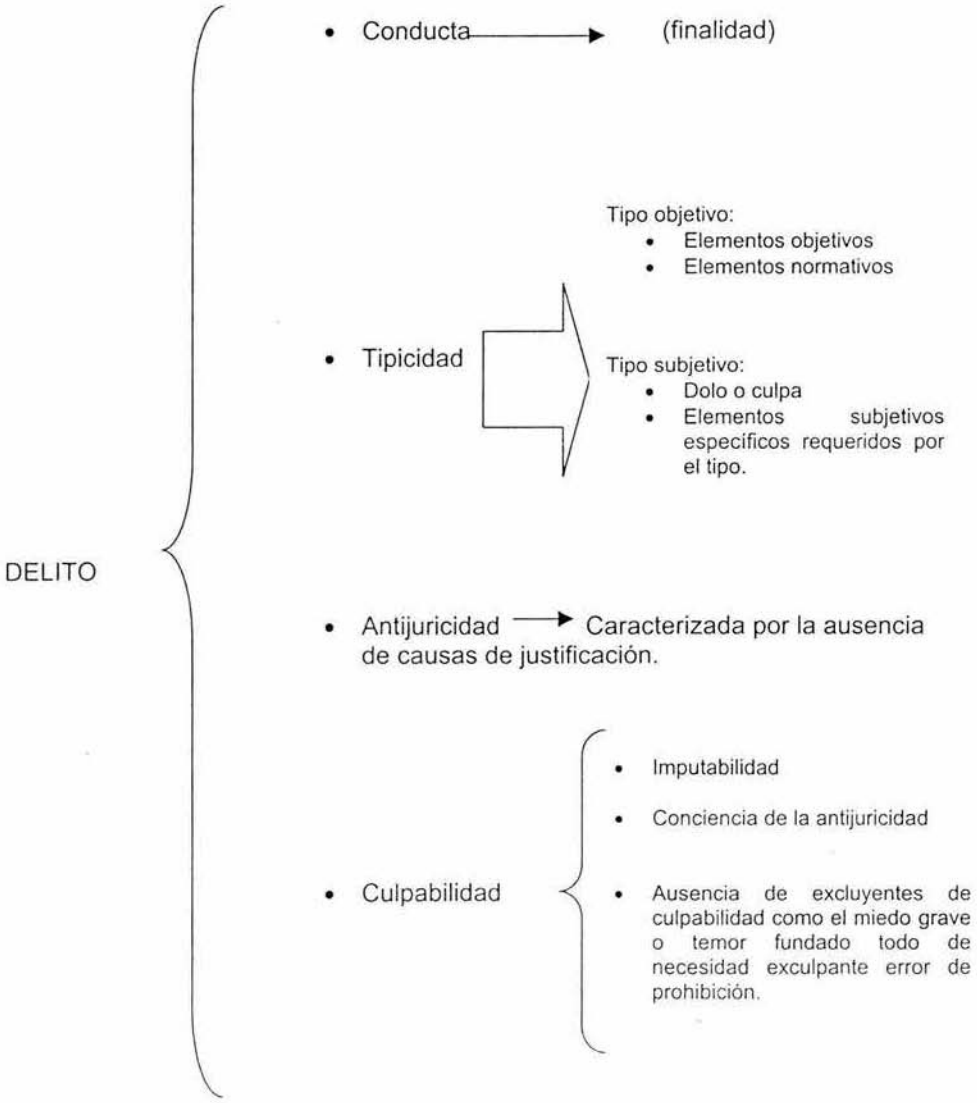
- La capacidad eventual de culpabilidad, para quienes hayan cumplido de los 14 a los 18 años de edad.

- Los sujetos con capacidad eventual de culpabilidad, como en el caso del sordomudo que a causa de su dolencia es retardado mental.

- La incapacidad de culpabilidad que se presenta en los estados mentales".[44]

[44] ORELLANA, Octavio Alberto Wiarco, LA PRETERINTENCIONALIDAD, TERCERA PARTE DE LA CULPABILIDAD, México 1959, p. 128-129.

El sistema finalista, fue expuesto en toda su extensión hacia 1940, para quedar como sigue:



Finalmente, concluimos que esta teoría reconoce esencialmente la base de que el hombre es un ser social responsable, que actúa conforme a un sentido, por lo que sus acciones aparecen invariablemente impregnadas de la finalidad por la propuesta, lleva a reconocer que, concretamente en el Derecho Penal, el acto, a partir de la voluntad y de la conciencia es lo que determina el contenido del orden valorativo jurídico. En otras palabras, el orden jurídico es un orden de regulación de la conducta humana, que es por esencia eminentemente final, es decir, caracterizada por su voluntad finalisticamente determinada, el ser humano aprovecha su conocimiento acerca de los procesos causales a fin de determinar la realización de sus objetivos.

2.4 CONCLUSIÓN Y DIFERENCIAS ENTRE LA TEORÍA CAUSALISTA Y FINALISTA DE LA ACCIÓN.

En forma resumida y abordando los principales puntos de divergencia entre el sistema Causalista y el finalista, exponen las siguientes conclusiones, que se apoyan en lo ya expuesto en este trabajo.

"La necesidad de perfeccionar las leyes penales y su aplicación es ineludible, la política criminal debe estar constantemente atenta a todo aquello que garantice una mejor convivencia social, sin detrimento de los derechos fundamentales del individuo".[45]

La profundización de los conceptos que conforman la teoría del delito es una consecuencia de esa necesidad, siempre perenne de sistematización que apoyada en el estudio de la ley proporcione los instrumentos valiosos para su conocimiento y aplicación.

---

[45] Castellanos, Op cit 76

No han faltado voces que consideran inútil y nociva la extrema tecnificación del estudio de la teoría del delito; tal parece que sólo unos cuantos, pueden ser capaces de comprender sus misterios, contra el principio de que las leyes, al estar dirigidas a todos, deben ser sencillas y comprensibles para el común denominador.

No cabe duda, que en parte, estas críticas son acertadas y por ello debemos procurar que las leyes penales, su interpretación y aplicación se vayan haciendo cada vez más sencillas y comprensibles.

El sistema como explicación coherente del estudio del delito y la ley, pretende ser instrumento valioso para quien al servirse de ella encuentre respuesta a múltiples problemas jurídico-penales de la vida cotidiana.

"El causalismo maneja una explicación de relaciones de causa a efecto, para explicar el delito. Así el primer elemento del delito, la acción, es una relación de causa a efecto, en la que únicamente interesa la manifestación la voluntad para la ejecución de los movimientos corporales, no así la finalidad de esa acción que como proceso subjetivo corresponde al estudio de la culpabilidad, la acción es "ciega".[46]

El sistema de la acción finalista rechaza esta concepción que considera reñida con la propia realidad y con lo preceptuado por la ley. No es posible, a su juicio, separar la voluntad de ejecutar una acción, de su finalidad; la acción es "vidente". Lo importante no es el resultado, como destaca el causalismo, sino la propia acción.

El causalismo coloca en el plano objetivo a la acción, la tipicidad y la antijuridicidad; a la culpabilidad pertenece lo subjetivo. El finalismo plantea que tal división forza la realidad, pues quien ejecuta una conducta toma en cuenta la finalidad de la misma.

---

[46] Castellanos, Op cit 78

La tipicidad para el sistema Causalista, aparece cuando la conducta encuadra en el tipo, en la norma, pero este encuadramiento es en relación a los elementos objetivos del tipo. La aparición de los elementos subjetivos del tipo fue uno de los problemas más serios que se plantearon a este sistema, y Binding elude la cuestión, sin conseguirlo, diciendo que estos llamados elementos subjetivos, son objetivos porque aparecen en la ley.

"El sistema finalista considera que al tipo corresponden elementos objetivos y subjetivos (también normativos) y que dentro de los elementos subjetivos muy destacadamente aparece el dolo y la culpa. Agrega este sistema, que ,la ley, al señalar por ejemplo, "al que ejecute"; "a quien cometa"; etc., está exigiendo que la acción típica tenga un contenido doloso, por lo que es congruente incluir en el tipo, el dolo (y la culpa), y no separarlos arbitrariamente, como lo hace el causalismo".[47]

El causalismo no puede explicar la tentativa atendiendo a una "acción ciega" y a un resultado no producido, en efecto, cómo saber qué se propuso el sujeto si sólo podemos formarnos un juicio sobre su mero comportamiento corporal y el resultado no aconteció. El finalismo al señalar que la acción es "vidente", no requiere del resultado para explicar cuál fue la finalidad del sujeto, ya que a este nivel se estudia su conducta dolosa. En forma semejante Ya a resolver el finalismo los problemas de la participación en el delito, partiendo de la acción finalista de cada participante, lo que el sistema Causalista no puede lograr al poner su énfasis en el resultado y porque el estudio del dolo, de su intención, de su, finalidad la remite a la culpabilidad.

El finalismo ubica en la teoría del tipo el estudio de error de tipo, referido a los errores invencibles, vencibles o irrelevantes, en que la conducta dolosa puede incurrir respecto de los elementos del tipo.

[47] Castellanos. Op cit 78

Así el error invencible destruiría el dolo de tipo, el vencible, podrá dar lugar a la culpa y el irrelevante dejará intacto el dolo. También se debe al finalismo la elaboración de la teoría del error de prohibición, que también puede ser invencible o vencible, el primero anula la culpabilidad del sujeto porque incurre en un error insuperable sobre la conciencia de la antijuricidad de la conducta, el error vencible da lugar a culpabilidad disminuida.

La teoría Causalista habla del error de hecho invencible y errores accidentales, pero los estudia en relación a la culpabilidad.

En el causalismo, el estudio de la *antijuridicidad* se ubica en un plano objetivo, sin embargo, el problema de elementos subjetivos del injusto vuelve a plantear problemas que quedan insolubles. El finalismo al ubicar el dolo y otros aspectos subjetivos en el tipo, no se plantea esas incongruencias del sistema Causalista.

Los causalistas colocan al dolo y la culpa en el terreno de la culpabilidad, y a la imputabilidad, como un presupuesto de la propia culpabilidad.

"El sistema finalista ubica, como ya hemos dicho al dolo y la culpa en el tipo, y a la culpabilidad le reserva el importante papel de llevar a cabo "el reproche" de conducta típica, apoyado en la posibilidad de poder actuar en el conocimiento de la *antijuridicidad,* y en la exigibilidad de conducta diversa a la ejecutada. La culpabilidad "reprocha" que el sujeto no se haya *motivado* en el sentido exigido por la norma".[48]

Se acusa al finalismo de haber dejado "vacía" a la culpabilidad, al despojarla del dolo y la culpa, Eduardo López Bentancur crítica que no nos parece acertada, pues la culpabilidad no ha quedado "vacía", sino que se le coloca en su verdadero papel, en aquel en donde al sujeto se le va a valorar, a "reprochar", por no haberse motivado a obrar conforme a la norma, conforme a los valores aceptados por la ley.

---

[48] Castellanos. Op cit 78

La culpabilidad va a ser la medida de la pena; qué papel más importante y delicado podemos concebir.

En consecuencia de la diversa solución, que le asignan causalistas y finalistas a los elementos del delito, también es diversa solución a los aspectos negativos del delito, desde los casos de ausencia de conducta, atipicidad, causas de justificación, y de inculpabilidad, que ya se fueron apuntando a lo largo de este trabajo.

La teoría finalista se ha venido abriendo campo en la teoría del delito. En México han predominado los penalistas afiliados al sistema Causalista, de ellos recibimos en las aulas y en la vida profesional múltiples enseñanzas, y para todos ellos nuestros respetos, pero seguros estamos de que el sistema finalista se seguirá abriendo camino; más aún, ya otros sistemas, algunos inspirados o basados en el finalismo, aparecen planteando nuevas soluciones, como son la teoría de la acción social, y muy especialmente el sistema lógico matemático propuesto por distinguidos penalistas mexicanos.

Por otra parte, en el siguiente imagen podemos observar de una mejor forma la estructura de la teoría causalista y finalista.

2.5 PRINCIPALES DIFERENCIAS ENTRE LA TEORÍA CAUSALISTA Y FINALISTA DE LA ACCIÓN.

"CAUSALISMO	FINALISMO
Considera la acción como un producto causal y mecánico	Existe una voluntad orientada en determinado sentido
No previene el resultado	La conducta tiene una finalidad
No estudia la intención del sujeto al realizar la conducta".[49]	

[49] APUNTES DE TEORÍA DEL DELITO EN LA LICENCIATURA EN DERECHO.

2.6 DUALIDAD ENTRE LA TEORÍA CAUSALISTA Y FINALISTA DE LA ACCIÓN.

1.- Los causalistas ubican en la culpabilidad al Dolo y la Culpa, mientras que los finalistas lo hacen en el tipo Penal de los delitos Dolosos

2.- Para los finalistas la Antijuricidad es una cuestión de la culpabilidad, independiente del Dolo; para los causalistas la Antijuricidad es parte del Dolo.

3.- Los Causalistas entienden que todos los elementos de la culpa corresponden a la cuestión de la culpabilidad; Los finalistas señalan que la infracción del deber de cuidado que caracteriza a la culpa debe abordarse en la tipicidad.

4.- La Imputabilidad en ambas teorías constituye un elemento del delito, pero en la teoría Causalista se considera un elemento autónomo e independiente; mientras que en la Finalista forma parte de la culpabilidad.

2.7 TEORÍA DEL FUNCIONALISMO POLÍTICO CRIMINAL

Después de las consecuencias de la segunda guerra mundial, se pronunció el interés de incorporar el respeto a los derechos humanos dentro de la legislación mundial.

A la vez, esta situación se reflejó en el campo de le ley penal, en una tendencia frecuentemente apuntada como orientación político criminal, significó la necesidad de entender el contenido de la propia ley penal en relación con la realidad social. Es decir, de entender que el Derecho tiene un contenido social y que esa realidad social, no solamente tiene que ser regulada, sino entendida y atendida por el Derecho, como consecuencia de los fines de la seguridad jurídica para la convivencia, sobre la base de protección a los bienes jurídicos de los miembros de la comunidad.

Uno de los principales sostenedores de éste teoría, Claus Roxin, señala "que el análisis del Derecho Penal exige tomar en cuenta sus fines; son los fines de política criminal del derecho los que deben dar la luz para explicar y para determinar la existencia del delito; la responsabilidad del autor y tercero para determinar la aplicación de la pena en base, precisamente a sus fines de política criminal".[50]

Finalmente, concluimos ya que en México, después de tener bastante tiempo adoptada la teoría Causalista en el Derecho Penal, se tomó la doctrina finalista, la cual se encuentra plasmada en la mayoría de nuestras legislaciones penales de las entidades que conforman la República Mexicana, así como en nuestra propia Constitución, sin embargo, consideró que se ha sufrido un retroceso en el avance del derecho penal, al mencionarse nuevamente el cuerpo del delito en el artículo 14 Constitucional, al tomarse nuevamente la teoría Causalista, para tener por demostrado el cuerpo del delito, circunstancia que impide desarrollar la legislación penal en sus ámbitos, toda vez que el finalismo proclama el resultado y el fin buscado por el sujeto, para tener por demostrado si este actúo dolosamente o culposamente o bien, no es responsable del resultado de la acción; al avance que se tenía en el ámbito del Derecho Penal se ha estancado, al tener el creador de la norma y del Derecho Penal, dudas respecto al finalismo, no obstante que éste, haya sido adoptado por la mayoría de las legislaciones de habla hispana y del Derecho Escrito.

2.8 TEORÍA PSICOLOGISTA DE LA CULPABILIDAD

Para el estudio de la culpabilidad, se considera otro elemento del delito que consiste en el nexo causal que une al sujeto con su acto.

Teoría psicologista o psicológica Para esta concepción, la culpabilidad en carácter psicológico, dejando toda valoración juridicidad para la antijuricidad, ya supuesta; la esencia de la culpabilidad consiste en el proceso intelectual-volitivo desarrollado en el autor, el estudio de la culpabilidad requiere el análisis psíquico del

[50] BETANCOURT López, Eduardo. TEORIA DEL DELITO. Editorial Porrúa. S.A México1994 pp.13-19.

agente, a fin de indagar en concreto cuál a sido su actitud respecto al resultado obviamente delictuoso, lo cierto es que la que la culpabilidad con base psicológica, consiste en un nexo psíquico entre el sujeto y el resultado; lo cual quiere decir que contiene dos elementos: uno volitivo, o como lo llama Jiménez de Asúa, o emocional; y otro intelectual. "El primero indica la suma de dos quereres: de la conducta y del resultado; y el segundo el intelectual, el conocimiento de la antijuridicidad de la conducta".[51]

No es aceptable la teoría psicológica de la culpabilidad, ya que el dolo o la culpa no bastan para integrarla, la concurrencia de la irreprochabilidad de ese nexo psicológico; de otra manera existiría la culpabilidad en los casos de defensa.

La culpabilidad para esta teoría no es sino otra cadena de relaciones que parten de la acción causal de la conducta que encuadra en un resultado típico; a la relación subjetiva, psíquica de su autor y ese resultado, sea a titulo culposos o doloso.

Vicenso Cavallo nos explica que 2la teoría psicologista se limita a establecer la relación psíquica del agente, pero no explica la razón por la cual éste es culpable".[52]

Finalmente, en conclusión podemos hacer mención que la corriente psicologista, la culpabilidad es el nexo psicológico que une al sujeto con su conducta, se agota en los elementos del dolo y la culpa, descubre que el estado de necesidad del sujeto activo actúa con estos dos elementos por lo que se dice que es insuficiente, asimismo, La culpabilidad con base psicológica, consiste en un nexo psíquico entre el sujeto y su conducta o el resultado material, según se trate de un delito de mera conducta o de resultado material.

[51] CASTELLANOS, Fernando, LINEAMIENTOS ELEMENTALES DEL DERECHO PENAL, México 2002, Editorial. Porrúa. Pp.234.
[52] ORELLANA, Octavio Alberto Wiarco, LA PRETERINTENCIONALIDAD, TERCERA PARTE DE LA CULPABILIDAD, México 1959, p. 44 y 45.

2.9 TEORÍA NORMATIVISTA DE LA CULPABILIDAD.

Reinhart Frank, profesor de la universidad de Munich, quien en 1907 fue calificado de "padre de la teoría normativa", al sostener que una acción realizada, no siempre es una acción culpable porque no es reprochable, y no lo es porque hay muchas que es imposible exigir al agente que obre conforme a la norma. Por consiguiente, la culpabilidad no consiste en un nexo psicológico entre el agente y su propio acto, si no en el juicio que los demás se formen de si se ha de un modo contrario a su deber, pudiendo haber obrado conforme al mismo, este juicio del mundo tiene un contenido de reproche, y así la esencia de viene a ser la reprobabilidad del injusto típico, de esta manera se lograba algo que no había no habría podido alcanzar psicologuismo, a saber: "unificar el concepto de culpabilidad tanto para los delitos dolosos como para los culposos, ya que, frente a los primeros, consistiría en reprochar a la gente el haberse rebelado, de un modo consiente, contra los mandatos o normas del Derecho, y en relación con los segundos, el haber infringido, por descuido de la vida social". [53]

La culpabilidad "es un juicio de reproche no es más que la reacción social o jurídica determinada por el delito cometido con todos sus elementos constitutivos."[54]

"Esta teoría fue ganando adeptos en los penalistas del sistema Causalista, por lo que la teoría normativista de la culpabilidad es la dominante, no se le concibe siempre de la misma manera, uno de los mayor en adelantos de los normativistas, radica en la posibilidad de incluir en la culpabilidad el concepto de exigibilidad de otra conducta, derivado de la exigencia normativa de conducirse de tal manera de no lesionar bienes jurídicos tutelados por la norma penal; y consecuentemente a este principio acepta los casos de no exigibilidad de otra conducta, como aspecto negativo del elemento de culpabilidad, es decir, como causa de inculpabilidad".[55]

---

[53] REYNOSO, Dávila, Roberto, TEORIA GENERAL DEL DELITO, 3 Ed, Porrúa, México 1998, p 198.
[54] Op, cit, pp12-16.
[55] ORELLANA, op cit. P.43.

En consecuencia, en la teoría normativita, el dolo y la culpa vienen a constituir un elemento de la misma, enfrenta el concepto de la culpabilidad es un juicio de reproche no es más que la reacción social o jurídica determinada por el delito cometido con todos sus elementos constitutivos.

.2.10 TEORIA SOCIOLOGISTA.

Proviene de la escuela positivista, considera al delito como un fenómeno natural y social producido por el hombre.

"El concepto social de acción esta en un plano pretipíco, referido más bien a un juicio ético; además, para los sociologistas basta que algo se haya querido, mientras la cuestión referente a que se ha querido, no será contestada por el concepto social de acción."[56]

Finalmente, en conclusión esta teoría se apega mucho a la escuela positivista se observa que para César Lombroso, el delito lo observa desde el punto de vista biológico o físico donde el hombre delincuente es un ser salvaje, a diferencia de Enrique Ferri, el delito desde el punto de vista natural, genético y hereditario, todo ello proviene de un aspecto social; el juez tiene la facultad para determinar la naturaleza delictuosa del acto y por ultimo la pena como medida de defensa, tiene por objeto la reforma de los infractores readaptables a la vida social.

2.11 EL DELITO, DEFINICION LEGAL Y DOCTRINAL.

La palabra delito deriva del verbo latino *delinquer*, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la Ley.

"El delito es una conducta del hombre, que consiste en la realización de un acto u omisión, descrito y sancionado por las leyes penales".[57]

---

[56] Op. cit, pp 21-27.
[57] MANUAL DEL JUSTICIABLE, de la Suprema Corte de Justicia de la Nación, Poder Judicial de la Federación, México, Mayo 2004.

DEFINICIÓN LEGAL DEL DELITO: de acuerdo con el artículo 7° del Código Penal Federal, "el Delito es el acto u omisión que sancionan las leyes penales".[58]

La palabra "delito", deriva del supino *delictum* del verbo *delinquere*, a su vez compuesto de *linquere*, dejar y el prefijo de, en la connotación peyorativa, se toma como *linquere viam o rectam viam*: dejar o abandonar el buen camino".[59]

Para MEZGER delito es la acción típicamente antijurídica y culpable. Este es un concepto dogmático del delito y forma parte de las concepciones materiales del delito. [60]

González Quintanilla, señala que el Delito "es un comportamiento típico, antijurídico y culpable".[61]

Asimismo, Ignacio Villalobos, define el Delito así "es un acto humano típicamente antijurídico y culpable".[62]

Por otra parte, Rafael de Pina Vara, considera que el Delito "es un acto u omisión constitutivo de una infracción de la ley penal".[63]

Francisco Carrara, Principal Exponente de la Escuela Clásica, sostiene que para el delito no es un ente de hecho, sino un ente jurídico y define al delito como "la infracción de la Ley del Estado, promulgada para proteger la seguridad de los ciudadanos resultante de un acto externo del hombre, positivo o negativo moralmente imputable y políticamente dañosos"[64]

Rafael Garòfalo, sabio jurista del positivismo que pretendió demostrar que el delito es un fenómeno o hecho natural, resultado necesario de factores hereditarios, de causas físicas y de fenómenos sociológicos por lo que define el delito natural como "la violación de los sentimientos altruistas de probidad y de piedad, en la medida media indispensable para la adaptación del individuo a la colectividad".[65]

---

[58] CODIGO PENAL FEDERAL
[59] REYNOSO, Dávila Roberto, TEORÍA GENERAL DEL DELITO, Ed. Porrúa, México 1998.
[60] MEZGER, TRATADO DEL DERECHO PENAL, Madrid, 1995. p.156.
[61] GONZÁLEZ Quintanilla, José Arturo, DERECHO PENAL MEXICANO. (PARTE GENERAL) Editorial Porrúa .S.A. México1993, pp.503
[62] VILLALOBOS, Ignacio, DERECHO PENAL MEXICANO. Editorial Porrúa. S.A. México 1975. pp. 198-200.
[63] DE PINA, Vara Rafael, DICCIONARIO DE DERECHO, Ed. Porrúa, México, 1998, p.219.
[64] CARRARA, Francisco, PROGRAMA DEL CURSO DE DERECHO CRIMINAL, parte general, volumen I, Editorial Temis, Bogotá, Colombia, P.30.
[65] CASTELLANOS, Op cit. 124.

Para Edmundo Mezger, "el delito es una acción punible; esto es, el conjunto de los presupuestos de la pena, por lo que considera que el delito es una acción típicamente antijurídica y culpable".[66]

Cuello Calón lo define "como la acción humana antijurídica, típica, culpable y punible."[67]

Por su parte Jiménez de Asúa, define al delito así: "es el acto típicamente culpable sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal". [68]

Últimamente, como se puede observar de las definiciones anteriormente citadas, se hace abstracción de la imputabilidad, ya que ésta implica la capacidad de ser sujeto activo del delito, o sea, no es un comportamiento propio del delito. La imputabilidad no es mencionada, por tratarse de una referencia al delincuente, no al delito. La imputabilidad como concepto penal se reduce a la capacidad de ser activo del delito, con dos referencias:

a) un dato de orden objetivo, constituido por la mayoría de edad dentro del derecho penal, que puede o no coincidir con la mayoría de edad civil o política y;

b) un dato de orden subjetivo, el que expresado en sentido llano se reduce a la normalidad mental, normalidad que comprende la capacidad de querer y comprender "el significado de la acción" y con lo que concluimos que el delito debe ser el conjunto de todos los presupuestos de la punibilidad.

[66] MEZGER, Op cit., p.156.
[67] EUGENIO, Cuello Calón op cit., p1.8.
[68] JIMÉNES DE ASUA, op cit. p 256.

2.12 ELEMENTOS DEL DELITO

El Delito tiene diversos elementos que conforman un todo. Para Maurach el delito es una acción típicamente antijurídica, atribuible; para Berling es la acción típica, antijurídica, culpable, sometida a una adecuada sanción penal y que llena las condiciones objetivas de penalidad.

La doctrina tradicionalmente considera los siguientes elementos del delito:

La tipicidad.- El acto u omisión coincide con la descripción de la figura delictiva contenida en la ley.

La antijuricidad.- Que implica que dicha conducta contraviene lo que dispone la norma jurídica, lo que puede darse cuando no exista una excluyente de responsabilidad o no haya una causa de licitud.

La imputabilidad.- Este elemento permite atribuir el delito a una persona, por tener la capacidad para comprender lo ilícito de su conducta.

La culpabilidad.- Mediante la cual es posible reprochar a un sujeto la ejecución de un hecho ilícito.

La punibilidad.- Particularidad que surge por tener previsto un castigo en la ley".[69]

[69] Manual del Justiciable en Materia Penal, Poder Judicial Federal,2004

Eduardo Mezger afirma que el delito "es una acción típicamente antijurídica y culpable".[70]

Para Jiménez de Asúa "es un acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad imputable a un hombre y sometido a una sanción penal."[71]

La teoría Héptatomica del delito, mejor conocida como la teoría de los siete elementos que son:

1.	**Conducta**
2.	**Tipicidad**
3.	**Antijuricidad**
4.	**Imputabilidad**
5.	**Culpabilidad**
6.	**Condiciones objetivas de Punibilidad**
7.	**Punibilidad.**

[70] CASTELLANOS, Op cit. 128.
[71] JIMÉNES DE ASÚA, op cit. p 256

De las definiciones anteriormente citadas así como las que se señalaron en párrafos anteriores, nos muestran como elementos del delito, según su concepción positiva y negativa, son los siguientes:

ASPECTOS POSITIVOS	ASPECTOS NEGATIVOS
a) Conducta o Hecho	Ausencia de conducta o hecho
b) Tipicidad	Ausencia del tipo
c) Antijuricidad	Causas de justificación
d) Imputabilidad	Causas de inimputabilidad
e) Culpabilidad	Causas de inculpabilidad
f) Condiciones objetivas	Falta de condiciones objetivas
g) punibilidad	Excusas absolutorias.[72]

[72] CASTELLANOS, Fernando, LINEAMIENTOS ELEMENTALES DEL DERECHO PENAL, México 2003 Editorial. Porrúa pp. 134

De acuerdo a nuestro Derecho Positivo Mexicano, el Código Penal Federal, en su artículo séptimo define al delito como el "acto u omisión que sancionan las leyes penales", así la conducta o hecho se obtiene de este artículo y del núcleo respectivo de cada tipo o descripción legal. La tipicidad se presentará cuando exista una adecuación de dicha conducta a alguno de los tipos descritos en el Código Penal; la antijuricidad se presentará cuando el sujeto no esté protegido por una causa de licitud descrita en el artículo 15 del Código Penal Federal. La imputabilidad se presenta cuando concurre la capacidad de obrar en el Derecho Penal, es decir, que no se presente la causa de inimputabilidad descrita en la fracción VII del artículo 15 de la Ley Penal Federal. Habrá culpabilidad de acuerdo a los artículos 8 y 9 de nuestra ley penal Federal. La punibilidad existe cuando no se presentan las excusas absolutorias descritas por nuestro Derecho Positivo Federal. Las condiciones objetivas de punibilidad se presentan cuando al definir la infracción punible se establecen requisitos constantes, pero aparecen variables de acuerdo a cada tipo penal; pueden o no presentarse.

Como se puede observar, el delito tiene un gran contenido en cuanto a los elementos que lo componen y en relación a éstos, existen diversas corrientes de la doctrina, los cuales tratan de explicar algunos de ellos, como la teoría causalista y finalista de la acción, la teoría psicologista y normativista, el modelo lógico y la teoría sociologista.

En conclusión en la elaboración de este apartado se observo que los elementos fundamentales del delito son la tipicidad, la antijuricidad y la culpabilidad, ya que el delito es un acto típico, todo acto humano para considerarse como delito debe adecuarse al tipo penal.

Es decir debe haber tipicidad. Si no hay adecuación no hay delito, o peor aun, si no hay tipo, la conducta no es delito. Por eso, todo lo que no esta prohibido u ordenado, está permitido; es un acto típicamente antijurídico, está en oposición a la norma jurídica, debe lesionar o poner en peligro un bien jurídicamente protegido. Un acto típicamente antijurídico puede dejar de ser tal si median las Causas de Justificación.

El acto típicamente antijurídico deber ser culpable; para que la culpabilidad pueda ligarse a una persona, debe existir los siguientes elementos de culpabilidad: imputabilidad, dolo o culpa y exigibilidad de un comportamiento distinto, pero la conducta deja de ser culpable si median las Causas de Inculpabilidad como: el caso fortuito, cumplimiento de un deber o un estado de necesidad (por ejemplo la legítima defensa).

El estado de necesidad tiene doble ubicación sistemática: es causa de justificación como también causa de inculpabilidad de la conducta.

Tiene esta doble ubicación porque subsana la inconveniencia de mantener a priori una clasificación de las Causas de Justificación y las Causas de Inculpabilidad. La determinación de su naturaleza queda librada a la jurisprudencia o a la doctrina.

Si al acto típicamente antijurídico le falta algún elemento de la culpabilidad o se dio alguna causa de inculpabilidad el delito deja de ser tal, no hay delito.

El último elemento constitutivo del delito es la punibilidad que es la privación de un bien jurídico a quien haya cometido, o intente cometer, un delito.

Un acto típicamente antijurídico y culpable debe ser sancionado con una pena de carácter criminal. Algunas veces a quien haya cometido un acto típicamente antijurídico y culpable no se le puede aplicar la sanción por las llamadas Causas de Impunidad.

2.13 LA CONDUCTA

La 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 una actividad o inactividad respectivamente. Es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito porque tiene una finalidad al realizarse la acción u omisión.

"La conducta puede ser de acción o de omisión y esta última se subdivide en omisión simple y comisión por omisión."[73]

La acción en sentido amplio consiste en la conducta exterior voluntaria, encaminada a la producción de un resultado, consistente en la modificación del mundo exterior o en peligro de que este llegue producirse.

"La conducta es el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito".[74]

Para Jiménez de Asúa "el acto es la manifestación de voluntad que, mediante acción, produce un cambio en el mundo exterior cuya modificación se aguarda."[75]

La conducta tiene tres elementos:

1) "un acto positivo o negativo (acción u omisión), una manifestación de la voluntad.

2) un resultado.

3) una relación de causalidad entre el acto y el resultado".[76]

El acto, es el comportamiento humano positivo o negativo que produce un resultado. Positivo será 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.

La conducta es un comportamiento humano voluntario, positivo o negativo encaminado a un propósito

Delito de Acción.- La acción se define como aquella actividad que realiza el sujeto, produciendo consecuencias en el mundo jurídico, en dicha acción debe de

---

[73] Op, cit. Pp. 83.
[74] CASTELLANOS, Op cit. 149.
[75] JIMÉNES DE ASÚA, Luis, PRINCIPIOS DEL DERECHO PENAL, LA LEY Y EL DELITO, Editorial sudamericana, Buenos Aires, 1990, p.210
[76] CASTELLANOS, Op cit. 156

darse un movimiento por parte del sujeto, de esta manera, la conducta de acción tiene tres elementos:

a) movimiento;

b) resultado;

c) relación de causalidad.

La acción es conducta omisiva o activa voluntaria, que consiste en un movimiento de su organismo destinado a producir cierto cambio, o la posibilidad, en el exterior del mundo (Teoría de la causalidad).

Es todo comportamiento humano que depende de la voluntad. El delito es acto humano, cualquier mal que no tiene origen en la actividad humana no puede reputarse como delito.

La posibilidad de cambio en la realidad se da en los delitos frustrados como también en la tentativa. "Si es involuntario (caso fortuito) u ocurre en el fuero interno y no llega a manifestarse, la acción se excluye del campo delictivo". [77]

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, es decir, 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.

Según nuestro Derecho Positivo Mexicano, en el Código Penal Federal en su artículo séptimo, el delito es "el acto u omisión que sancionan las leyes penales", de donde se desprende el elemento conducta pudiéndose presentar como una acción u omisión.

[77] López, Bentancur, Op. Cit. 87-89

La omisión, para Cuello Calón, es "la inactividad voluntaria cuando existe el deber jurídico de obrar".[78]

La omisión es el voluntario no hacer algo que el ordenamiento jurídico esperaba que el sujeto hiciese.

La acción negativa viola la norma imperativa.

Sus elementos son:

- Inactividad o abstención voluntaria. (Se da en los delitos de simple actividad),
- El resultado antijurídico. Es decir la producción de resultado que el omitente tiene él deber de impedir; y
- La relación de causalidad. Es el resultado antijurídico debe ser consecuencia del comportamiento omisivo.

La omisión, según Cuello Calón, "es la inactividad voluntaria cuando existe el deber jurídico de obrar."[79]

La omisión tiene cuatro elementos:

a) Manifestación de la voluntad.

b) Una conducta pasiva. (inactividad).

c) Deber jurídico de obrar.

d) Resultado típico jurídico.

[78] EUGENIO, Cuello Calón. DERECHO PENAL I, 8ª Edición, p.8.

[79] Op, cit. P288.

Estos 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. La primera no produce un resultado material, la segunda sí.

En los **delitos de simple omisión**, se viola 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.

Los delitos de omisión simple producen un resultado típico, y los de comisión por omisión un resultado típico y uno material.

"Delitos de Comisión por Omisión: Son aquellos donde el sujeto viola un mandato de acción, junto con una prohibición de comisión, en otras palabras, el sujeto no hace lo que debe hacer, ocasionando con ello un resultado que no debe ser ocasionado".[80]

En conclusión, la conducta 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 una actividad o inactividad respectivamente. Es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito porque tiene una finalidad al realizarse la acción u omisión o bien 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, que se dividen en delitos de acción que es la 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; los delitos de omisión es el voluntario no hacer algo que el ordenamiento jurídico esperaba que

---

[80] REYNOSO, Davila Roberto, TEORÍA GENERAL DEL DELITO, Ed. Porrúa, México 1998, P. 23.

el sujeto hiciese; en 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 voluntad del agente", esto es la afirmación de que no puede constituir una conducta delictiva cuando no se presenta la voluntad del agente; mientras en los de comisión por omisión se viola una norma preceptiva penal o de otra rama del derecho y una norma prohibitiva penal.

2.14 LA AUSENCIA DE CONDUCTA.

La ausencia de conducta es el elemento negativo de la conducta, abarca la ausencia de acción o de omisión de la misma, en la realización de un ilícito.

Existe ausencia de conducta si falta alguno de los elementos esenciales del delito, este no se integrara, en consecuencia, si la conducta esta ausente, evidentemente no abra delito a pesar de las apariencias, es uno de los aspectos negativos, o mejor dicho, impeditivos de la formación de la figura delictiva, por ser la actuación humana positiva o negativa, la mas indispensable del delito como de todo problema jurídico y se puede presentar de la siguientes formas:

- "Fuerza física superior exterior irresistible.-se requiere que se ejerza violencia en la persona del acusado y que este involuntariamente solo sirva de instrumento en la producción del daño.

- Fuerza mayor.- es el acontecimiento ajeno a la conducta del actor y producido al margen de la misma con fuerza incontrastable, liberándolo de su responsabilidad". [81]

[81] CASTELLANOS, Op cit. 124.

"Las causas que excluyen la acción o conducta, cuando es violentado por una fuerza exterior que no puede resistir VIS-absoluta, fuerza física que depende del hombre, supera la voluntad del sujeto de tal modo que es incapaz de autodeterminarse y VIS mayor esta es la fuerza mayor depende de la naturaleza".[82]

2.15 TIPICIDAD

La tipicidad es el encuadramiento de una conducta con la descripción hecha en la ley.

Celestino Porte Petit define a "la tipicidad como la adecuación de la conducta al tipo, que se resume en la fórmula *nullum crimen sine tipo."*[83]

La tipicidad es la adecuación, o encaje del acto humano voluntario ejecutado por el sujeto a la figura descrita por la ley como delito.

Si la adecuación no es completa no hay delito. La tipicidad es la adecuación, el encaje, la subsunción del acto humano voluntario al tipo penal.

La tipicidad es la adecuación de la conducta al tipo penal. En este sentido diversos autores han dado su definición de tipicidad; dentro de las más importantes tenemos la expresada por Francisco Blasco y Fernández de Moreda, la cual dice: "la acción típica es sólo aquella que se acomoda a la descripción objetiva, aunque saturada a veces de referencia a elementos normativos y subjetivos del injusto de una conducta que generalmente se reputa delictuosa, por violar, en la generalidad de los casos, un precepto, una norma, penalmente protegida"[84]

Se debe tener cuidado de no confundir la tipicidad con tipo, la primera se refiere a la conducta, y el segundo pertenece a la ley, a la descripción o hipótesis plasmada

---

[82] REYNOSO, op cit., P.55.
[83] PORTE, Petit Candaudao, Celestino, APUNTES DE LA PARTE GENERAL DEL DERECHO PENAL., Editorial Porrúa, 1983, p 419-420.
[84] CASTELLANOS, Fernando, LINEAMIENTOS ELEMENTALES DEL DERECHO PENAL, México 2002, Editorial Porrúa pp 117

por el legislador sobre un hecho ilícito, es la fórmula legal a la que se debe adecuar la conducta para la existencia de un delito.

"Tipo es el instrumento legal, lógicamente necesario, predominantemente descriptivo que tiene por función la individualización de conductas humanas penalmente relevantes de tipo objetivo y subjetivo sancionado por las leyes penales".[85]

Javier Alba Muñoz define el tipo como "la descripción legal de la conducta y del resultado y, por ende, acción y resultado quedan comprendidos en él."[86]

La tipicidad se encuentra fundamentada en el artículo 14 Constitucional, párrafo tercero, que a la letra dice: "En los juicios de orden criminal, queda prohibido imponer, por simple analogía y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata".[87]

Por lo que podemos concluir, que tipicidad es la adecuación de la conducta con la descripción hecha en la ley, razón por la que no hay delito sin ley, si no se encuentra la conducta descrita como es el caso de los delitos informáticos, no existe este tipo de delitos, motivo por el cual no pueden ser sancionados, por no encontrarse descritos en una ley como delito, por tal motivo no existe tal delito.

2.16 AUSENCIA DE TIPICIDAD

El aspecto negativo de la tipicidad es la atipicidad. La atipicidad es la falta de adecuación de la conducta al tipo penal, si la conducta no es típica, jamás podrá ser delictuosa.

"Es la ausencia de la adecuación de la conducta al tipo, si la conducta no es típica, jamás podrá ser delictuosa, suele distinguirse entre ausencia del tipo esta se presenta cuando el legislador deliberada o inadvertidamente, no describe una

---

[85] CASTELLANOS, Op cit. 168.
[86] Op, cit, p168.
[87] Constitución Política de los Estados Unidos Mexicanos, p.13

conducta que, según el sentir genera, debería ser incluida en el catalogo de loas delito y la ausencia de atipicidad surge cuando existe el tipo pero no se amolda a el la conducta dada".[88]

Es importante diferenciar la atipicidad de la falta de tipo, siendo que en el segundo caso, no existe descripción de la conducta o hecho, en la norma penal.

Las causas de atipicidad par a Luis Jiménez de Asúa son:

1. "ausencia de la calidad o número exigido por la ley en cuanto a los sujetos activos y pasivos.

2. si falta el objeto material o jurídico.

3. cuando no se dan las referencias temporales o especiales requeridas en el tipo.

4. al no realizarse al hecho por los medios comisitos especialmente señalados en la ley.

5. si faltan los elementos subjetivos del injusto legalmente exigidos.

6. por no darse, en su caso, la antijuricidad especial."[89]

Como consecuencia de la atipicidad, podemos citar en tres hipótesis los efectos de la misma:

1. no integración del tipo.

2. traslación de un tipo a otro.

3. existencia de un delito imposible.

---

[88] CASTELLANOS. Op cit. 175.
[89] JIMÉNES DE ASÚA, Luis. PRINCIPIOS DEL DERECHO PENAL. LA LEY Y EL DELITO. Editorial sudamericana. Buenos Aires, 1990. p.940.

Finalmente, como conclusión en toda atipicidad existe la falta de tipo; en el caso de un hecho específico no encuadra exactamente en el descrito por la ley, respecto de el no existe tipo, como se estipula en el Código Penal Federal, en su artículo 15, fracción II, como una causa de excusión del delito cuando se demuestre la inexistencia de alguno de los elementos que integran la descripción típica del delito de que se trate.

2.17 LA ANTIJURICIDAD

La antijuricidad la podemos considerar como un elemento positivo del delito, es decir, cuando una conducta es antijurídica, es considerada como delito. Para que la conducta de un ser humano sea delictiva, debe contravenir las normas penales, es decir, ha de ser antijurídica; o bien es lo contrario a Derecho, por lo tanto, no basta que la conducta encuadre en el tipo penal, se necesita que esta conducta sea antijurídica, considerando como tal, a toda aquella definida por la ley, no protegida por causas de justificación, establecidas de manera expresa en la misma.

Raúl Carrancá y Trujillo, utiliza la denominación "causas que excluyen la incriminación."[90]

La antijuridicidad es la oposición del acto voluntario típico al ordenamiento jurídico.

El acto o conducta humana que se opone al ordenamiento jurídico no debe justificarse. La condición de la antijuridicidad es el tipo penal. El tipo penal es el elemento descriptivo del delito, la antijuridicidad es el elemento valorativo.

Cuello Calón, sostiene que "la antijuricidad presupone un juicio, una estimación de la oposición existente entre el hecho realizado y una norma jurídico-penal".[91]

---

[90] RAÚL, Carrancá y Trujillo, TRATADO DE DERECHO PENAL, TITULO I, P. 16.
[91] Cuello Calón. Op cit. P. 284..

En conclusión se puede decir que la antijuricidad es toda conducta que va en contra del orden jurídico, toda conducta típica que se realiza a sabiendas de que va a causar un daño en el mundo y que se encuentra sancionada por la norma.

2.18 CAUSAS DE JUSTIFICACIÓN

La ausencia de la antijuricidad son las causa de justificación, es cuando es un hecho presumiblemente delictuoso falta la antijuricidad, podemos decir: no hay delito, por la existencia de una causa de justificación, es decir, el individuo ha actuado en determinada forma sin el ánimo de transgredir las normas penales, Así, si un hombre ha matado a otro, en defensa de su vida injustamente atacada, estará en una causa de justificación, excluyéndose la antijuricidad en la conducta del homicida. Las causas de justificación son aquellas condiciones que tienen el poder de excluir la antijuricidad de una conducta típica, representa un aspecto negativo del delito; en presencia de alguna de ellas falta uno de los elementos esenciales del delito.

Son también llamadas causas de exclusión del delito, "son situaciones previstas en la ley penal que impiden que una conducta o hecho pueda ser considerado como delito, debido a que la conducta tipificada no es sancionable cuando se cumplen ciertas condiciones que la propia ley señala".[92]

Algunas causas de justificación conforme al artículo 15 del Código Penal Federal son:

1. **"Legitima defensa**; es la repulsa de una agresión antijurídica y actual o inminente por el atacado o por terceras personas contra el agresor sin traspasar la medida necesaria para la protección de la persona o de los bienes o intereses jurídicos en inminente peligro de daño y dentro de la racional proporción de los medios empleados para impedirla o repelerla siempre que el agredido o quien ejerza la defensa no haya provocado la agresión ni exista

[92] El Manual del Justiciable en Materia Penal, Poder Judicial de la Federación,2004

otro medio mas practico e irracional para evitarla, Artículo 15, fracción IV del Código Penal Federal".[93]

"Para la Escuela Clásica, la defensa legítima descansa en la necesidad; ante la imposibilidad de que en un momento dado el Estado acuda en auxilio del injustamente atacado, para evitar la consumación de la agresión, es lícito y justo que él se defienda; así, la defensa privada es sustitutiva de la pública; y para los positivistas, si el agresor muestra su temibilidad al atacar injustamente, resultará lícito cuanto se haga para rechazarlo, por tratarse de un acto de justicia social; el sujeto que se defiende no es peligroso.[94]

Para Hegel, "si la agresión injusta es la negación del Derecho, la defensa legítima es la negación de esa negación y, por lo tanto, la afirmación del Derecho, siendo su fin la anulación de la injusticia".[95]

De acuerdo con Jiménez de Asúa, viene a fundamentar la defensa legítima "la preponderancia de intereses pues debe considerarse de mayor importancia el interés del agredido que el del injusto agresor".[96]

Carrancá y Trujillo, conciliando diversas opiniones, afirma que "la defensa privada se legitima suficientemente, tanto por la necesidad, como por la ausencia de temibilidad en el sujeto, revelada por sus motivos y fin, así como por la imposibilidad en que el Estado se encuentra de acudir en defensa del interés agredido injustamente".[97]

En conclusión, la legítima defensa es cuando se repele una agresión real, actual e inminente en protección de bienes jurídicos propios o ajenos, esto es, que por repeler entendemos rechazar, evitar, impedir, no querer algo, por lo que es la necesidad de evitar una conducta que cause un daño, para proteger un bien jurídico tutelado como puede ser la vida, el patrimonio, la integridad corporal, libertad físico o sexual entre otros.

---

[93] REYNOSO, Dávila, Roberto, TEORIA GENERAL DEL DELITO, 3 Ed, Porrúa, México 1998, p 123.
[94] CASTELLANOS, Op. cit.p.192.
[95] Op cit.192.
[96] Op cit, 192
[97] Op cit, 192

2. **Estado de necesidad**; es el peligro actual o inmediato para bienes jurídicamente protegidos, que solo puede evitarse mediante la lesión de otro bien jurídico tutelado; Situación de peligro actual de los intereses jurídicos protegidos por el Derecho, en el que no queda otro remedio que la violación de los intereses de otra persona. Artículo 15, fracción V del Código Penal Federal.

"El estado de necesidad es una situación de peligro de daño actual e inminente, real y grave de la persona o de los bienes o interese jurídicos, que sólo puede ser evitada por quien se encuentra en peligro o por un tercero, mediante un daño en la persona o bienes de otro, de menor e entidad del que trata de evitarse, siempre que no exista otro medio más práctico y menos perjudicial y no haya ocasionado dolosamente el estado de necesidad, ni quien por su tenga el deber de afrontar el peligro".[98]

Para Von Liszt, 2el estado de necesidad es un estado de peligro presente, que amenaza los intereses protegidos en la ley y en el cual no queda otro recurso si no el de violar los intereses ajenos jurídicamente protegidos".[99]

Por lo que podemos concluir que el estado de necesidad es cuando se encuentra en peligro un bien jurídico tutelado el cual solo puede ser evitada por quien se encuentra en peligro o por un tercero, mediante un daño en la persona o bienes de otro, de menor e entidad del que trata de evitarse, siempre que no exista otro medio más práctico y menos perjudicial y no haya ocasionado dolosamente el estado de necesidad.

[98] REYNOSO,Op cit, p 145.
[99] BETANCOURT López, Eduardo. TEORIA DEL DELITO. Editorial Porrúa. S.A.México1994.pp.162.

3. **Cumplimiento de un deber;** la acción u omisión se realice en cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional del medio empleado para cumplir el deber o ejercicio el derecho y que este ultimo no se realice con el solo propósito de perjudicar al otro. Artículo 15, fracción VI del Código Penal Federal.

"En el cumplimiento de un deber opera una causa de justificación cuando la conducta típica se realiza en cumplimiento de un deber jurídico o ejercicio de un derecho siempre que exista necesidad racional del medio empleado para cumplir el deber para ejercer ele derecho y que no se realice con el solo propósito de perjudicar a otro".[100]

4. **Ejercicio de un derecho**; Está exento de responsabilidad el que en ejercicio legítimo de un derecho, oficio o cargo, cumplimiento de un deber o la ley, vulnere un bien jurídico.

"Es la acción u omisión que se realice un cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional del medio empleado para cumplir el deber o ejercer el derecho y que no se realice con el solo propósito de perjudicar a otro".[101]

Finalmente, entendemos como cumplimiento de un deber o ejercicio de un derecho a la persona que es facultada o bien se le dota de un derecho para realizar actos concretos con la finalidad de salvaguardar el orden jurídico.

Por otra parte, el código penal federal considera en su capitulo IV, como Causas de exclusión del delito

[100] Op. cit. p. 155.
[101] Bentarcur, Op cit. P172-173.

"ARTICULO 15.- El delito se excluye cuando:

I.- El hecho se realice sin intervención de la voluntad del agente;

II.- Se demuestre la inexistencia de alguno de los elementos que integran la descripción típica del delito de que se trate;

III.- Se actúe con el consentimiento del titular del bien jurídico afectado, siempre que se llenen los siguientes requisitos:

a) Que el bien jurídico sea disponible;

b) Que el titular del bien tenga la capacidad jurídica para disponer libremente del mismo; y

c) Que el consentimiento sea expreso o tácito y sin que medie algún vicio; o bien, que el hecho se realice en circunstancias tales que permitan fundadamente presumir que, de haberse consultado al titular, éste hubiese otorgado el mismo;

IV.- Se repela una agresión real, actual o inminente, y sin derecho, en protección de bienes jurídicos propios o ajenos, siempre que exista necesidad de la defensa y racionalidad de los medios empleados y no medie provocación dolosa suficiente e inmediata por parte del agredido o de la persona a quien se defiende.

Se presumirá como defensa legítima, salvo prueba en contrario, el hecho de causar daño a quien por cualquier medio trate de penetrar, sin derecho, al hogar del agente, al de su familia, a sus dependencias, o a los de cualquier persona que tenga la obligación de defender, al sitio donde se encuentren bienes propios o ajenos

respecto de los que exista la misma obligación; o bien, lo encuentre en alguno de aquellos lugares en circunstancias tales que revelen la probabilidad de una agresión;

V.- Se obre por la necesidad de salvaguardar un bien jurídico propio o ajeno, de un peligro real, actual o inminente, no ocasionado dolosamente por el agente, lesionando otro bien de menor o igual valor que el salvaguardado, siempre que el peligro no sea evitable por otros medios y el agente no tuviere el deber jurídico de afrontarlo;

VI.- La acción o la omisión se realicen en cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional del medio empleado para cumplir el deber o ejercer el derecho, y que este último no se realice con el solo propósito de perjudicar a otro;

VII.- Al momento de realizar el hecho típico, el agente no tenga la capacidad de comprender el carácter ilícito de aquél o de conducirse de acuerdo con esa comprensión, en virtud de padecer trastorno mental o desarrollo intelectual retardado, a no ser que el agente hubiere provocado su trastorno mental dolosa o culposamente, en cuyo caso responderá por el resultado típico siempre y cuando lo haya previsto o le fuere previsible.

Cuando la capacidad a que se refiere el párrafo anterior sólo se encuentre considerablemente disminuida, se estará a lo dispuesto en el artículo 69 bis de este Código;

VIII.- Se realice la acción o la omisión bajo un error invencible:

A) Sobre alguno de los elementos esenciales que integran el tipo penal; o

B) Respecto de la ilicitud de la conducta, ya sea porque el sujeto desconozca la existencia de la ley o el alcance de la misma, o porque crea que está justificada su conducta.

Si los errores a que se refieren los incisos anteriores son vencibles, se estará a lo dispuesto por el artículo 66 de este Código;

IX.- Atentas las circunstancias que concurren en la realización de una conducta ilícita, no sea racionalmente exigible al agente una conducta diversa a la que realizó, en virtud de no haberse podido determinar a actuar conforme a derecho; o

X.- El resultado típico se produce por caso fortuito".

"ARTÍCULO 16.- Al que se exceda en los casos de defensa legítima, estado de necesidad, cumplimiento de un deber o ejercicio de un derecho a que se refieren las fracciones IV, V, VI del artículo 15, se le impondrá la pena del delito culposo".

"ARTÍCULO 17.- Las causas de exclusión del delito se investigarán y resolverán de oficio o a petición de parte, en cualquier estado del procedimiento".[102]

La antijuridicidad puede presentarse de manera formal con la infracción a una norma, un mandato o una prohibición del orden jurídico.

Asimismo, de forma material, lo socialmente dañoso concibe al delito como natural, cuyas consideraciones sería el libre albedrío de intérprete.

[102] Código Penal Federal, Editorial Delma, México 2004, p. 6-8.

2.19 LA IMPUTABILIDAD

La imputabilidad es la capacidad de querer y entender, en el campo del Derecho Penal. Querer es estar en condiciones de aceptar o realizar algo voluntariamente y entender es tener la capacidad mental y la edad biológica para desplegar esa decisión.

El aspecto negativo de la imputabilidad es la inimputabilidad, consistente en la incapacidad de querer y entender en el mundo del Derecho. Son aquellas causas en las que si bien el hecho es típico y antijurídico, no se encuentra el agente en condiciones de que se le pueda atribuir el acto que perpetró.

Luis Jiménez Asúa expone que "la imputabilidad criminal no es cosa distinta de la imputabilidad moral, sino esta misma aplicada en concreto al autor de un delito y puede definirse como el conjunto de condiciones necesarias para que el hecho punible pueda y deba ser atribuido a quien voluntariamente lo ejecutó, como a su causa eficiente y libre."[103]

La imputabilidad es la capacidad psíquica de una persona de comprender la antijuridicidad de su conducta y de no adecuar la misma a esa comprensión.

El aspecto negativo de la imputabilidad es la inimputabilidad; consistente en la incapacidad de querer y entender en el mundo del derecho.

Jiménez Asúa sostiene que "son causas de inimputabilidad la falta de desarrollo y salud de la mente, así como los trastornos pasajeros de las facultades mentales que privan o perturban en el sujeto la falta de conocer el deber."[104]

Finalmente la imputabilidad podemos definirla como la capacidad, condicionada por la madurez y salud mental, de comprender el carácter antijurídico de la propia acción u omisión y de determinar de acuerdo a esa compresión o bien es la capacidad de querer o entender en el mundo del derecho.

---

[103] Op. cit. p 326.
[104] Op. cit. p 339.

Por lo tanto, ésta implica la capacidad de ser sujeto activo del delito, o sea, no es un comportamiento propio del delito. La imputabilidad no es mencionada, por tratarse de una referencia al delincuente, no al delito.

2.20 LA INIMPUTABILIDAD

Como la imputabilidad es soporte básico y esencialismo de la culpabilidad, si aquella no existe esta y sin culpabilidad no puede configurarse el delito, luego la inimputabilidad es indispensable para la formación d la figura delictiva.

Jiménez de Asúa sostiene que son causas de inimputabilidad la falta de desarrollo y salud de la mente, así como los trastornos pasajeros de las facultades mentales que privan o perturban en el sujeto la facultad de conocer el deber. [105]

Pero algunas veces un sujeto deja de ser imputable por las llamadas **CAUSAS DE INIMPUTABILIDAD** que son:

- "Inmadurez mental: Es la falta de desarrollo mental como lo son los menores de edad.

- Trastorno mental transitorio: perturbación de de las facultades mentales pasajera de corta duración.

- Falta de salud mental: Es cuando no se encuentran bien de sus facultades mentales".[106]

La inimputabilidad es el estado de incapacidad para conocer el deber ordenado por la norma y la ineptitud de actuar, por cuenta propia, con arreglo a su mandato.

Las causas de inimputabilidad son aquellas situaciones que, si bien la conducta es típica y antijurídica, hacen que no sea posible atribuir el acto realizado al sujeto por no concurrir en él: salud mental, conciencia plena, suficiente inteligencia o madurez psíquica.

---

[105] Jiménez de Asúa. Op cit. P. 339.
[106] Bentarcour. op cit. P. 198.

Finalmente la inimputabilidad es la no capacidad de querer o entender en el mundo del derecho; esto es, aquellas causas en las que si bien el hecho es típico y antijurídico, no se encuentra el agente en condiciones de que se pueda atribuir el acto que perpetro, como pude ser los menores de edad, sonámbulos, o que se encuentren bajo los efectos del alcohol, de las drogas, entre otros trastornos.

2.21 LA CULPABILIDAD

El concepto de la culpabilidad, dependerá de la teoría que se adopte, pues no será igual el de un psicologista, el de un normativista o el de un finalista. Así, el primero diría, la culpabilidad consiste en el nexo psicológico que une al sujeto con la conducta o el resultado material, y el segundo, en el nexo psicológico entre el sujeto y la conducta o el resultado material, reprochable, y el tercero, afirmaría, que la culpabilidad es la reprochabilidad de la conducta, sin considerar el dolo como elemento de la culpabilidad, sino de la conducta. La culpabilidad en la tesis finalista se reduce a la reprochabilidad y a diferencia de la teoría normativa el dolo y la culpa no son elementos de la culpabilidad porque son contenido del tipo. "la culpabilidad es por lo tanto, responsabilidad, apartándose consecuentemente de los normativitas mantienen el dolo y la culpa en la culpabilidad, constituyendo como se afirma por un sector un mixtum compositum, de cosas no pueden mezclarse".[107]

El concepto de culpabilidad como tercer aspecto del delito y de acuerdo a la definición anterior, nos señala cuatro importantes elementos que la conforman y son: "una ley, una acción, un contraste entre esta acción y esta ley, y el conocimiento de esta situación, según lo manifestó Maggiore."[108]

Para Zaffaroni, "es la reprochabilidad de un injusto a un autor, la que solo es posible cuando revela que el autor a obrado con una disposición interna a la norma violada".[109]

La culpabilidad es un elemento básico del delito y es el nexo intelectual y emocional que una al sujeto con el acto delictivo.

---

[107] Bentarcour, Op cit. Pp.213.
[108] MAGGIORE, DERECHO PENAL I, Editorial Temis, Bogotá, 1954 p 451.
[109] Zaffaroni, Eugenio Raúl. TRATADO DE DERECHO PENAL, Ed. Cardenas, México 1998, p 12

La culpabilidad es la reprochabilidad de la conducta de una persona imputable y responsable, que pudiendo haberse conducido de una manera no lo hizo, por lo cual el juez le declara merecedor de una pena.

Para que haya culpabilidad tiene que presentarse los siguientes presupuestos o elementos de la culpabilidad:

- Imputabilidad,
- Dolo o culpa (estos elementos son también llamados: formas de culpabilidad) y,
- La exigibilidad de una conducta adecuada a la prohibición o imperatividad de la norma.

"Por faltarle alguno de estos presupuestos, o por existir las llamadas, Causas de Inculpabilidad el autor no actúa culpablemente, en consecuencia esta exento de responsabilidad criminal". [110]

Los elementos de la culpabilidad según Jiménez Asúa "son los motivos, las referencias de las acción a la total personalidad del autor."[111]

En conclusión podemos decir que la culpabilidad consiste en el nexo psicológico que une al sujeto con la conducta o el resultado material, y el segundo, en el nexo psicológico entre el sujeto y la conducta o el resultado material, reprochable, y el tercero, afirmaría, que la culpabilidad es la reprochabilidad de la conducta, sin considerar el dolo como elemento de la culpabilidad, sino de la conducta.

[110] Bentancour, op cit. 216-218.
[111] JIMÉNES DE ASÚA, Luis, PRINCIPIOS DEL DERECHO PENAL, LA LEY Y EL DELITO, Editorial sudamericana, Buenos Aires, 1990, p.210

2.22 FORMAS DE COMISIÓN DE LOS DELITOS.

Como se ha venido mencionando en los capítulos anteriores, el artículo 7° del Código Penal Federal, aduce: "Delito es el acto u omisión que sancionan las leyes penales. Los delitos pueden ser: I. Dolosos; II. Culposos. El delito es doloso cuando el agente quiere o acepta el resultado, o cuando éste es consecuencia necesaria de la conducta realizada. El delito es culposo cuando habiéndose previsto el resultado, se confió en que no se produciría; cuando se causó por impericia o ineptitud.

EL DOLO

Es la producción de un resultado típicamente antijurídico, con conciencia de que se quebranta el deber, con conocimiento de las circunstancias del hecho y el curso esencial de la relación de causalidad existente entre la manifestación humana y el cambio del mundo exterior, y con voluntad de realizar la acción y con representación del resultado que se quiere.

Los delitos se cometen en dos formas:

Dolosa.- En términos generales, cuando hay la voluntad de cometer el delito, es decir cuando se conocen sus elementos o se prevé como posible el resultado y se quiere o acepta la realización del hecho descrito por la ley.

Culposa.- En general, cuando no existe la intención de cometer el delito, es decir cuando se produce el delito que no se previó al ser previsible, o se previó con la confianza en que no se produciría, en virtud de la violación a un deber de cuidado, que debía y podía observarse según las circunstancias y condiciones personales.

No obstante lo anterior, en algunas entidades federativas los Códigos Penales contemplan también a la preterintencionalidad como otra forma de cometer delitos, la cual se manifiesta cuando se produce un resultado delictivo que va más allá del

querido o aceptado, es decir, "cuando por la forma y medio de ejecución se acredita plenamente que el resultado excedió el propósito original del sujeto que lo realiza".[112]

Para Jiménez Asúa "el dolo es la producción de un resultado típicamente antijurídico, con conciencia de que se quebranta el deber, con conocimiento de las circunstancias de hecho y del curso esencial de la realización de causalidad existente entre la manifestación humana y el cambio en el mundo exterior, con voluntad de realizar la acción y con representación del resultado que se quiere o ratifica".[113]

Cullo Calón afirma que "el dolo es la voluntad consciente dirigida a la ejecución de un hecho que es delictuoso".[114]

En conclusión podemos decir que el dolo consiste en el conocimiento de la realización de circunstancias que pertenecen al tipo, y voluntad y aceptación de realización del mismo o bien en el actuar, consciente y voluntario dirigido a la producción de un resultado típico y antijurídico.

ELEMENTOS DEL DOLO:

Elemento volitivo. Tiene que actuar la voluntad. El individuo tiene que querer hacer, es la voluntad de realizar el acto, es la volición del hecho típico.

Elemento Intelectual. "El sujeto debe saber lo que hace y esperar un resultado. Para que exista dolo tiene que haber estos dos elementos del dolo; esta constituido por la conciencia de que se quebranta el deber".[115]

LA CULPA

La culpa, es la segunda forma de culpabilidad, con base en el psicologuismo. Cuello Calón, expresa: "existe culpa cuando obrando sin intención y sin la diligencia debida se causa un resultado dañoso, previsible y penado por la ley".

---

[112] Manual del Justiciable en Materia Penal, Poder Judicial de la Federación, 2004.
[113] Jiménez de Asúa, Op cit. P417.
[114] Cuello Calon, Op cit. P.441.
[115] CASTELLANOS, Op cit. P. 238.

Carrara, por su parte, expuso que la culpa es una voluntaria omisión de diligencia, donde se calculan las consecuencias posibles y previsibles del mismo hecho".[116]

Para Carrara, "la culpa es una voluntaria misión de diligencia, donde se calculan las consecuencias posibles y previsibles del mismo hecho".[117]

Finalmente, en conclusión la culpa es cuando se obra sin intención y sin la diligencia debida, causando un resultado dañoso posible y penado por la ley.

A manera de ejemplo, el delito de homicidio es doloso cuando existe la comprensión y la voluntad de privar a otro de la vida; es preterintencional cuando existe la comprensión y la voluntad de querer sólo lesionar a otro y de este hecho surge la muerte no querida; y es homicidio culposos si falta no sólo la comprensión y la voluntad de producir la muerte, sino también la idea de lesionar a otro.

2.23 LA INCULPABILIDAD

"La de Inculpabilidad es el aspecto negativo de la culpabilidad, esta se va a dar cuando concurren determinadas causas o circunstancias extrañas a la capacidad de conocer y de querer, en la ejecución de un hecho realizado por algunas causas de Inculpabilidad son: el caso fortuito, cumplimiento de un deber o un estado de necesidad (por ejemplo la legítima defensa)".[118]

El autor no actúa culpablemente, en consecuencia, también, esta exento de responsabilidad criminal.

El estado de necesidad tiene doble ubicación sistemática: es causa de justificación como también causa de inculpabilidad de la conducta. Tiene esta doble ubicación porque subsana la inconveniencia de mantener a priori una clasificación de

[116] Cello Calón, Op cit, p. 446.
[117] Bentancour, op cit. P. 232.
[118] op cit. P. 236.

las Causas de Justificación y las Causas de Inculpabilidad. La determinación de su naturaleza queda librada a la jurisprudencia o a la doctrina.

Es la falta de reprochabilidad ante el derecho penal por falta de voluntad o conocimiento del hecho.

CAUSA DE INCULPABILIDAD

- Ignorancia y error: Son actitudes Psíquicas del sujeto, en la efectuación de alguna conducta, la ignorancia es el desconocimiento total de un hecho, por lo que es de esperarse que la conducta se realice en sentido negativo y el error es una idea falsa o equivocada respecto a un objeto, cosa o situación constituyendo un estado positivo.

- Error de derecho: cuando el sujeto en la realización de un hecho delictivo alega ignorancia o error de la ley.

- Error de hecho: se divide en error esencial y accidental.

  - "El error esencial el sujeto realiza una conducta antijurídica, pensando que es jurídica, es decir, hay desconocimiento de su antijuricidad.

  - El error accidental no cae sobre circunstancias esenciales del hecho, sino en secundarias, como error de golpe, persona y de delito".[119]

En conclusión podemos decir que la inculpabilidad es el juicio de reproche que se le hace a un sujeto por el injusto penal cometido, o bien es la ausencia de culpabilidad en donde se da por ignorancia o error como lo es el error de derecho, de hecho y accidenta, asimismo, la no exigibilidad de otra conducta y en la falta del nexo causal emocional entre el sujeto y su acto esto es la falta del nexo intelectual y emocional que une al sujeto con su acto.

[119] BENTANCOUR, OP CIT. 240.

2.24 LAS CONDICIONES OBJETIVAS DE PUNIBILIDAD

Son ciertas circunstancias exigidas por la ley penal, para la imposición de la pena, que no pertenecen al tipo del delito, y no condicionan la antijuricidad y tampoco tienen carácter de culpabilidad.

El maestro Maggiore manifiesta que las condiciones objetivas de punibilidad son:

1. "son solamente suspensivas, no resolutivas.

2. suponen un delito completo en todos los elementos esenciales; si algunos de estos faltan, no habrá delito, aunque la condición se verifique.

3. si no se verifica la condición de punibilidad, el delito no es punible, ni siquiera como intentado; también la tentativa supone la verificación de la condición.

4. no es punible la participación o el favorecimiento en un delito condicional, cuya condición de punibilidad no se haya verificado.

5. el momento consumativo del delito condicional coincide no con la consumación efectiva, sino con la realización de la condición."[120]

Para Porte Petit, "las condiciones objetivas de punibilidad no son elementos constitutivos del delito, ya que no se requiere su existencia".[121]

Por lo que podemos decir que las condiciones objetivas de punibilidad son aquellos requisitos establecidos en algunos tipos penales, los cuales sino se presentan no es factible que se configure el delito; de ahí que al manifestarse sólo en algunos tipos penales, es por que no constituyen elementos básicos del delito, sino secundarios, asimismo, son aquellos requisitos establecidos en algunos tipos penales, los cuales si no se presentan no son factibles que se configure el delito.

---

[120] MAGGIORE, DERECHO PENAL I, Editorial Temis, Bogotá, 1954, p.383.

[121] Porte Petit Candaudap, Celestino, APUNTAMIENTOS DE LA PARTE GENERAL DEL DERCHO PENAL, Ed. Porrúa, Mexico, 1998 p.245.

2.25 LA FALTA DE CONDICIONES OBJETIVAS DE PUNIBILIDAD.

La ausencia de las condiciones objetivas de punibilidad, es el aspecto negativo de las mismas.

Jiménez de Asúa expresa que "cuando en la conducta concreta falta la condición objetiva de punibilidad, es obvio que no puede castigarse."[122]

Para Maggiore "las condiciones objetivas de punibilidad se diferencian de dos elementos, en que si no se verifican, el delito existe antológicamente, aunque no pueda ejecutarse la pretensión punitiva del estado; en tanto que si falta alguno de los elementos, no hay delito".[123]

El maestro Porte Petit expresa que "cuando existe una hipótesis de ausencia de condiciones objetivas de punibilidad concurre una conducta o hecho, adecuación al tipo, antijuricidad, imputabilidad y culpabilidad, pero no punibilidad en tanto no se llena la condición objetiva de punibilidad lo que confirma que es una consecuencia del delito".[124]

En conclusión podemos manifestar que la ausencia de condiciones objetivas de punibilidad no pueden castigarse las conductas ilícitas, en donde el incumplimiento de las condiciones de punibilidad, traerá consigo el impedimento de la aplicación de la sanción correspondiente.

2.26 LA PUNIBILIDAD

La punibilidad es un elemento secundario del delito, que consiste en el merecimiento de una pena, en función o por razón de la comisión de un delito; dichas penas se encuentran señaladas en nuestro Código Penal Federal.

---

[122] JIMÉNES DE ASÚA, Luis, PRINCIPIOS DEL DERECHO PENAL, LA LEY Y EL DELITO, Editorial sudamericana, Buenos Aires, 1990, p.425.
[123] Maggiore. Op cit. P. 279.
[124] Porte Petit Candaudap, Celestino, APUNTAMIENTOS DE LA PARTE GENERAL DEL DERCHO PENAL, Ed. Porrúa, Mexico, 1998 p.245.

Cuello Calón, considera que "la punibilidad no es más que un elemento de la tipicidad, pues el hecho de estar la acción conminada con una pena, constituye un elemento del tipo delictivo."[125]

Por su parte Ignacio Villalobos, tampoco considera a la punibilidad como elemento del delito, ya que el concepto de éste no concuerda con el de la norma jurídica: una acción o una abstención humana son penadas cuando se les califica de delictuosas, pero no adquieren este carácter porque se les sancione penalmente.

"Las conductas se revisten de delictuosidad por su pugna con aquellas exigencias establecidas por el Estado para la creación y conservación del orden en la vida gregaria y por ejecutarse culpablemente. Mas no se pueden tildar como delitos por ser punibles".[126]

Jiménez de Asúa dice que son "excusas absolutorias las causas que hacen que a un acto típico, antijurídico, imputable a un autor y culpable, no se asocie pena alguna por razones de utilidad pública."[127]

Finalmente, la punibilidad consiste en el merecimiento de una pena en función de la realización de cierta conducta, es decir, es el castigo aplicable a una conducta ilícita, sancionada por las leyes penales, en otras palabras, es punible una conducta cuando por su naturaleza amerita ser penada, el merecimiento de una pena.

2.27 LAS EXCUSAS ABSOLUTORIAS.

Las excusas absolutorias son aquellas circunstancias específicamente señaladas en la ley y por las cuales no se sanciona al agente.

Así como la punibilidad no es considerada por muchos autores de elementos del delito, así tampoco la imputabilidad como se mencionó en el capítulo anterior.

---

[125] EUGENIO, Cuello Calón. DERECHO PENAL I, 8ª Edición.

[126] VILLALOBOS, Ignacio. DERECHO PENAL MEXICANO. Editorial Porrúa, S.A. México 1975. pp. 455.

[127] JIMÉNES DE ASÚA, Luis. PRINCIPIOS DEL DERECHO PENAL. LA LEY Y EL DELITO. Editorial sudamericana, Buenos Aires, 1990, p.426.

Las excusas absolutorias son aquellas específicas y excepcionales causas por las cuales el legislador deja impune una conducta típica, antijurídica y culpable, en el caso de las excusas absolutorias operan las causas donde revelan que el legislador prefirió aplicar medidas de política criminal, a pesar de que el principio de justicia reclamara la imposición de una pena.

Para Jiménez de Asúa son excusas absolutorias "las causas que hacen que a un acto típico, antijurídico, imputable a un autor y culpable, no se asocie pena alguna por razones de utilidad pública".[128]

Pavón Vasconcelos, después de un análisis minucioso en la legislación penal federal, descarta la mayoría de ellas (encubrimiento entre parientes, o ligados por el afecto o amistad; favorecimiento a la evasión por parientes; el aborto en el caso de con motivo de una violación). Agrupa las excusas absolutorias de la siguiente manera:

1.- "En razón del arrepentimiento y de la mínima peligrosidad del agente; artículos 138 (deposición de armas por el rebelde) y 375 (robo cuyo valor no exceda del salario mínimo.

2.- En razón exclusiva de la mínima o nula peligrosidad por el autor; artículo 333, primera parte (aborto por imprudencia de la propia mujer embarazada) y 340 (injurias reciprocas)".[129]

Las principales excusas absolutorias para Carrancá y Trujillo son:

1. "En razón de los móviles afectivos revelados.
2. En razón de la maternidad consciente.
3. En razón del interés social preponderante.

[128] Jiménez de Asúa, op cit. P. 456.
[129] PAVÓN, Vasconcelos Francisco, MANUAL DE DERECHO PENAL MEXICANO, pagina 395.

4. En razón de la temibilidad específicamente mínima revelada".[130]

Finalmente, en conclusión las excusas absolutorias son aquellas circunstancias específicamente establecidas en la ley y por las cuales no se sanciona al agente, son causas por las cuales la ley exceptúa al delincuente de ser merecedor de una pena, ya sea por que se le conceda el perdón del daño causado entre otras.

[130] Carrancá y Trujillo Raúl, DRECHO PENAL MEXICANO. Ed. Libros de méxico. 1997. p. 378.

CAPITULO III

3.1 Antecedentes históricos de los delitos informáticos e Internet

3.2 Estructura de las computadoras.

3.3 Lenguajes de programación de las computadoras.

3.4 Principales lenguajes de programación.

3.5 Tratamiento internacional y nacional de los delitos informáticos.

3.6 Postura de diversos organismos internacionales en materia de regulación informática

3.7 Legislación comparada de los delitos informáticos.

3.8 Legislación nacional.

3.9 Tratado del libre comercio de América

3.10 Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio, e incluso con el comercio de mercancías falsificadas.

3.11 Código penal del estado de Sinaloa.

3.12 Ley federal de derechos de autor y código penal federal.

CAPITULO III. ANTECEDENTES HISTORICOS Y CONCEPTOS DE LOS DELITOS INFORMATICOS E INTERNET, ASIMISMO, EL TRATAMIENTO JURÍDICO NACIONAL E INTERNACIONAL.

3. I. ANTECEDENTES HISTORICOS DE LOS DELITOS INFORMATICOS E INTERNET.

Para adentrarnos al estudio de las conductas antisociales generadas por los sistemas informativos también llamados Delitos Informáticos, o en sus diferentes denominaciones como delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora o delincuencia relacionada con el ordenador, por lo que entraremos al conocimiento y manejo de lo que es la computadora en nivel operacional y de estructuración, (ya que ésta como se verá más adelante puede ser objeto o fin de dichos delitos), así como la noción de diferentes conceptos relacionados con la computadora y el Internet, esto es para poder tener un mejor manejo del tema.

De manera elemental, diremos que la computadora tiene una estructura a nivel operacional y a nivel estructural.

Habida cuenta que es una máquina automatizada de propósito general, integrada por los elementos de entrada, un procesador central, dispositivos de almacenamiento y elemento de salida, ello nos da la pauta para considerar sus elementos fundamentales a nivel operacional, a saber:

El nacimiento de la informática está relacionado con la necesidad que ha sentido siempre el hombre de disponer de un sistema que le permita manejar gran cantidad de información con relativa rapidez, así como de efectuar cálculos a gran velocidad y de modo mecánico que le libere de las penosas tareas asociadas con estas actividades.

Así tenemos que la informática es un neologismo derivado de los vocablos información y automatización, y en sentido general, es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma

de decisiones, y tomando en consideración que los instrumentos operativos de la informática son las computadoras, es necesario exponer los principales rasgos de las mismas en los siguientes términos.

Desde tiempos muy remotos el hombre, al verse en la necesidad de cuantificar sus pertenencias, animales, objetos de caza, pieles, etc., ha tenido que procesar datos. En un principio, este procedimiento fue muy rudimentario, ya que sólo utilizaba sus manos y almacenaba toda la información posible en su memoria. Esto impedía un flujo fácil de la información, porque al no existir representaciones fijas de los elementos que se tenían en un proceso determinado, las conclusiones a las que llegaban resultaban ser meras especulaciones, puesto que el hombre, para contar estaba limitado al número de sus deudas, y esto fue superado cuando empezó a utilizar otros medios como cuentas, granos y objetos similares.

Posteriormente, inventó sistemas numéricos que le permitieron realizar sus operaciones con mayor confiabilidad y rapidez, e ideó algunas herramientas que le ayudaron en su afán de cuantificar; y entre las primeras creaciones del hombre dirigidas a facilitar las operaciones de cálculo podemos mencionar:

A) EL ÁBACO.

"Fue el primer dispositivo mecánico para realizar cálculos, el cual apareció en forma independiente en varias culturas de la antigüedad, aunque, generalmente, se ha atribuido el crédito de su realización al pueblo babilónico".[131]

Así tenemos que la palabra ábaco encuentra su raíz etimológica en la voz fenicia abak que significa "tabla lista cubierta de arena", es decir, marcos dotados de guías metálicas por las que se mueven cuentas ensartadas en ellas y cuyas posiciones permiten realizar operaciones aritméticas sencillas con rapidez. Estas tabletas de arcilla tienen una antigüedad de 4,000 años y con ellas se llevaban registros de bancos y empresas de préstamos que funcionaban en aquella época.

[131] Téllez, Julio Valdés, DERECHO INFORMÁTICO, Instituto de investigaciones jurídicas, México 1987, p. 12.

"El Código de Hammurabi incluye referencias de transacciones de negocios realizadas con el ábaco, tales como contratos, escrituras, bonos, recibos, inventarios, ventas y otros tipos de operaciones semejantes; asimismo, revela que se usaban, comúnmente, en giros y cheques, y que se cobraban derechos aduanales y peajes en los transbordadores y carreteras. También se han descubierto registros estatales de títulos de propiedad que se usaban para fines impositivos".[132]

Finalmente, podemos concluir que el ábaco que actualmente conocemos, el mismo apareció a fines del Imperio Romano y con él se pueden realizar, con impresionante rapidez, operaciones de suma y resta, así como de multiplicación y división. Por último, el ábaco ha resistido la prueba del tiempo y la velocidad, ya que en la actualidad se utiliza en la realización de operaciones, lo cual, hoy en día, resulta extraordinario, teniendo en cuenta que se trata de un proceso manual; asimismo, estos dispositivos rudimentarios de cálculo todavía se emplean en la actualidad en algunos lugares de Asia, así como en las culturas donde aún se utiliza el sistema arábigo.

B) TABLAS DE LOGARITMOS (1614).

"La dificultad para realizar operaciones de multiplicación y división motivó a John Napier a crear un nuevo método que redujera de manera notable ese trabajo".[133]

Fue así como surgieron las tablas de logaritmos, a través de las cuales es posible realizar multiplicaciones en forma sencilla y rápida; en donde las multiplicaciones se traducen en sumas y las divisiones en restas; sin embargo, había que crear las tablas y sus antialgoritmos e imprimirlas, lo cual representaba un enorme trabajo, que fue realizado por un compañero de Napier, H. Briggs.

---

[132] CD-ROM, JUSTICIA CIBERNETICA.
[133] AWAD, Elias M. PROCESAMIENTO AUTOMÁTICO DE DATOS. México. 1982 p.51.

"No obstante la magnitud del esfuerzo que realizaron, las tablas tuvieron errores que fueron detectados tiempo después".[134]

C) REGLA DE CÁLCULO (1930).

Poco tiempo después de que Naiper inventó la tabla de logaritmos, surgió otro nuevo invento, menos exacto, pero mucho más fácil de utilizar, y al cual se le dio el nombre de regla de cálculo.

Funcionaba con base en la medición de longitudes entre dos reglitas que guardaban relación, utilizando la escala logarítmica.

"Esta herramienta ha sido sumamente utilizada, inclusive en la actualidad, y lo resultados de las operaciones que se realizan con ella se aproximan con suficiente exactitud. No es sino hasta estos últimos años que ha sido desplazada por las calculadoras electrónicas de bolsillo".[135]

D) LA MÁQUINA DE PASCAL (1642).

Blas Pascal creó una máquina capaz de sumar y restar mediante la combinación de una serie de ruedas dentadas. Cada una de dichas ruedas tenía diez dientes que correspondían a los números del 9 al 10, siendo el sistema de tal tipo que, el paso de nueve a cero, daba lugar a un salto de la rueda inmediatamente continua al lado izquierdo. Así tenemos que el dispositivo llamado pascalina, era semejante a los dispositivos mecánicos que se emplean en la actualidad en los cuentakilómetros de los vehículos automóviles.

[134] TÉLLEZ. Op CIT. P. 12.
[135] Tellez, op cit. P. 13

Sin embargo, Pascal llegó a introducir, en versiones posteriores mejoradas, un elemento de memoria mecánico que permitía acumular resultados parciales durante la realización de las operaciones.

"A esta sumadora se le considera como la primera máquina de calcular construida por el hombre".[136]

E) LA MÁQUINA DE GOTTFRIED LEIBNIZ (1646).

Por su parte, Gottfried Leibniz "desarrolló y mejoró el dispositivo creado por Blas Pascal, logrando que la máquina fuese capaz de realizar las cuatro operaciones aritméticas básicas, es decir, la suma, la resta, la multiplicación y la división de forma mecánica". [137]

F) LA TARJETA PERFORADA (1804).

Joseph Marie Jacquard, en Francia, construyó una máquina para tejer complicados diseños de telas. Esta máquina funcionaba con tarjetas perforadas que contenían información del camino que deben seguir los hilos de la tela para lograr un diseño determinado. Esta idea y otras más participaron en el desarrollo de los sistemas de proceso de datos que hoy día se manejan. La idea de Jacquard tuvo grandes repercusiones, ya que "introdujo la automatización y con ella se convirtió en el padre de las tarjetas perforadas".[138]

---

[136] op cit. P.13.
[137] AWAD, op cit, p.52.
[138] op cit p.53.

G) LA MÁQUINA DE BABARE (1834).

Uno de los más notables contribuyentes en el desarrollo de las máquinas de cálculo fue el inglés Charles Babare, quien tuvo el apoyo de su Gobierno para realizar una máquina que fuera capaz de efectuar cálculos complejos y de esta forma eliminar los errores en que frecuentemente se incurría. Esta máquina trabajaba con base en el "método de las diferencias", y la cual fue creada para corregir los errores de las tablas de logaritmos.

No obstante la utilidad que representaría este proyecto, el trabajo no pudo concluirse, ya que el Gobierno Británico, después de haber gastado 17,000 libras, suspendió la subvención.

Tiempo después, Babbage ideó una máquina analítica que sería capaz de ejecutar procesos más complicados como la multiplicación y la división, almacenando resultados intermedios en un dispositivo interno. Así tenemos que ésta máquina contaba con las tablas de logaritmos, realizando decisiones simples, y finalmente, entregaba un resultado impreso de manera automática.

Por último, la idea de utilizar tarjetas perforadas fue tomada por Babbage para "alimentar datos a la máquina analítica, variables o expresiones matemáticas en las que se deseaba realizar algún cálculo; sin embargo, el invento de Babbage fue superior a la capacidad técnica de su época y por lo tanto, no pudo realizarse. Cabe señalar que la máquina de Babbage fue determinante en el desarrollo de las computadoras actuales, ya que cien años después de que él la concibió, sus bases sirvieron de pauta para la realización de la primera computadora electrónica".[139]

H) EL CÓDIGO DE HERMAN HOLLERITH (1880).

En sentido estricto, cabe considerar que los auténticos inicios de la informática datan del siglo XIX, más concretamente de los trabajos realizados por Herman Hollerith (1860-1929), quien era miembro de la oficina del censo de los Estados Unidos de Norteamérica.

---

[139] Téllez, op. cit. P. 13

La contribución de Hollerith consistió en emplear una cinta, que más tarde sustituyó por tarjetas, en las que se grababa la información mediante perforaciones en lugares determinados, siguiendo la idea de telares automáticos, para la realización de copias de ciertos prototipos de telas cuyas muestras eran difíciles de reproducción. Gracias a dicho dispositivo creado en 1890, era posible realizar mecánicamente operaciones tales como la clasificación, duplicación y copia de fichas perforadas.

Por último, "los sistemas de este tipo, que reciben el nombre de preordenadores, se siguen empleando en la actualidad de un modo restringido".[140]

Por otra parte, difícilmente encontraremos en la historia otro ejemplo de transformación tan rápido y amplio como el provocado por la aparición de las computadoras y sus profundas implicaciones; por lo que, en el ámbito operacional, la computadora puede ser definida como la máquina automatizada de propósito general, integrada con elementos de entrada, procesador central, dispositivo de almacenamiento y elementos de salida; y a continuación daremos una breve visión de la evolución de las computadoras.

a) El siguiente paso en el camino del tratamiento auténtico de la información de la computadora se debió a los trabajos de Howard H. Aiken (1900-1973), quien desarrolló entre 1939 y 1944, en el seno de la compañía IBM, el ordenador conocido por ASCC (siglas de Automatic Sequence Controlled Calculator) o MARK I, el cual fue la primera computadora electromecánica automática. Esta máquina se basaba en un dispositivo eléctrico simple, conocido como el relé, y su programación se llevaba a cabo mediante una cinta perforada, es decir, seguía las ideas de la máquina analítica, capaz de realizar cualquier operación matemática sin intervención humana, calculando los resultados con la ayuda de las unidades de almacenamiento (memoria).

[140] Op cit, p.13.

No obstante, "esta máquina era relativamente lenta, ya que su velocidad de operación dependía de la rapidez de sus numerosos componentes (alrededor de 750,00), motivo por el cual no pudo construirse, ya que el nivel técnico de la época no lo permitía; sin embargo, fue utilizada durante quince años para realizar cálculos astronómicos".[141]

b) El siguiente paso se produjo gracias a la aplicación de la electrónica a la resolución de este tipo de problemas. En 1946, la Escuela Moore de Ingeniería Electrónica, situada en Filadelfia, construyó la primera máquina electrónica de calcular, la cual había sido diseñada en la Universidad de Pennsylvania, y a la que se le dio el nombre de ENIAC (siglas inglesas de Electronic Numerical Integrator and Computer, calculador e integrador numérico electrónico). Esta máquina fue considerada como el primer calculador digital carente de piezas móviles Asimismo, la programación del ENIAC se llevaba a cabo mediante el establecimiento de conexiones entre cables eléctricos y el accionamiento de una gran cantidad de interruptores. En las décadas siguientes, el progreso de este tipo de instalaciones fue cada vez más acelerado y siguió una serie de etapas que recibieron el nombre de generaciones, y las cuales abarcaban periodos determinados según se trataba del sistema físico o del lógico, estando dichas generaciones están interrelacionadas, ya que una y otra dependían entre sí.

La primera generación la constituyeron los ordenadores que se construyeron entre los años 1950 y 1960. Se trataban de las primeras máquinas de este tipo que se fabricaron con fines comerciales, siendo el componente electrónico básico el que hacía posible su funcionamiento, y al cual se le dio el nombre de válvula de vacío, consistente en un dispositivo electrónico formado por dos electrodos encerrados en una ampolla, en la que se habían practicado el vacío.

Estas máquinas se programaban directamente en el lenguaje máquina y eran capaces de realizar hasta 1.000 instrucciones por segundo; disponían, asimismo, de una capacidad de memoria que podía llegar hasta las 20.000 posiciones.

---

[141] op. cit.p 14

La segunda generación es la que comprendía los ordenadores construidos entre los años 1960 y 1965.

Dicha generación se caracterizó por el hecho de que el componente electrónico básico sobre el que descansaba era el transistor, el cual consistía en un dispositivo electrónico que actuaba como un interruptor, ya que determinaba el paso o no de la corriente entre dos puntos en función de la tensión aplicada a un tercero; asimismo, el empleo de éste transistor hacía que dicha generación sobresaliera por lograr una sustancial reducción de consumo de energía y del volumen ocupado por las máquinas, así como por un enorme aumento de la fiabilidad y de la velocidad de cálculo de las instalaciones. Los progresos del sistema lógico de los ordenadores dieron paso a la aparición de los sistemas operativos, el procesamiento en régimen de tiempo compartido, los lenguajes de alto nivel, etc.

La tercera generación que abarca desde 1965 a 1975 se caracterizó, fundamentalmente, por la resección de las dimensiones de las instalaciones, ya que su construcción y funcionamiento se basaba en el empleo de los circuitos integrados, en donde un circuito integrado llevaba a albergar hasta 20.000 componentes de una superficie de 25 mm2.

La cuarta generación que abarca desde 1975 hasta nuestros días, se caracteriza, principalmente, por la continuación del proceso de integración, el cual culminó en 1975, con la consecución de una escala de integración que permitía colocar 60,000 componentes en una superficie de 25 mm2.

Asimismo, ésta generación se encuentra relacionada con la aparición del microprocesador (chip en el que se integra la unidad aritmética lógica, la unidad de control y los registros, es decir, con la obtención mediante circuitos integrados de una unidad central de proceso). La aparición del microordenador permitió, además, que la informática se popularizara, llegando a todos los rincones del planeta y aplicándose a una gran cantidad de actividades del ser humano, pasando a formar parte de su vida.

De igual manera, ésta etapa se caracteriza por la especialización de las aplicaciones de la informática, entre las que destacan las telecomunicaciones, el tratamiento electrónico de la imagen, las bases de datos, la inteligencia artificial, el desarrollo de sistemas expertos, el desarrollo de autómatas o robots capaces de reconocer formas e interactuar con el medio en el que desarrollan su actividad, y cuya creciente aplicación en los procesos industriales ha generado una nueva rama de la técnica, llamada robótica, así como otras más.

Finalmente se habla de la llamada quinta generación, la cual se encuentra puesta en marcha por las industrias japonesas del sector, mediante la cual, y a partir de 1981, se trabaja en el desarrollo de ordenadores inteligentes, desde el punto de vista del sistema físico, sin por ello abandonar la idea de un sistema lógico que trabaje sobre la base de la simulación de los procesos que tienen lugar en el intelecto humano. También recibe el nombre de quinta generación dado que se considera que este nuevo concepto revolucionará los ordenadores, tal y como sucedió con las válvulas de vacío, los circuitos integrados, etc. El concepto de las máquinas de la quinta generación se basa en cuatro elementos fundamentales y las cuales son:

1. El módulo de resolución de problemas;

2. El dispositivo de gestión de las bases de conocimientos, es decir, aquella parte del sistema que alberga los conocimientos de los especialistas en la materia y en la que la información está representada mediante reglas de producción o redes semánticas;

3. Una interfase de lenguaje natural; y,

4. Un modulo de programación.[142]

[142] CD-ROM, JUSTICIA CIBERNETICA

3.2 ESTRUCTURA DE LAS COMPUTADORAS.

Tomando en cuenta que la computadora es una máquina automatizada de propósito general, integrada por elementos de entrada, un procesador central, dispositivos de almacenamiento y elementos de salida, ello nos dan la pauta para considerarlos como sus elementos fundamentales en el ámbito operacional, y los cuales consisten en:

A) "ELEMENTOS DE ENTRADA, representado por la forma de alimentación de información a la computadora, por medio de datos e instrucciones realizados por elementos periféricos tales como pantallas, lectoras de soportes magnéticos, discos, disquetes, etc2.[143]

B) "EL PROCESADOR CENTRAL, siendo el dispositivo en que se ejecutan las operaciones lógico-matemáticas, conocido más comúnmente como unidad central del proceso, es decir, el CPU (siglas en inglés)";[144]

D) DISPOSITIVO DE ALMACENAMIENTO, el cual contiene o almacena la información que se ha de procesar;

D) ELEMENTOS DE SALIDA, siendo los medios en los que se reciben los resultados del proceso efectuado (pantalla, impresoras, graficadoras). Por otra parte, a nivel estructural la computadora está integrada por los siguientes elementos:

A) HARDWARE, constituido por las partes mecánicas, electromecánicas y electrónicas, como estructura física de las computadoras y encargadas de la

[143] Téllez, op. cit p.16.
[144] op.,it p.16.

captación, almacenamiento y procesamiento de información, así como la obtención de resultados; y

B) "**SOFTWARE**, que constituye la estructura lógica que permite a la computadora la ejecución del trabajo que se ha de realizar".[145]

3.3 LENGUAJES DE PROGRAMACIÓN DE LA COMPUTADORA.

Así tenemos que para que las computadoras puedan funcionar en los términos adecuados, es necesaria la utilización de los llamados lenguajes de programación, considerados como aquellos medios que permiten la comunicación entre el hombre y la máquina, es decir, entre la computadora y el usuario.

Dichos lenguajes, si bien caracterizados por complicados revestimientos técnicos, procuran ser lo más afines posibles al llamado lenguaje natural o coloquial, con la intención de facilitar el "diálogo interactivo"; sin embargo, no dejan de ser, en su mayoría, complejos y de ahí que se mencionen diferentes niveles de los mismos, como por ejemplo, alto, bajo, etc.

3.4 PRINCIPALES LENGUAJES DE PROGRAMACIÓN

A) "LENGUAJE FORTRAN.

Este lenguaje apareció en 1957, y significa Fórmula Traductora, y el cual es caracterizado por sus fines inminentemente científicos y matemáticos.

---

[145] AWAD, op cit, p.57

B) LENGUAJE ALGOL.

Este lenguaje significa Lenguaje Algoritmico, y el cual surgió en 1958, también con propósitos fundamentalmente científicos.

C) LENGUAJE COBOL.

Este lenguaje se encuentra orientado a negocios comunes y fue creado en 1960, dirigido a aplicaciones administrativas.

D) LENGUAJE BASIC.

Este lenguaje significa Código de Instrucciones Simbólicas para Principiantes de todo Propósitos, apareciendo en 1958, y el cual se encuentra caracterizado por su relativa sencillez, pronunciada potencia y versatilidad; pretendiendo unificar y facilitar el acceso general a las computadoras.

E) LENGUAJE PASCAL.

Este leguaje apareció como un lenguaje de propósito general, enfocado a una programación estructurada.

F) LENGUAJE ADA.

Este lenguaje, en la actualidad, es utilizado, fundamentalmente, por el Departamento de Defensa de los Estados Unidos.

G) OTROS".[146]

Cabe mencionar que los lenguajes mencionados con antelación no son los únicos existentes en la actualidad, sino que existen muchísimos más, de los que podemos mencionar al lenguaje CANDE, el lenguaje APLE, etc.

El inicio del Internet, se remonta a 1969, cuando la Agencia de Proyectos de Investigación Avanzada en Estados Unidos, conocida por sus siglas, "ARPA", desarrolló ARPANET, una especie de red que unía redes de cómputo del ejército y de laboratorios universitarios que hacían investigaciones sobre la defensa.

Esta red, permitió primero a los investigadores de Estados Unidos acceder y usar directamente supercomputadoras localizadas en algunas universidades y laboratorios clave; después, compartir archivos y enviar correspondencia electrónica.

A finales de 1970 se crearon redes cooperativas descentralizadas, como UUCP, una red de comunicación mundial basada en UNIX y USENET (red de usuarios), la cual daba servicio a la comunidad universitaria y más adelante a algunas organizaciones comerciales.

En 1980, las redes más coordinadas, como CSNET (red de ciencias de cómputo), y BITNET, empezaron a proporcionar redes de alcance nacional, a las comunidades académicas y de investigación, las cuales hicieron conexiones especiales que permitieron intercambiar información entre las diferentes comunidades.

En 1986, se creó la NSFNET (red de la Fundación Nacional de Ciencias), la cual unió en cinco macro centros de cómputo a investigadores de diferentes Estados de Norte América, de este modo, esta red se expandió con gran rapidez, conectando redes académicas a más centro de investigación, remplazando así a ARPANET en el trabajo de redes de investigación. ARPANET se da de baja en marzo de 1990 y CSNET deja de existir en 1991, cediendo su lugar a INTERNET.

---

[146] CD-ROM, JUSTICIA CIBERNETICA

Esta red se diseñó para una serie descentralizada y autónoma de uniones de redes de computo, con la capacidad de transmitir comunicaciones rápidamente sin el control de persona o empresa comercial alguna y con la habilidad automática de renrutar datos si una o más uniones individuales se dañan o están por alguna razón inaccesibles.

Cabe señalar que entre otros objetivos, el sistema redundante de la unión de computadoras se diseñó para permitir la continuación de investigaciones vitales y comunicación cuando algunas partes de ésta red se dañaran por cualquier causa.

Gracias al diseño de Internet, y a los protocolos de comunicación en los que se basan un mensaje enviado por éste medio puede viajar por cualquiera de diversas rutas, hasta llegar a su destino, y en caso de no encontrarlo, será renrutado a su punto de origen en segundos.

Una de las razones del éxito de Internet, es su interoperatividad, es decir, su capacidad para hacer que diversos sistemas trabajen conjuntamente para comunicarse, siempre y cuando los equipos se adhieran a determinados estándares o protocolos, que no son sino reglas aceptadas para transmitir y recibir información.

Actualmente, cualquier persona puede ofrecer su propia página, un lugar virtual en el WWW (World Wide Web) o abrir su propio foro de discusión, de los que hoy en día existen alrededor de veinte mil y que abordan desde temas muy interesantes hasta muy deleznables, incluyendo comportamientos criminales.

El espíritu de la información que se maneja en Internet es que sea pública, libre y accesible a quien tenga la oportunidad de entrar a la red, lo cual marca un principio universalmente aceptado por los usuarios y que a dado lugar a una normativa sin fronteras y de lo cual podemos deducir, en términos jurídicos, cual sería la ratio iuris o razón de ser de esta especial normatividad.

Se intenta que Internet, sea, un medio interactivo viable para la libre expresión, la educación y el comercio. No existe institución académica, comercial, social o gubernamental que pueda administrarla. Son cientos de miles de operadores y redes

de cómputo, que de manera independiente, deciden usar los protocolos de transferencia y recepción de datos para intercambiar comunicaciones, información. No existe un lugar que concentre o centralice la información de Internet. Sería técnicamente imposible.

Los individuos tienen una amplia gama de formas de introducirse al Internet, a través de los proveedores de acceso a Internet, conocidos en el medio de las telecomunicaciones como (Internet Service Provider).

En términos de acceso físico, se puede usar una computadora personal, conectada directamente (por cable coaxial o de fibra óptica) a una red (un proveedor de servicios de Internet, por ejemplo), que éste a su vez, conectada a Internet; o puede hacerse una computadora personal con un módem conectado a una línea telefónica a fin de enlazarse a través de ésta a una computadora más grande o a una red, que esté directa o indirectamente conectada a Internet.

Ambas formas de conexión son accesibles a las personas en una amplia variedad de Instituciones académicas, gubernamentales o comerciales. Lo cierto es que hoy en día el acceso a la red de Internet es cada vez más sencillo en Universidades, bibliotecas y cibercafeterias, lo cual está estrechamente relacionado con el número de proveedores de servicios de Internet.

INTERNET EN MEXICO, fue el primer país latinoamericano en conectarse a Internet, lo cual ocurrió a finales de la década pasada, en febrero de 1989, a través de los medios de acceso e interconexión de teléfonos de México, compañía mexicana que había constituido el monopolio telefónico del pais hasta el once de agosto de 1996. Los primeros enlaces de Internet en el país, que tuvieron fines exclusivamente académicos, por cierto, se establecieron en el Instituto Tecnológico de Estudios Superiores de Monterrey, el Instituto Politécnico Nacional, la Universidad de Guadalajara y la Universidad de las América en Puebla.

En este periodo el uso internacional del Internet origina una normativa no escrita, seguida por los usuarios de nuestro país, la cual se basaba en usos, sin reglas formales, fundada más bien en consideraciones de tipo ético entre la

comunidad académica. En 1994 se incorporan instituciones comerciales en nuestro país, dando lugar a una visión diferente del fenómeno de Internet.

La "era de la información", impone en nuestro país, al igual que en el mundo globalizado, nuevas formas de organización, en los negocios, el mundo de la academia, los gobiernos y, cada vez más, en todas las actividades habituales a pesar de que la cultura de la informática y de la información en México se encuentran aún en sus inicios, hoy en día la tecnología de la información constituye para muchas empresas y universidades nacionales un instrumento insustituible para la realización de trabajos específicos. El uso de la computadora como instrumento o herramienta de trabajo, según datos del INEGI, es incipiente, en 1994 sólo existían 2.2 computadoras personales por cada cien habitantes, lo que ubica a nuestro país en el lugar numero veintiocho a nivel mundial en este aspecto.

"Es previsible que el mundo virtual traiga consigo cambios de importancia en las instituciones jurídicas existentes, así como el desarrollo de instituciones jurídicas nuevas que regulen nuevos intereses y nuevas relaciones".[147]

Los servicios más importantes que brinda el INTERNET, en general son los siguientes:

a) CORREO ELECTRONICO, siendo el servicio de mayor uso, de mayor tráfico y, por lo tanto, de mayor importancia para el surgimiento, en la actualidad, de diversas relaciones contractuales. Permite escribir y enviar mensajes a una persona o grupo de personas conectadas a la red;

b) TRANSFERENCIA DE ARCHIVOS, el cual permite transferir archivos, los cuales pueden ser de texto, gráficas, hojas de cálculo, programas, sonido y vídeo.

[147] BARRIOS, Garrido Gabriela, INTERNET Y DERECHO EN MÉXICO, Ed. Mc Graw Hill, México, 2001,P 175.

c) ACCESO REMOTO A RECURSOS DE COMPUTO POR INTERCONECCION, (telnet), es una herramienta interactiva que permite introducirse, desde una computadora en casa o en la oficina, a sistemas, programas y aplicaciones disponibles en otra computadora, generalmente ubicada a gran distancia y con gran capacidad;

d) WORD WIDE WEB, el servicio más nuevo y popular de Internet, caracterizado por la interconexión de sistemas a través del hipertexto, por medio del cual pueden transmitirse textos, gráficas, animaciones, imágenes y sonido. Se le considera un elemento importante de mercadotecnia.

e) GRUPOS DE DISCUSION (Usenet), existen hoy día alrededor de quince mil grupos enfocados a diversos temas, en la actualidad se llega alrededor de cien mil mensajes por día;

f) COMUNICACIÓN EN TIEMPO REAL, (Internet Relay Chat), es la posibilidad de establecer diálogos inmediatos en tiempo real, a través de Internet, permitiendo a dos o más personas "dialogar" simultáneamente por escrito, sin importar la distancia geográfica. Esta forma de comunicación es análoga a la línea de teléfono, sólo que emplea el teclado o monitor en lugar del auricular.

Ahora bien, el concepto y noción de "CIBERNETICA" si atendemos a la etimología de dicha palabra, proviene del vocablo "cibernética" que toma su origen de la voz griega "Kybernetes piloto", y kybernes", concepto referido al arte de gobernar. Esta palabra alude a la fusión del cerebro con respecto a las máquinas.

La noción de **"INFORMATICA"**, es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en el año de 1962.[148]

[148] BARRIOS, Garrido Gabriela, INTERNET Y DERECHO EN MÉXICO, Ed. Mc Graw Hill, México, 2001 P.180

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

Mora y Molino, la definen como "un estudio que delimita las relaciones entre los medios es decir equipo, y los datos y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado".[149]

Mario G. Lozano, caracteriza a la informática como "un producto de la cibernética, en tanto un proceso científico relacionado con el tratamiento automatizado de la información en un plano interdisciplinario".[150]

La definición que podemos dar del **INTERNET**, es que este no es un cuerpo físico o tangible, sino una red gigante que interconecta una innumerable cantidad de redes locales de computadoras. Es la red de redes.

También podemos considerar que Internet es un sistema internacional de intercambio de información que une a personas, instituciones, compañías y gobiernos alrededor del mundo, de manera casi instantánea, a través del cual es posible comunicarse, con un solo individuo, con un grupo amplio de personas interesadas en un tema específico o con el mundo en general.

Es un medio de comunicación que tendrá un profundo efecto social, si tomamos en cuenta la teoría de la aldea global, del canadiense Marshall Muluhan.

En términos generales, Internet se ha convertido en un polémico escenario de contrastes en donde todo es posible: desde encontrar información de contenido invaluable, de alcances insospechados en el ámbito de la cultura, la ciencia y el desarrollo personal, hasta caer en el terreno del engaño, la estafa o la corrupción de menores.

---

[149] Mora, José Luis, Molina Enzo, INTRODUCCIÓN A LA INFORMÁTICA, 1999,p.85.
[150] Op. cit.86

Se calcula que Internet enlaza hoy día a 60 millones de computadoras personales en un extenso tejido electrónico mundial, lo cual hace necesario entenderla como un fenómeno social, dado el crecimiento exponencial que ha mostrado.

Entendiendo al Internet como la red de redes, donde como se mencionó entrelaza a 60 millones de computadoras personales a nivel mundial, sin tomar en cuenta la cantidad de personas que puedan conectarse a la red de redes sin tener una computadora personalizada, esto nos da una idea del desarrollo tan amplio que ha tenido en la última década.

Así pues, se habla constantemente de los beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual, más sin embargo, también dicho avance nos muestra otra cara de la moneda, siendo las conductas delictivas, pues se abrió la puerta a conductas antisociales que se manifiestan en formas que hasta ahora no era posible imaginar.

"Los sistemas de computadoras ofrecen oportunidades nuevas para infringir la ley, y ha creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales".[151]

3.5 TRATAMIENTO INTERNACIONAL Y NACIONAL DE LOS DELITOS INFORMATICOS.

Los delitos informáticos constituyen una gran laguna en nuestras leyes penales, así pues, el derecho comparado nos permite hacer una lista de los delitos que no están contemplados en el Código Penal y que requieren análisis urgente por parte de nuestros académicos, penalistas y legisladores. Por lo tanto, en este apartado se verá que países disponen de una legislación adecuada para enfrentarse con el problema sobre el particular:

---

[151] BARRIOS, Garrido Gabriela, INTERNET Y DERECHO EN MÉXICO, Ed. Mc Graw Hill, México, 2001.

➢ TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR LA ORGANIZACIÓN DE LAS NACIONES UNIDAS:

Los delitos informáticos constituyen una gran laguna en nuestras leyes penales, así pues, el derecho comparado nos permite hacer una lista de delitos que no están contemplados en el Código Penal Federal y que requieren de un análisis urgente por parte de nuestros académicos, penalistas y legisladores, por lo tanto, a nivel de las organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del octavo congreso sobre prevención del delito y justicia penal, celebrado en 1990 en la Habana Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos, por tal motivo, el principal problema era la reproducción y difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos , por lo que el congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer a esta formas de delincuencia ya era necesario adoptar medidas preventivas para evitar su aumento.

Las conductas o acciones que considera las Naciones Unidas como delitos informáticos son las siguientes:

I) Los Fraudes cometidos mediante manipulación de computadoras: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común.

II) La manipulación de programas; este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas que tienen conocimiento especializados en programación informática.

III) La Manipulación de datos de salida; se efectúa fijando un objetivo al funcionamiento del sistema informático, el ejemplo más común es el fraude que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

IV) Fraude efectuado por manipulación informáticas de los procesos de cómputo.

V) Falsificaciones informáticas; cuando se alteran datos de los documentos almacenados en forma computarizada.

VI) Como instrumentos; las computadoras pueden utilizarse también para efectuar falsificación de documentos de uso comercial

VII) Sabotaje Informático; es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

VIII) Los Virus; Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.-

IX) Los Gusanos; los cuales son análogos al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

X) La Bomba lógica o cronológica; la cual exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

XI) Acceso no autorizado a servicios u sistemas informáticos; esto es por motivos diversos desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

XII) Piratas Informáticos o Hackers; este acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones.

XIII) Reproducción no autorizada de programas informáticos de protección legal; la cual trae una pérdida económica sustancial para los propietarios legítimos.

Partiendo del estudio comparativo de las medidas que se han adoptado a nivel internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera del delito informático y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, deben mencionarse la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición. Teniendo presente esa situación, consideramos 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 los miembros de la comunidad internacional.

En otro orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos.

Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promover se la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad).

Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta qué punto el derecho penal se extiende a esferas afines con un criterio importante para

ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.[152]

En conclusión, considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que pueden entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación corno delito punible de la conducta descrita en la "lista facultativa", especialmente la alteración de datos de computadora y el espionaje informático; así como que por lo que se refiere al delito de acceso no autorizado precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Además, señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

3.6 POSTURA DE DIVERSOS ORGANISMOS INTERNACIONALES EN MATERIA DE REGULACIÓN INFORMÁTICA

El objetivo de este capítulo es presentar todos aquellos elementos que han sido considerados tanto por organismos gubernamentales internacionales como por diferentes Estados, para enfrentar la problemática de los delitos informáticos a fin de incorporar a la vida jurídica la regulación de dichas conductas.

En este orden, debe mencionarse que durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen las leyes derechos penales nacionales.

---

[152] NACIONES UNIDAS, Prevención del delito y justicia penal en el contecto del desarrollo, realidades y perspectivas de la cooperación internacional. Documento preparado por la Secretaría (A/CONF. 144/5). Octavo congreso de las Naciones Unidas sobre Prevención del delito y tratamiento del delincuente. La Habana, Cuba, 27 de Agosto- 7 de Septiembre 1990.

En un primer término, debe considerarse que en 1983, la OCDE inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

De esta forma, la OCDE en 1986 publicó un informe titulado Delitos de Informática: Análisis de la Normativa Jurídica, en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales (Lista Mínima), como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

La mayoría de los miembros de la Comisión Política de Información, Computadores y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos (Lista Optativa o Facultativa) como espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales, y el acceso o empleo no autorizado de sistemas de computadoras.

Con objeto de que se finalizara la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La Lista Mínima preparada por la OCDE se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité Especial de Expertos sobre Delitos Relacionados con el Empleo de las Computadoras, del Comité Europeo para los Problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el Consejo de Europa aprobó la recomendación R (89)9 sobre delitos informáticos, en la que se "recomienda a los gobiernos de los Estados Miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras y en particular las directrices para los legisladores nacionales".

Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el Derecho Penal, así como una

lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente, en 1992, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.

En este contexto, se considera que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de delitos informáticos, ello es resultado de las características propias de los países que los integran, quienes, comparados con México u otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Por otra parte, a nivel de organizaciones intergubernamentales de carácter mundial, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo.

Por tal motivo, si bien el problema principal, hasta ese entonces, era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento. En general, se supuso que habría un gran número de casos de delitos informáticos no registrados.

Por todo ello, en vista de que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

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

a) Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.

b) Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

c) Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

d) No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

e) Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

f) Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Teniendo presente esa situación, es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. 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 los miembros de la comunidad internacional.

En otro orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo, Alemania, en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el Derecho Penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación, deberá tenerse en cuenta hasta qué punto el Derecho Penal se extiende a esferas afines con un criterio importante para ello, como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

Considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que puede entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura, y con referencia a la aplicabilidad de su legislación vigente, la tipificación

como delito punible de la conducta descrita en la Lista Facultativa, especialmente la alteración de datos de computadora y el espionaje informático.

Así como que por lo que se refiere al delito de acceso no autorizado, precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia. Además, se señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

En general, se ha pretendido contribuir mediante recomendaciones a la uniformidad de las normas que sancionan los delitos informáticos en el ámbito internacional, sin dejar de observar la tradición jurídica de cada país.[153]

3.7 LEGISLACIÓN COMPARADA

TRATAMIENTO INTERNACIONAL.

Un análisis 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, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados por los ordenadores.

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.

---

[153] COMISIÓN DE LAS COMUNIDADES EUROPEAS. Europa en la vanguardia de la sociedad mundial de la información: plan de actuación móvil, Bruselas, 21.11.1996 COM (96) 607 final; COMISIÓN DE LAS COMUNIDADES EUROPEAS. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Contenidos ilícitos y nocivos en Internet. Bruselas, 16.10.1996 COM (96) 487 final.

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Comunicación de la Comisión. Seguimiento del Libro Verde sobre Derechos de Autor y Derechos afines en la sociedad de la información. Bruselas, 20.11.1996 COM (96) 568 FINAL.

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.

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho Penal tradicional, existen, al menos en parte, relevantes dificultades. Éstas proceden en buena medida de la prohibición jurídico-penal de analogía, y en ocasiones son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales de occidente existe un amplio consenso sobre estas valoraciones que se refleja en las reformas legales de los últimos años.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, a continuación se presenta los siguientes casos particulares:

A) ALEMANIA.

Para hacer frente a la delincuencia relacionado con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

1. Espionaje de datos.

2.- Estafa Informática.

3.- Falsificación de datos probatorios.

4.- Alteración de Datos.

5.- Sabotaje Informático.

6.- Utilización abusiva de cheques o tarjetas de crédito.[154]

Cabe mencionar que esta solución fue también adoptada en los Países Escandinavos y en Austria.

Alemania también cuenta con una Ley de Protección de Datos, promulgada el 27 de enero de 1977, en la cual, en su numeral primero menciona que "el cometido de la protección de datos es evitar el detrimento de los intereses dignos de protección de los afectados, mediante la protección de los datos personales contra el abuso producido con ocasión del almacenamiento, comunicación, modificación y cancelación (proceso) de tales datos. La presente ley protege los datos personales que fueren almacenados en registros informatizados, modificados, cancelados o comunidades a partir de registros informatizados".

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, "dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos".[155]

B) AUSTRIA.

Ley de reforma del Código Penal del 22 de diciembre de 1987, la cual contempla los siguientes delitos:

"1.- Destrucción de Datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

---

[154] TELLEZ Valdes, Julio. DERECHO INFORMÁTICO, segunda edición, México, Editorial De McGram Hill, 1996, p.162-188.
[155] Téllez, op cip. P.143-174.

2.- Estafa Informática. (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos".[156]

C) CHILE.

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Esta ley se refiere a los siguientes delitos:

La destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas de prisión.

Asimismo, dentro de esas consideraciones se encuentran los virus.

Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.

Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

Legislación - Contexto Nacional

En el contexto nacional se pueden encontrar legislaturas que castiguen algunos de los tipos de delitos informáticos, para lo cual se deben citar:

El código procesal penal.

La Ley de Fomento y Protección de la Propiedad Intelectual.

» Código Procesal Penal.

[156] CD, Informática y Derecho, Informática Jurídica, Tecnológico de Monterrey.

Dentro de esta ley se contemplan algunos artículos que guardan relación con los delitos informáticos, específicamente con los siguientes:

La difusión, exhibición, explotación de pornografía infantil por medios informáticos (Art. 172 Y 173).

Estafa agravada, realizar manipulación que interfiera el resultado de un procesamiento o transmisión de datos (Art. 216 Num.5).

Delitos relativos a la propiedad intelectual (Art. 226 Y 227).

Además en dicho código se establece que la realización de estos delitos puede significar para los delincuentes penas de prisión que van desde los 6 meses hasta los 8 años (dependiendo del tipo de delito). Referido a esto es necesario menciona que en nuestro país desgraciadamente no se cuenta con la capacidad instalada para controlar este tipo de Cuenta con una ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993, la cual en sus cuatro numerales menciona: Artículo 1° "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo". Artículo 2° " El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio". Artículo 3°"

El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

Artículo 4° " El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si

quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".[157]

D) ESTADOS UNIDOS.

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. La nueva leyes un adelanto porque está directamente en contra de los actos de transmisión de virus.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

Cabe mencionar, la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional; que modificó al Acta de Fraude y Abuso Computacional de 1986. Dicha acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año de prisión.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos; específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen.

---

[157] CD, Informática y Derecho, Informática Jurídica, Tecnológico de Monterrey.

Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple que se debe entender como acto delictivo.

Es interesante también señalar que el Estado de California, en 1992 adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta ley de 1994.[158]

E) FRANCIA.

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

- Intromisión fraudulenta que suprima o modifique datos.

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

- Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.

- Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema.[159]

Las disposiciones penales están contempladas en sus numerales del 41 al 44, los cuales contemplan lo siguiente: Artículo 41" El que hubiere procedido o mandado proceder a la realización de tratamientos automatizados de información nominativa sin que hubieran sido publicados los actos reglamentarios previstos en el artículo 15 o formuladas las denuncias previstas en el artículo 16, supra, será castigado con pena de privación de libertad de seis meses a tres años y con pena de multa de 2

[158] Téllez, op cit, 175-198.
[159] TELLEZ Valdes, Julio. DERECHO INFORMÁTICO, segunda edición, México, Editorial De Mc Gram Hill, 1996, p. 202-218

000 a 200 000 francos, o con una sola de estas dos penas. Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos, en las condiciones que determinare y a expensas del condenado".

Artículo 42 " El que hubiere registrado o mandado registrar, conservando o mandando conservar informaciones nominativas con infracción de las disposiciones de los artículos 25, 26 y 28, será castigado con pena de privación de libertad de uno a cinco años y con pena de multa de 20 000 a 2 000 000 francos, o con una de estas dos penas.

Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos en las condiciones que determine, y a expensas del condenado.

Artículo 43. "El que habiendo reunido, con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento, informaciones nominativas cuya divulgación tuviere como efecto atentar contra la reputación o la consideración de la persona o la intimidad de la vida privada; hubiere, sin autorización del interesado y a sabiendas, puesto tales informaciones en conocimiento de una persona que no estuviere habilitada para recibirlas a tenor de las disposiciones de la presente ley o de otras disposiciones legales, será castigado con pena de privación de libertad de dos a seis meses y con pena de multa de 2 000 a 20 000 francos, o con una de las dos penas.

El que por imprudencia o negligencia, hubiere divulgado o permitido divulgar informaciones de la índole de las que se mencionan en le párrafo anterior, será castigado con pena de multa de 2 000 a 20 000 francos. Artículo 44 "El que, disponiendo de informaciones nominativas con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento las hubiere desviado de su finalidad, según la misma hubiera sido definida, bien en el acto reglamentario previsto en el artículo 15, supra, o en las denuncias formuladas en aplicación de los

artículos 16 y 17, bien en una disposición legal, será castigado con pena de privación de libertad de uno a cinco años y con multa de 20 000 a 2000 000 francos".[160]

F) ITALIA.

En un país con importante tradición criminalista, como Italia, nos encontramos tipificados en su Código Penal los siguientes delitos:

a) Acceso Abusivo. Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso a aquél sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.

b) Abuso de la calidad de operador de sistemas. Este delito es un agravante al delito de acceso abusivo y lo comete quien tiene la posibilidad de acceder y usar un sistema informático o telemático de manera libre por la facilidad de la comisión del delito.

c) Introducción de virus informáticos. Es penalmente responsable aquel que cree o introduzca a una red programas que tengan la función específica de bloquear un sistema, destruir datos o dañar el disco duro, con un castigo de reclusión de hasta dos años y multas considerables.

d) Fraude Informático.- Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un injusto beneficio, ocasionando daño a otro. También se entiende como tal la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en ellos contenidos o pertenecientes a ellos, cuando se

[160] DAVARA Rodríguez, Miguel angel. DERECHO INFORMATICO. México. Editorial Aranzadi. 1993, P.319

procure una ventaja injusta, causando daño a otro. La punibilidad de este tipo de delito es de meses a tres años de prisión, más una multa considerable.

e) Intercepción abusiva.- Es un delito que se comete junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. Asimismo, es la intercepción fraudulenta, el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público, mediante cualquier medio, de la información, de esas publicaciones; este delito tiene una punibilidad de 6 meses a 4 años de prisión. Asimismo, se castiga el hecho de realizar la instalación de equipo con el fin anterior.

f) Falsificación informática. Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. En este caso, se presupone la existencia de un documento escrito (aunque se debate doctrinariamente si los documentos electrónicos o virtuales pueden considerarse documentos escritos). En este caso, la doctrina italiana tiene muy clara la noción de "documento informático", al cual define como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.

g) Espionaje Informático.- Es la revelación del contenido de documentos informáticos secretos o su uso para adquirir beneficios propios, ocasionado daño a otro.

h) Violencia sobre bienes informáticos. Es el ejercicio arbitrario, con violencia, sobre un programa, mediante la total o parcial alteración, modificación o cancelación del mismo o sobre un sistema telemático, impidiendo o perturbando su funcionamiento.

i) Abuso de la detentación o difusión de Códigos de acceso (contraseñas).

j) Violación de correspondencia electrónica, la cual tiene agravantes si causare daños.

Por su parte, la Constitución de la República Portuguesa, hace mención sobre la utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976, y la cual menciona:

Artículo 35: " Utilización de la Informática.

1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización.

2. La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos.

3. Queda prohibida la atribución de un número nacional único a los ciudadanos".[161]

G) ESPAÑA.

En el Nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicará pena de prisión o multa. En lo referente a:

La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa.

En materia de estafas electrónicas, el nuevo Código Penal de España, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

[161] CD, Informática y Derecho, Informática Jurídica, Tecnológico de Monterrey.

De lo anterior, se advierte que en diferentes países se han preocupado por el mal uso que pueda tener los grandes avances tecnológicos, el cual sin una reglamentación adecuada pueden desbordarse y salir de un control, así pues, la apremiante necesidad de que en nuestro Código Penal del Estado, se contemplen de una forma u otra.

La legislación y regulación sobre los delitos informáticos en otros países, constituye un gran avance para países como en el nuestro que no tienen una legislación al respecto, por lo anterior, no se va ha realizar una crítica a las anteriores disposiciones legales, ya que cada país contempló dichas normas de acuerdo a sus necesidades propias, como se puede observar en líneas precedentes, (ya que algunos países se enfocaron propiamente a proteger el derecho a la privacidad, y a la propiedad intelectual, o como el que disponga de informaciones nominativas y haga un mal uso de ello; otros tantos a proteger al patrimonio de las personas afectadas como en los fraudes informáticos etcétera). Más sin embargo como se mencionó con anterioridad, nos ayudan y nos dan la pauta para que nuestros legisladores contemplen las figuras delictivas de "delitos informáticos", de acuerdo a nuestra realidad".[162]

H) GRAN BRETAÑA.

Debido a un caso de hacking en mil novecientos noventa y uno, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado hasta con cinco años de prisión o multas.

Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

---

[162] TELLEZ Valdes, Julio DERECHO INFORMÁTICO, segunda edición, México, Editorial De Mc Gram Hill, 1996, p. 250-272

I) HOLANDA

El uno de Marzo de mil novecientos noventa y tres entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría) y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

3.8 LEGISLACION NACIONAL DEL DELITO INFORMATICO.

En México, Internet no se ha regulado de manera expresa, como tampoco en el resto de los países latinoamericanos. Su uso gira en torno a cierto Código Ético y la tendencia Institucional es que será un fenómeno "autorregulable".

A pesar de los índices de crecimiento del uso de la computadora y de Internet, México enfrenta un problema social consistente en lo que denominamos "analfabetismo informático", del cual el Poder Legislativo no está exento, por lo que muchos congresistas no entienden el concepto y la estructura de Internet. Asimismo, nos atrevemos a afirmar que tanto los jueces como los magistrados que forman parte del Poder Judicial tienen hoy día la misma carencia.

Es difícil prever el pronunciamiento de los tribunales federales o de la Suprema Corte de Justicia Mexicanos en un caso cuya resolución se base esencialmente en un conflicto por el uso de Internet, por lo cual no se tiene conocimiento de la existencia de tesis ni jurisprudencia algunas que se refieran a los medios electrónicos en general y a Internet en especial.

Como se mencionó es un Código Ético el que puede regular la conducta de los usuarios, mas sin embargo, existe en nuestro país una regulación administrativa sobre las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos, en este sentido, se considera pertinente recurrir a aquellos tratados internaciones de los que el Gobierno de México es parte en virtud de que el artículo 133 Constitucional "establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión".[163]

Para él desarrollo de este capítulo se analizará la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos.

En este entendido, consideramos pertinente recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte en virtud de que "el artículo 133 constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión".[164]

[163] CD, Informática y Derecho, Informática Jurídica, Tecnológico de Monterrey.
[164] Constitución Política de los Estados Unidos Mexicanos, p.*.

3.9 TRATADO DE LIBRE COMERCIO DE AMÉRICA DEL NORTE (TLC)

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la 6a. parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además que deberán conceder derechos de renta para los programas de cómputo.

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse el contenido del párrafo primero del artículo 1717 titulado Procedimientos y Sanciones Penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.

Asimismo, debe mencionarse que en "el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos, sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información".[165]

Llama la atención que en su párrafo segundo habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que estos contienen medios electrónicos o magnéticos.

3.10 ACUERDO SOBRE LOS ASPECTOS DE LOS DERECHOS DE PROPIEDAD INTELECTUAL RELACIONADOS CON EL COMERCIO, INCLUSO EL COMERCIO DE MERCANCÍAS FALSIFICADAS.

El Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT), manteniendo su vigencia hasta nuestros días.

Consideramos que debe destacarse el hecho de que en este acuerdo, en el artículo 10, relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

Además, en la parte sobre observancia de los derechos de propiedad intelectual, en la sección I de obligaciones generales, específicamente en el artículo 41, se incluye que los miembros del acuerdo velarán porque en su respectiva legislación nacional se establezcan procedimientos de observancia de los derechos de propiedad intelectual.

[165] Tratado de Libre Comercio (TLC) Parte 3, Diario Oficial de la Federación, Lunes 20 de Diciembre de 1993.

Asimismo, en la sección u, denominada procedimientos penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales además de que, "los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias.

Finalmente, en la parte VII, denominada disposiciones institucionales, disposiciones finales, en el artículo 69 relativo a la cooperación internacional, se establece el intercambio de información y la cooperación entre las autoridades de aduanas en lo que se refiere al comercio de mercancías de marca de fábrica o de comercio falsificadas y mercancías piratas que lesionan el derecho de autor.

Como se observa, "el tratamiento que los dos instrumentos internacionales que se han comentado otorgan a las conductas ilícitas relacionadas con las computadoras es en el marco del derecho de autor".[166]

En este entendido, cabe destacar que el mismo tratamiento que le han conferido esos acuerdos internacionales a las conductas antijurídicas antes mencionadas, es otorgado por la Ley Federal del Derecho de Autor que a continuación se analiza.

3.11. CODIGO PENAL DEL ESTADO DE SINALOA.

El único estado de la República que contempla en su legislación los delitos informáticos es el Estado de Sinaloa. Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos informáticos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

[166] Tratado de Libre Comercio (TLC) Parte 3, Diario Oficial de la Federación, Lunes 20 de Diciembre de 1993

Título Décimo. "Delitos contra el Patrimonio"

Capítulo V. Delito Informático.

Artículo 217.- Comete delito informático, la persona que dolosamente y sin derecho:

"1.- Use o entre a una base de datos, sistemas de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistemas o red. Al responsable del delito informático se le impondrá una pena de seis meses a dos años de prisión o de noventa a trescientos días de multa". [167]

En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado. Consideramos que se ubicó el delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícito, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad.

Por lo anterior, es necesario que en nuestro Estado, también exista una conciencia sobre la necesidad de legislar en este aspecto, creando el tipo penal adecuado a estas conductas antisociales, lo cual sería, un freno eficaz para su comisión.

Tal vez porque aún no se han visto en gran escala los estragos que pueden ocasionar estos tipos de conductas, y porque mucha gente aún no se ha incorporado

[167] CÓDIGO PENAL DEL ESATDO DE SINALOA

al mundo de la telecomunicación, nuestros legisladores se han quedado al margen en cuanto a este aspecto.

3.12 LEY FEDERAL DE DERECHOS DE AUTOR Y CODIGO PENAL FEDERAL.

"Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997". [168]

Esta ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos. Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.

Entendemos que la redacción de la fracción limita su aplicación, por 10 que en el Capítulo IV del presente trabajo, referido a la Propuesta que hacemos sobre el tratamiento de esta problemática en México, sugerimos una nueva redacción para la fracción IV del citado Código Penal, teniendo en cuenta la trascendencia negativa de esta conducta ilícita que amerita un tratamiento más fuerte que el administrativo.

Por otra parte, el artículo 104 de dicha ley se refiere a la facultad del titular de los derechos de autor sobre un programa de computación o sobre una base de datos, de conservar aún después de la venta de ejemplares de los mismos el derecho de autorizar o prohibir el arrendamiento de dichos programas.

---

[168] TELLEZ Valdes, op cit, p. 276

Por su parte, el Artículo 231, fracción II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por esta Ley" y "Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular.

Según nuestra opinión, la redacción de estas fracciones trata de evitar la llamada piratería de programas en el área del comercio, permite la regulación administrativa de este tipo de conducta, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, al igual que las infracciones contempladas para los programas de virus.

Además, la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su artículo 215 al Título Vigésimo Sexto del Código Penal citado, donde se sanciona con multa de 300 a 3 mil días o pena de prisión de seis meses hasta seis años al que incurra en este tipo de delitos. Sin embargo, la regulación existente no ha llegado a contemplar el delito informático como tal, sino que se ha concretado a la protección de los derechos autorales y de propiedad industrial, principalmente.

En este entendido, consideramos que por la gravedad de la conducta ilícita en sí, y por las implicaciones que traería aparejadas, está totalmente justificada su regulación penal.

En otro orden, el Artículo 109 de la Ley citada, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información.

Así, al acceso no autorizado a una base de datos de carácter personal de un Hospital de enfermos de SIDA puede ser utilizado contra estas personas quienes a causa de su enfermedad, se encuentran marginados socialmente, en la mayoría de los casos.

Asimismo, consideramos que la protección a este tipo de bases de datos es necesaria en virtud de que la información contenida en ellas, puede contener datos de carácter sensible, como son los de las creencias religiosas o la filiación política.

Adicionalmente pueden ser susceptibles de chantaje, los clientes de determinadas instituciones de créditos que posean grandes sumas de dinero, en fin, la regulación de la protección de la intimidad personal es un aspecto de suma importancia que se encuentra regulado en este artículo.

Esta Ley, además establece en el Título X, en su capítulo único, artículo 208, que el Instituto Nacional del Derecho de Autor es la autoridad administrativa en materia de derechos de autor y derechos conexos, quien tiene entre otras funciones, proteger y fomentar el derecho de autor además de que está facultad para realizar investigaciones respecto de presuntas infracciones administrativas e imponer las sanciones correspondientes.

Por otra parte, debe mencionarse que en abril de 1997 se presentó una reforma a la fracción III del artículo 231 de la Ley Federal del Derecho de Autor así como a la fracción III del artículo 424 del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal.

De esta forma, las modificaciones a la ley autoral permitieron incluir en su enunciado la expresión "fonogramas, videogramas o libros", además del verbo "reproducir".

Para quedar de la siguiente manera:

"Art. 231

...

...

III. Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta Ley".[169]

Con las reformas al Código Penal se especifica que:

"Art. 424

III. A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende, copias de obras, fonogramas, videogramas o libros protegidas por la Ley Federal al del Derecho de Autor en forma dolosa, a escala comercial y sin autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos".

Sobre el particular, debe mencionarse que durante la modificación a la Ley en diciembre de 1996 se contempló parcialmente lo que se había acordado en el TLC y que por tal razón fue necesaria una segunda modificación, en abril del año en curso para incluir la acción de "reproducción".[170]

De igual forma el artículo 424 que habia sufrido una modificación en diciembre de 1996, fue reformado en su fracción tercera en abril pasado para incluir la reproducción y su comisión en una forma dolosa.

[169] LEY DE DERECHOS DE AUTOR, ED. PORRUA.
[170] Código Penal FGederal, p. 182.

Sobre el particular, y por considerar de interés el contenido de la exposición de motivos cuando esta ley se presentó ante la Cámara de Diputados, a continuación se presentan algunos comentarios pertinentes respecto a los elementos que deben contemplarse en la atención a la problemática de los derechos de autor en nuestro país.

De esta forma, cuando se inició la iniciativa correspondiente, se dijo que la importancia de pronunciarse al respecto era que con dicha iniciativa se atendía la complejidad que el tema de los derechos autorales había presentado en los últimos tiempos lo cual exigía una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión.

Además, se consideró que debido a que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de Derecho de Reforma al Código Penal para el Distrito Federal en materia de Fuero Federal, proponiendo la adición de un título Vigésimo Sector denominado "De los delitos en materia de derechos de autor".

Al respecto, se consideró conveniente la inclusión de la materia en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas y por otro en un instrumento más adecuado para la procuración y la administración de justicia, al poderse disponer en la investigación de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.[171]

En este orden, como se menciono anteriormente, que esta ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos. Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del

[171] Exposición de motivos de la Comisión de justicia de la Cámara de Diputados Doc. 184/LVI/96 (I P.O. Año III) DICT, durante analisis de la Ley Federal de Derechos de Autor

acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia, de derecho de autor deben ser aplicadas cuan ocurren ilícitos relacionados con los citados programas y las bases de datos.

Apreciamos que aún cuando la infracción se circunscribe al área del comercio, permite la regulación administrativa de este tipo de conductas ilícitas, como una posibilidad de agotar la vía administrativa antes de acudir a la penal.

CAPITULO IV.

4.1 Concepto de los delitos informáticos.

4.2 Sujeto activo

4.3 Sujeto pasivo

4.4 Principales características

4.5 Conductas ilegitimas más comunes de los delitos Informáticos.

4.6 Tipo delitos informáticos.

4.7 Conductas que se cometen a través de la computadora y del Internet, tradicionalmente denominados "delitos informáticos".

4.8 Casos verídicos

4.9 Estadísticas sobre los delitos informáticos.

CAPITULO IV

4.1 CONCEPTOS DE DELITOS INFORMATICOS.

Como se señaló, es indispensable el uso de la computadora y del manejo del Internet, para la comisión de conductas delictivas denominadas "Delitos Informáticos", sin embargo, aún en la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe una concepto propio de los llamados delitos informáticos. Aún cuando no existe dicha definición con carácter universal, se han formulado conceptos funcionales atendiendo a las realidades concretas de cada país. Por lo que se refiere a nuestro país, cabe destacar lo mencionado por Julio Téllez Valdes, al decir que hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, requiere que la expresión "delitos informáticos" esté consignada en los Códigos Penales, lo cual en México, al igual que en otros muchos no ha sido objeto de tipificación aún.

Mencionando algunas de las diferentes definiciones que nos aportan estudiosos en la materia, sobre los Delitos Informáticos, diremos que para: Carlos Zarzaza, en su obra Criminalista y tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".[172]

Para Hilda Callegari, el delito informático es "aquel que se da con la ayuda de la informática o de técnicas anexas".[173]

Rafael Fernández Calvo, define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título I de la Constitución Española".[174]

---

[172] SARZANA, Carlos, CRIMINALIDAD Y TERNOLOGIA, Roma, Italia, p.53.
[173] CALLEGARI, Lidia, DELITOS INFORMÁTICOS Y LEGISLACIÓN", Revista de la facultad de derecho Medellin, Colombia,1985 p.115.
[174] FERNÁNDEZ, Calvo, Rfael, EL TRATAMIENTO DEL LLAMADO DELITO INFORMÁTICO. P.1150

María de la Luz Lima, dice que el "delito informático en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea con método, medio o fin".[175]

El doctor Julio Téllez Valdez, menciona dos clasificaciones del Delito Informático para efectos de conceptualización, que parte de lo típico y lo atípico. En el cual en el concepto típico de Delitos Informáticos nos dice que "son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin". En el concepto atípico menciona que "son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin".[176]

El Departamento de Investigación de la Universidad de México, señala como delitos informáticos a "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático".

Así pues, y realizando una definición personal sobre los delitos informáticos, diremos que: "son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal y que en su realización se valen de las computadoras como medio o fin para su comisión".

4.2 EL SUJETO ACTIVO.

Las personas que cometen los "Delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes.

Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación labora 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.

---

[175] LIMA DE LA LUZ, María. DELITOS ELECTRONICOS. En Criminalia. México, Academia Mexicana de Ciencias Penales, Editorial Porrua 1984. 100 p.
[176] Téllez, op.cit.p.104-105

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 cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

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

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

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios entre otros".

Asimismo, este criminológico estadounidense dice que tanto la definición de los "delitos informáticos" como las de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete.

Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Hay dificultad para elaborar estadísticas sobre ambos tipos de delitos.

La "cifra negra" es muy alta; hay dificultades para descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables" otra coincidencia que tiene estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad". [177]

Por nuestra parte, consideramos que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo, que dada la naturaleza de nuestro objeto de estudio nos vemos en la necesidad de limitar.

EL SUJETO PASIVO O VÍCTIMA

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

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

[177] TELLEZ Valdes, Julio. **Derecho Informático**. 2a. ed. México. Ed. Mc Graw Hill 1996. Pp. 103-104

acciones antes mencionadas, debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

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

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

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración e impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.[178]

4.4 LAS PRINCIPALES CARACTERÍSTICAS

Julio Téllez Valdés clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio y como fin u objetivo.

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

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

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

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

d) Lectura, sustracción o copiado de información confidencial.

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

f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

[178] TELLEZ Valdés, Julio. **Derecho Informático.** 2a. ed. México: Ed. Mc Graw Hill 1996. Pp. 103-104

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

h) Uso no autorizado de programas de cómputo.

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

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

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

l) Acceso a áreas informatizadas en forma no autorizada.

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

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

Como por ejemplo de lo anterior:

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

b) Destrucción de programas por cualquier método.

c) Daño a los dispositivos de almacenamiento.

d) Atentado físico contra la máquina o sus accesorios.

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

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)". [179]

María de la Luz Lima, presenta una clasificación, de lo que ella llama "delitos electrónicos", diciendo que existen tres categorías, a saber:

a) "Los que utilizan la tecnología electrónica como método: conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

b) Los que utilizan la tecnología electrónica como medio: conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

c) Los que utilizan la tecnología electrónica como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla". [180]

En lo que se refiere a delitos informáticos, Olivier Hance en su libro Leyes y Negocios en Internet, considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

---

[179] TELLEZ Valdes, Julio. DERECHO INFORMÁTICO. segunda edición, Mexico, Editorial De Mc Gram Hill, 1996, p.105.
[180] LIMA DE LA LUZ, María. DELITOS ELECTRONICOS. En Criminalia. México, Academia Mexicana de Ciencias Penales, Editorial Porrúa 1984, 221 p.

a) "Acceso no autorizado: es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.

b) Actos dañinos o circulación de material dañino: una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).

c) Interceptación no autorizada: en este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él.

d) Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado estos tres tipos de comportamiento ilícito cometidos a través de las computadoras". [181]

Por lo anterior, se puede apreciar que los que cometen este tipo de ilícitos, son personas con conocimientos sobre la informática y cibernética, los cuales, se encuentran en lugares estratégicos o con facilidad para poder acceder a información de carácter delicado, como puede ser a instituciones crediticias o del gobierno, empresas o personas en lo particular, dañando en la mayoría de los casos el patrimonio de la víctima, la cual, por la falta de una ley aplicable al caso concreto, no es denunciada quedando impune estos tipos de conductas antisociales; siendo esto alarmante, pues como se mencionó en líneas precedentes este tipo de acciones tienden a proliferar y ser más comunes, por lo que se pretende en la presente

[181] OLIVIER Hance LEYES DE NEGOCIACIÓN EN INTERNET.

investigación, es crear una conciencia sobre la necesidad urgente de regular estas conductas, ya que debe ser legislado de una manera seria y honesta, recurriendo a las diferentes personalidades del 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.

Después de ubicar las características que tienen el tipo de delitos informáticos así como sus sujetos y víctimas, se entrará al estudio de su Clasificación:

"La mayoría de los estudiosos en la materia clasifican a este tipo de acciones de dos formas, como instrumento o medio y como fin u objeto.

Aún así autores como Sarzana mencionan que estos ilícitos pueden clasificarse en atención a que producen un provecho para el autor y provocan un daño contra la computadora como entidad física y que procuren un daño a un individuo o grupos, en su integridad física, honor o patrimonio".[182]

Por otra parte, Davara Rodríguez, considera que "hay que distinguir el medio y el fin, para poder encuadrar una acción dolosa dentro de este tipo de delitos, el medio por el que se comete debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática, y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito; una finalidad deseada que causa un perjuicio a otro, a un tercero".[183]

[182] SARZANA, Carlos, CRIMINALIDAD Y TERNOLOGIA, Roma, Italia, p.53
[183] DAVARA Rodríguez, Miguel angel. DERECHO INFORMATICO. México. Editorial Aranzadi, 1993. P. 320

4.5 CONDUCTAS ILEGITIMAS MÁS COMUNES:

A) **HACKER**: Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas.

El término de hacker en castellano significa "cortador".

Las incursiones de los piratas son muy diferentes y responden a motivaciones dispares, desde el lucro económico a la simple diversión. Los "Hackers", son fanáticos de la informática, generalmente jóvenes, que tan sólo con un ordenador personal, un modem, gran paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, saltándose todas las medidas de seguridad, y leer información, copiarla, modificarla, preparando las condiciones idóneas para realizar un fraude, o bien destruirla. Se pueden considerar que hay dos tipos;

1) los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad;

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

B) CRACKER: Para las acciones nocivas existe la más contundente expresión, "Cracker" o "rompedor", sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender; es decir, presenta dos vertientes, el que se cuela en un sistema informático y roba información o produce destrozos en el mismo, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia.

C) PHREAKER: Es el que hace una actividad parecida a la anterior, aunque ésta se realiza mediante líneas telefónicas y con y/o sin el auxilio de un equipo de cómputo. Es el especialista en telefonía, empleando sus conocimientos para poder utilizar las telecomunicaciones gratuitamente.

D) VIRUCKER: Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o inutilizar la información contenida. Existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

E) PIRATA INFORMATICO: Es quien reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor.

4.6 TIPOS DE DELITOS INFORMÁTICOS.

1. MANIPULACIÓN DESDE UNA COMPUTADORA A UN SISTEMA DE PROCESAMIENTO DE DATOS.

Incluye comportamientos que registren cambio de datos o informaciones con la finalidad de obtener un beneficio económico, generalmente datos que representan activos, como por ejemplo depósitos de dinero, acreditaciones, créditos, o más bien relacionados a objetos físicos como por ejemplo la información sobre manejos de inventario.

Su perpetración aumenta cuando "se utilizan en mayor medida los llamados "cajeros automáticos" o los POS, que quiere decir puntos de venta".[184]

2. ESPIAR, FISGONEAR Y ROBAR DE SOFTWARE.

Están relacionados a la obtención de información de investigaciones, direcciones de clientes, proveedores, copiando programas y métodos para posteriormente ser entregadas a la competencia.

La radiación electrónica que emite una terminal de computadora puede ser captada y registrada sin mayor complicación desde cerca de un kilómetro del lugar de su instalación.

3. SABOTAJE INFORMÁTICO.

"Se refieren principalmente a la destrucción de datos y programas e inclusive de los equipos informáticos, así como la posibilidad de causar costos circuitos".[185]

4. ROBO DE SERVICIOS.

Se produce generalmente cuando los empleados o dependientes utilizan sin autorización alguna las máquinas del empleador, para realizar trabajos para terceros o para beneficio particular.

---

[184] DAVARA Rodríguez, Miguel angel. DERECHO INFORMATICO. México. Editorial Aranzadi, 1993. P. 323
[185] DAVARA OP CIT. P. 325

Según Tiedemann este es uno de los supuestos que requiere tipo penal específico.

5. ACCESO NO AUTORIZADO A SISTEMAS DE PROCESAMIENTO DE DATOS.

"Se produce cuando se entre a una base de datos ajena ya sea para obtención de información, destrucción de la misma, alterar por vía de artificio con el objeto de obtener dinero, bienes o información". [186]

De la misma forma también se incluye la modalidad que intercepta o interfiere alguna comunicación en la red de computadoras.

6. DEFRAUDACIÓN EN LOS NEGOCIOS ASISTIDOS POR UN COMPUTADOR.

"Se refiere al uso de computador para defraudar o desenmascarar acciones claramente punibles, como por ejemplo datos contables, planilla de sueldo de maestros, alteración o existencia o stock, etc". [187]

Las diferentes formas que pueda adoptar el delito informático son de tal dimensión que para un profano prácticamente serian inimaginables limitados quizás únicamente por la astucia del autor, su capacidad técnica y las deficiencias de control existentes en la instalación invadida.

Para darmos una idea del ámbito del problema conozcamos las diversas formas en las que el delito informático puede producirse sin que ello suponga de ninguna manera que estamos ante una lista cerrada sino tan sólo de una relación enumerativa de las situaciones más frecuentes.

---

186 DAVARA OP CIT, P.324
187 DAVARA OP CIT, P.325.

7. INTRODUCCIÓN DE DATOS FALSOS O DATA DIDDLING

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

Un antecedente muy publicitado es el Caso Blair, conocido por un delito cometido en Maryland en mayo de 1980. Janeth Blair, empleada de las oficinas de seguridad social, ingresaba desde su terminal informática, que se encontraba conectado con un computador central, transacciones falsas para producir la emisión de cheques fraudulentos, consiguiendo por este procedimiento apropiarse de cerca de Ciento Doce mil Dólares. Este delito fue descubierto de manera casual por el empleado del banco a cuyo nombre eran girados los cheques quien sospechó al verificar la existencia de gran cantidad de cheques con el mismo número de afiliación a la seguridad social pero expedido a diferentes titulares.

La Sra. Janeth Blair fue acusada de 43 cargos de falsificación y desfalco.

8. EL CABALLO DE TROYA O " TROJAN HORSE"

Inspirado en las épicas hazañas contadas por Homero en su obra "La Ilíada" que narra la toma de la Ciudad de Troya. Ulises mandó construir un enorme caballo de madera vacío el cual obsequió a los troyanos en señal de paz, sin embargo, en su interior ocultaba gran cantidad de soldados y pertrechos militares de la época, los cuales permanecieron ocultos hasta que se diera la orden a fin de sitiar la ciudad.

Los habitantes de Troya al creer que habían ganado la guerra, introdujeron el caballo en la ciudad y celebraron el triunfo con una gran fiesta, pero durante la noche, cuando todos dormían confiados y bajo los efectos del alcohol, los soldados de Ulises salieron del caballo y abrieron las puertas de la ciudad ingresando los

soldados enemigos tomando la ciudad sin que los troyanos opusieran mayor resistencia.

Por esta razón, la denominación "Caballo de Troya" se aplica a algo que en apariencia es inofensivo para tranquilidad de la víctima, pero cuando desencadena su dañino potencial causa verdaderos estragos.

Luego de esta breve referencia mitológica que nos explica la razón de su nombre podemos precisar que este método consiste en la inclusión de instrucciones dentro del programa de uso habitual una rutina para que realice un conjunto de funciones desde luego, no autorizadas, para que dicho programa ejecute en ciertos casos de una forma distinta a como estaba previsto.

Puede tratarse en determinados casos de la ejecución de cálculos erróneos por ejemplo aumentando el importe de la lista de un empleado, desviando ingresos hacia cuentas ficticias, etc. También puede presentarse cuando se imprimen documentos no autorizados o inclusive no imprimir documentos reales, por ejemplo emitir cheques a proveedores fantasmas o no imprimir cheques a proveedores reales cuando previamente se les ha cancelado su deuda, ya que se ha alterado la forma de pago transfiriendo los fondos a una cuenta que pertenece al defraudador.

"Un procedimiento usualmente utilizado en la banca es por ejemplo introducir una modificación al programa del tratamiento de cuentas corrientes para que siempre que se consulte un saldo lo multiplique por diez, por cien, por mil, por cien mil etc. con lo que es posible autorizar pagos, transferencias superiores a lo real"[188].

Por sus características es necesario poseer una capacidad técnica suficiente al menos saber programar y además tener acceso al programa para poder manipularlo.

Es importante agregar que en todo este tipo de ilícitos el programa manipulado ha estado en funcionamiento habitual desde hace un buen tiempo y casi nunca se trataba de programa de nueva creación.

---

188 DAVARA Rodríguez, Miguel Angel. DERECHO INFORMATICO. México. Editorial Aranzadi, 1993, P. 323

El motivo es muy simple, los programas nuevos suelen ser sometidos a procesos de revisión y chequeo para detectar cualquier anomalía que puedan afectarlos. Sin embargo un programa que ha estado en funcionamiento correctamente durante un prolongado tiempo no se cuestiona, y salvo casos absolutamente excepcionales, jamás sus resultados son sometidos a comprobación.

Debido a ello la modalidad de Caballo de Troya es una de las más peligrosas y al mismo tiempo difíciles de detectar.

Un ejemplo claro de este método es un caso real sucedido en una entidad de crédito al cual no se le dio publicidad y del que se desconoce incluso el nombre del autor.

Este caso ocurrió a fines de 1984 y el procedimiento utilizado por el autor, aparentemente un ex empleado de centro de cómputo de la entidad, fue el introducir una rutina en el programa de tratamiento de cuentas corrientes para que un determinado día, aproximadamente seis meses después de haber dejado su trabajo, y a una hora nocturna predeterminada se autorizase el pago a un talón de una cuenta corriente sin consultar el saldo.

Posteriormente la misma rutina borraba parte del programa modificado con lo cual se eliminaba el rastro de la comisión del delito.

Otro caso similar en sucedió en 1985 en una importante entidad bancaria cuando en una oportunidad tres personas, supuestamente antiguos empleados de la institución, manipularon el sistema informático abriendo dos cuentas en diferentes oficinas de la ciudad con nombres distintos y falsos, lo que les permitió disponer de talonarios de cheques al mismo tiempo que las cuentas ingresaran al sistema del banco.

Pues bien, después de unos días de funcionamiento normal y sin que se haya explicación alguna, en las cuentas se hicieron asientos falsos por un total de 24 millones de dólares.

"Los malos elementos fueron detenidos al ser descubiertos después de haber cobrado cinco cheques y en posesión de documentos falsos que identificaban a las personas en cuyo nombre estaban abiertas las cuentas".[189]

9. EL SALAME, REDONDEO DE CUENTAS O" ROUNDING DOWN".

Es tal vez la técnica más sencilla de realizar y la que menos probabilidades tiene de ser descubierta.

"La modalidad consiste en introducir o modificar unas pocas instrucciones de los programas para reducir sistemáticamente una cantidad transfiriéndola a una cuenta distinta o proveedor ficticio que se abre con nombre supuesto y que obviamente la controla el defraudador".[190]

Por ejemplo puede darse el caso de disminuir constantemente en unos céntimos las cuentas corrientes de un cliente bancario, pequeños saldos de proveedores, reducir los talones de impresión para el pago a acreedores, transfiriendo luego estas pequeñas cantidades a la cuenta particular del autor.

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

La razón principal por la que es tan difícil descubrir este tipo de hechos es porque las cuentas o el importe total del listado, siguen estando "cuadrados" por lo que no se deduce ninguna señal de alarma que pueda indicar lo que está sucediendo.

---

[189] TELLEZ Valdes, Julio. DERECHO INFORMÁTICO, segunda edición, México, Editorial De Mc Graw Hill, 1996, 105 p.
[190] DAVARA Rodríguez, Miguel angel. DERECHO INFORMATICO. México, Editorial Aranzadi, 1993, P.323.

Por ejemplo se da el caso al redondear cuentas bancarias y acreditar los montos resultantes a una cuenta determinada repitiendo automáticamente la operación sin intervención posterior del autor.

Un caso real se dio en los Estados Unidos donde un programador tenía bajo su responsabilidad el sistema mecanizado de personal en el cual introdujo pequeñas modificaciones en los cálculos del plan de inversiones corporativas. La empresa había acordado con sus trabajadores que les retendría una pequeña cantidad de sus salarios para invertirlos en valores. Lo que realizó el programador fue retirar pequeñas cantidades de lo descontado cada empleado para transferirlo a su propia cuenta.

10. USO INDEBIDO DE PROGRAMAS O "SUPERZAPPING"

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

"El nombre proviene de un programa llamado usuperzap" y es una especie de llave que permite abrir cualquier rincón de una computadora por más protegida que pueda estar".[191]

Estos programas pertenecen al grupo de los llamados" Programas de Acceso Universal" de uso imprescindible en cualquier instalación de ciertas dimensiones cuando fallan los procedimientos normales para recuperar o reiniciar "el sistema",

Efectivamente, cuando un sistema informático almacena gran cantidad de información se hace necesario disponer de un mecanismo de emergencia que permita entrar a cualquier punto del sistema en caso que se produzca alguna avería o lo que normalmente se ha denominado "caída del sistema".

[191] DAVARA Rodríguez, Miguel angel. DERECHO INFORMATICO. Mexico. Editorial Aranzadi, 1993, P.323.

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

Los programas de utilidad son una herramienta valiosa y muchas veces imprescindible en los casos de caída del sistema pero igualmente un arma peligrosísima cuando se encuentra al alcance de personas que lo utilizarán con otras intenciones.

No es necesario insistir que su acceso debe ser restringido y con adecuados controles.

No obstante suelen estar archivados en las librerías de producción junto con el resto de programas de uso común y generalizado, con lo cual cualquier técnico podría tener la posibilidad de utilizarlo indebidamente.

Con la modalidad de superzaping es posible alterar los registros de un fichero sin que quede constancia de tal modificación lo cual hace sumamente difícil descubrir y detectar el autor de tales eventos.

Aparentemente se suelen registrar los ingresos a une sistema y las transacciones que se han procesado en una determinada operación actualizando los registros con un dato específico como por ejemplo la hora de ingreso.

Sin embargo los programas de acceso universal permiten modificar directamente la información sin activar los programas de actualización ni introducir ninguna operación al computador. Aún más, sin dejar rastro si la persona que lo está usando sabe como realizarlo.

Bastaría con hacer coincidir el momento de la modificación no autorizada con el comienzo o el final de la ejecución del programa verdadero de actualización y algún error intencionado en el sistema que requiera la utilización del programa de acceso universal.

En ese preciso momento tendremos cargado en el sistema el fichero que queremos modificar y el programa que nos permite modificar no registrándose por lo tanto su utilización no justificada ni del fichero, ni del programa de utilidad.

"Cuando se descubran las alteraciones de los datos se pensará que ha sido un funcionamiento erróneo del programa de actualización, un funcionamiento inadecuado del computador o una transacción errónea y en esas direcciones se encaminará la investigación las cuales seguramente no abordarán a ningún puerto".[192]

En el mejor de los casos si se descubre como se realizó la alteración de datos será muy difícil probarlo.

Un conocido caso con el método del superzaping ocurrió New Jersey en donde el autor comenzó a desviar fondos desde las cuentas de diferentes clientes hacia la de unos amigos sin que quedara en el sistema ninguna evidencia de las modificaciones efectuadas en los saldos de cuenta corriente.

El delito se descubrió por los reclamos efectuados por uno de los afectados lo cual motivó una investigación que culminó con la detención del sujeto.

11. PUERTAS FALSAS o "TRAPS DOORS"

Es una costumbre en el desarrollo de aplicaciones complejas que los programas permitan introducir interrupciones en la lógica de los desarrollos del mismo, con el objeto de chequear por medio de los procesos informáticos si los resultados intermedios son correctos, producir salidas de emergencia y de control a fin de guardar resultados parciales en ciertas áreas del sistema para comprobarlos después.

Inclusive algunas veces este procedimiento se enlaza con rutinas del sistema operativo para facilitar una "puerta de entrada al programa" que no estaba prevista, pero de esta manera facilitan la labor de desarrollo y prueba de programas.

---

192 DAVARA Rodriguez, Miguel angel. DERECHO INFORMATICO. México. Editorial Aranzadi, 1993, P. 323.

"El problema radica en tener la seguridad de que cuando los programas entran en proceso de producción normal todas esas "puertas falsas" hayan desaparecido, y aunque parezca mentira, las puertas creadas no se eliminan, permitiendo a su paso puertas de acceso al programa con el agravante que por ser elementos temporales creados por la computadora no constan en la documentación del sistema".[193]

Es de uso frecuente para posibles recuperaciones en caso de "Caída del Sistema" a mitad de un proceso ir grabando en cinta resultados intermedios o copia de las transacciones procesadas, o incluso ciertas áreas de memoria para la recuperación más rápida y sencilla.

Las puertas falsas se realizan por personas que no las crearon, pero que una vez descubiertas se aprovechan de ella. Sin necesidad de poseer una formación informática profunda.

Tal es el caso de unos ingenieros en una fábrica de automóviles en Detroit que descubrieron una puerta falsa en una red de servicio publico de time- sharing de Florida.

Después de una serie de intentos consiguieron ingresar con una llave de ingreso de alto nivel, según parece la del propio presidente ejecutivo de la compañía y utilizándola pudieron apoderarse de diferentes programas clasificados de carácter reservado y archivados en el computador bajo la denominación de secreto comerciales, al mismo tiempo que utilizaban la red sin cargo económico alguno.

12. BOMBAS LÓGICAS O" LOGIC BOMBS".

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

---

[193] [illegible]

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

Un conocido caso de bomba lógica se presentó en setiembre de 1981 y tuvo como protagonista un programador de computadoras de 26 años de edad que trabajaba para el departamento de defensa en Washington D. C. en los Estados Unidos de Norteamérica.

Resulta que el programador se sintió frustrado y discriminado al no recibir una promoción que supuestamente le correspondía, por lo que decidió vengarse. El trabajo de este empleado consistía en el mantenimiento de las nóminas del sistema de personal lo que le permitía tener acceso a todos los programas y a la información contenida en la base de datos de dicho sistema.

Decidido a vengarse escribió unas rutinas para incluir en los programas que a cierta señal se borren y destruyan gran parte de la información que él procesaba en los sistemas.

Posteriormente comenzó a buscar otro trabajo para lo cual solicitó vacaciones en su empleo siendo así que consiguió un nuevo trabajo.

Unos días después que recibió la confirmación de su nuevo empleo, y en ese mismo momento aprovechando la hora del almuerzo, introdujo la rutina que tenía programada, incluyendo un control que se activaría seis meses desde la fecha de su salida de su anterior empleo.

En efecto, seis meses después de haber abandonado a su anterior trabajo cuando se estaban procesando las nóminas de personal la rutina introducida por él funcionó como había previsto su autor, borrando la mayor parte de información de los registros de personal.

Dada que el programa había estado funcionando largo tiempo y nadie dudaba de su funcionamiento se volvieron a probar con las copias de seguridad las que también resultaron dañadas.

El descubrir el motivo de los daños al sistema y recomponer la información requirió gran esfuerzo de personal y de tiempo lo que puede dar una idea del costo que se supuso, pero no fue posible probar la autoría del hecho, aunque las sospechas recayeron sobre su verdadero autor, el que nunca fue acusado formalmente ni juzgado ni castigado.

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

Consiste en programar una instrucción que revisa la fecha del dia, lo que permite una fecha de caducidad oculta que ha introducido el fabricante del software al instalarlo en el computador del cliente y que no será eliminada o prorrogada hasta que el cliente pague los nuevos derechos. Esto constituye una verdadera forma de coacción ilegal pero que es utilizada por una falta de protección adecuada de sus derechos de autor.

13. ATAQUES ASINCRONICOS O "ASYNCHRONIC ATTACKS"

Los sistemas informáticos en la mayoría de casos funcionan ejecutando más de dos comandos u órdenes a la vez o en otras circunstancias una instrucción sucesiva de la otra en forma secuencial.

Cabe recordar que el sistema operativo es el conjunto de programas que controlan el funcionamiento del computador y todos sus dispositivos periféricos (discos, cintas, impresoras), la entrada de los datos procesados por el programa, la ejecución de los programas de las diferentes aplicaciones y la salida de la información elaborada hacia los dispositivos exteriores.

El sistema operativo es imprescindible para el funcionamiento del equipo y su desarrollo es responsabilidad del fabricante.

Una de las principales funciones del sistema operativo de las computadoras es controlar la ejecución simultánea de varios programas a la vez.

Otra función fundamental del sistema operativo es optimizar la ocupación de memoria central reasignando áreas en función de las necesidades de cada uno de los programas que están ejecutando en cada momento.

De otro lado el sistema operativo asigna a los programas otras funciones de clasificación, intercambio, etc.

Por lo tanto el sistema operativo es quien controla y maneja todos los errores que pueden producirse tanto en la computadora como en los programas que se están ejecutando, avisando al operador por medio de mensajes de cualquier situación anormal que se produzca.

Pues bien, los programas funcionan en forma sincrónica, es decir, ejecutando sus instrucciones en un orden fijo predeterminado de nivel en nivel, en tanto que el sistema operativo funciona en forma asincrónica es decir ejecutando sus órdenes de manera independiente, en función de una gran cantidad de factores ajenos a él.

Esto produce rigurosidad en los programas en ejecución conformando las llamadas "Colas de Espera" que se van a ir desbloqueando en función de la disponibilidad de los datos o comandos que estaban esperando.

Uno de los típicos casos en el que puede producirse es en los llamados puntos de recuperación del sistema.

Cuando se procesan programas complejos y de larga duración se establecen puntos de recuperación cada cinco o diez minutos por ejemplo gravando en soporte magnético externo (diskettes) el estado del programa, lo que implica que si el sistema "SE CAE ", es decir, que se interrumpa el proceso por una situación de error no recuperable, por ejemplo falta de energía eléctrica no es necesario retroceder desde el principio del programa sino bastará hacerlo desde el último punto de recuperación ya que todo se encuentra grabado, reiniciando de esta manera el proceso.

Pues bien, si entre dos puntos de recuperación se provoca voluntariamente una "caída del sistema" y en el intermedio se manipula los parámetros en que se va a apoyar el sistema operativo para reiniciar resulta obvio que las condiciones en que se ejecuten serán distintas a las originales por lo que sus resultados serán por lo menos diferentes, fraudulentos o erróneos.

14. RECOJO DE INFORMACIÓN RESIDUAL O "SCA VENGING".

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

La denominación proviene del anglicismo "lo scavenge" que significa recoger la basura.

Simplemente se va aprovechando las finalizaciones de los trabajos reales en el computador para obtener la información residual que ha quedado en la memoria.

La modalidad más frecuente es la "Impresión Diferida" preparando la unidad para que posteriormente imprima sin ningún tipo de protección siendo fácilmente recuperable sin necesidad de utilizar ninguna clave de acceso.

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

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

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

Una de las formas más simples del scavenging electrónico es cuando se ordena la impresión diferida ya que en la computadora queda preparada la información que posteriormente se imprimirá sin ningún tipo de protección, siendo sumamente fácil recuperar la información sin la necesidad de utilizar ningún tipo de clave o cualquier procedimiento de seguridad.

El caso más célebre de scavening ocurrió en Los Ángeles por un estudiante de ingeniería eléctrica. El estudiante simultáneamente trabajaba como vendedor de equipos de comunicaciones lo cual le permitió adquirir un conocimiento bastante profundo de como operaban los sistemas mecanizados de la empresa.

Al haber recogido cada mañana los papeles que depositaban en el exterior del centro de procesamiento de datos de la compañía. El estudiante simulando ser un publicista convenció a los directivos de la empresa para lanzar un boletín que reforzaría considerablemente la imagen de la compañía. Esto le permitió recopilar información, añadida a la compra de una camioneta en una subasta de la propia compañía. El estudiante pidió telefónicamente mercadería para una empresa que había seleccionado previamente. Para ser despachada por la noche por la cantidad de 30 mil dólares, lo que hizo fue recoger la mercadería y distribuirla a diferentes compradores.

El estudiante fue descubierto al ser denunciado por su ayudante a quien se negó a aumentar el dinero que le pagaba por sus servicios especiales.

El estudiante fue acusado de varios delitos y el 5 de julio de 1972 fue condenado por el Juez M. Deal a dos meses en una correccional, 500 dólares de multa y tres años de libertad vigilada.

15. DIVULGACIÓN NO AUTORIZADA DE DA TOS O DA TA LEAKCAGE

Consiste en sustraer información confidencial almacenada en un computador central desde un punto remoto, accediendo a ella, recuperándola y finalmente enviándola a una unidad de computador personal, copiándola simultáneamente.

La sustracción de información confidencial es quizás uno de los cánceres que con mayor peligro acechan a los grandes sistemas informáticos.

Se ha empleado también bajo la denominación de espionaje industrial, pues sería particularmente débiles al sustraerse aspectos claves de su actividad empresarial, como por ejemplo estrategias de mercado, nuevos productos, fórmulas de producción, etc.

Inclusive hay cierto tipo de empresas que dependen de la privacidad de su información como las empresas de publicidad directa en donde tiene ficheros completos de su público objetivo.

16. ACCESO A AREAS NO AUTORIZADAS O PIGGYN BAKING

Pese a no tener una traducción específica consiste en acceder a áreas restringidas dentro de la computadora o de sus dispositivos periféricos como consecuencia de puertas abiertas o dispositivos desconectados.

Se da también cuando el usuario que está trabajando en un terminal en un nivel autorizado que le permite realizar ciertas funciones reservadas deja el terminal conectado, con lo que cualquier otra persona puede continuar trabajando sin necesidad de identificarse pudiendo efectuar operaciones que en condiciones normales no le estarían permitidas.

17. SUPLANTACION DE LA PERSONALIDAD

Puede ser entendida como la suplantación de personalidad fingiendo ser una persona que no es imitándola e inclusive remedándola.

Algunos sistemas requieren la identificación con una clave para acceder al sistema. Más adelante se ha requerido la posesión de algo pudiendo ser una llave o tarjeta magnética. Y aún podríamos complicarlo aun más si adicionamos dispositivos de reconocimiento biométrico como identificación con la palma de la mano o dactilográfica, scanners de retina o del iris, reconocimiento de voz, etc.

Un caso muy frecuente de Impersonation o suplantación de personalidad se da en el robo de las tarjetas de crédito y de cajeros automáticos.

Los autores del delito se hacen pasar por un empleado de la central de tarjetas de crédito, llamando telefónicamente al titular para solicitarle que con el objeto de anular la posibilidad de utilización fraudulenta de la tarjeta robada le revele su clave secreta o personal.

Como es fácil advertir, una vez descubierta la clave a la persona desconocida que las ha llamado utilizan la tarjeta para sacar el dinero de los cajeros automáticos hasta su límite máximo de crédito.

Otro caso célebre es el que hicieron los estudiantes de una universidad norteamericana al mandar una carta en papel oficial a todos los usuarios de computadoras de la universidad advirtiéndoles que el número de conexión al sistema había sido cambiado, solicitándoles su número anterior.

Posteriormente y debido a que lo primero pedía el sistema al conectarse era la clave de identificación, los estudiantes recogieron la clave e indicaron que hasta nueva orden volvieran a usar su número antiguo, obteniendo así el número clave de todos los usuarios del sistema, descubriendo todos los secretos de los estudiantes de la universidad.

Una vez descubierto el procedimiento todas las claves fuero cambiadas.

18. PINCHADO DE LíNEAS INFORMATICAS WIRETAPPING

Se trata de pinchar o interferir líneas de transmisión de datos y recuperar la información que circula en ellas, generalmente se produce en el mismo origen de la transmisión. No es necesario tener equipo sofisticado, sólo se requerirá un pequeño casete, una grabadora, una radio portátil AM-FM, un módem para demodular las señales telefónicas analógicas y convertirlas en digitales, y una pequeña impresora para listar la información que se hubiera captado. La forma de realizarlo depende del sujeto que lo ejecuta.

19. HURTO DE TIEMPO

Se da cuando los empleados utilizan sin autorización las horas de la máquina del empleador por ejemplo para realizar trabajos particulares hurtando el tiempo del computador o del servicio de procesamiento de datos y por tanto incrimina un uso no autorizado.

20. SIMULACIÓN E IMITACIÓN DE MODELOS O SIMULA TION AND MODELING.

Se trata del uso de la computadora para simular y planificar la comisión de un delito antes de realizarlo.

La utilización de la computadora se realiza de forma mediata para conseguir un fin ilícito como ejemplos podemos señalar desde la simulación del robo de una bóveda de un banco hasta el contador que contrató los servicios contables de una empresa para estudiar detenidamente las repercusiones de los asientos fraudulentos que pensaba realizar para sustraer una cantidad importante de dinero.

Aquí se difiere de los anteriores tipos de delitos informáticos pues el computador que puede ser usado para simular situaciones previsibles o efectuar modelos que representen el comportamiento previsible de una empresa, una fábrica, una inversión, es utilizado equivocadamente con fines delictivos.

No obstante lo mencionado consideramos que este tipo en particular por la finalidad distinta al uso normal de la computadora así como la escasez de los delitos cometidos por este método no sería recomendable su tipificación.

21. PIRATAS O "HACKERS".

Conocido también como "Pirateo Informático", consiste en entrar sin autorización a una computadora y explorar su interior.

No existe aparentemente límite pudiendo acceder por vía remota a servicios de noticias, servicios financieros, información financiera, instalaciones universitarias, correo electrónico, computadoras oficiales.

22. CRACKERS

Es el típico Hacker que no ingresa al sistema por curiosidad o porque le represente un reto para entender el funcionamiento de cualquier sistema. En realidad nos referimos a la persona que conscientemente ingresa a un sistema con la finalidad de destruir información.

Existen dos vertientes:

a) El que ingresa en un sistema informático y roba información produciendo destrozos en el mismo.

b) El que se dedica a desproteger todo tipo de programas, tanto para hacerlas plenamente operativas como para los programas que presentan anticopias.

23. PHREAKERS

Es el especialista en telefonía. Se le podría llamar el pirata de los teléfonos, sobre todo emplea sus conocimientos para poder utilizar las telecomunicaciones gratuitamente. Los principales perjudicados son los usuarios nacionales e internacionales y las compañías telefónicas.

Existen muchos software que hacen posible la comunicación por computadora a un teléfono como el "NetPhonof" creado por IOT Corporatíon que permite realizar llamadas internacionales desde una computadora personal a un teléfono fijo o celular a cualquier parte del mundo. El sistema se basa en la transmisión de la voz vía Internet.

El software o programa digitaliza la voz para que viaje a través de la red. Esta nueva modalidad de comunicarse por teléfono se ha desatado con fuerza en los países donde la tecnología se encuentra en mayor desarrollo esta posibilidad estará disponible en mayor volumen en la medida que la tecnología derivada se extienda a

otros, lo que permite comunicarse de una pe hacia un teléfono o de una pe hacia otra PC.

Los usuarios no necesitan coordinar con su interlocutor la hora y el día para estar en línea en el momento de la llamada. Quien efectúa la llamada sólo necesita una pe con conexión a Internet para comunicarse con otra persona.

24. LOS VIRUS

Son una serie de claves programáticas que pueden adherirse a otros programas, propagarse a otros sistemas informáticos. Un virus puede ingresar por una pieza de soporte lógico que se encuentre infectado desde una forma remota ingresando al programa.

25. GUSANOS

Se fabrica en forma análoga al virus con miras a infiltrarlo en programas normales de procesamiento de datos o para modificar o destruir la información, pero se diferencia del virus porque no puede regenerarse.

Si se asimilara a la medicina podría decirse que es una especie de tumor benigno. Ahora las consecuencias del ataque de un gusano pueden ser tan peligroso como el de un virus.

26. DELITOS DE CONNOTACIÓN SEXUAL POR INTERNET.

De la misma manera deben considerarse las conductas que ponen a disposición de menores de edad imágenes de contenido altamente sexual explícito y que ponen en riesgo su formación integral ocasionando trastornos en normal desenvolvimiento de su personalidad. Se debería controlar esto mediante el acceso a estas páginas web con doble clave. Así mismo evitar casos de prostitución infantil por esta vía.[194]

[194] DAVARA Rodriguez, Miguel angel. DERECHO INFORMATICO. México. Editorial Aranzadi, 1993, P.323-329.

4.7 CONDUCTAS QUE SE COMETEN A TRAVES DE LA COMPUTADORA Y DEL INTERNET, TRADICIONALMENTE DENOMINADOS "DELITOS INFORMATICOS".

A pesar de que el concepto de delito informático engloba tanto los delitos cometidos contra el sistema como los delitos cometidos mediante el uso de sistemas informáticos, en este apartado se hablará del delito informático como aquél que está íntimamente ligado a la informática, es decir, las conductas realizadas a través del mundo virtual del ciberespacio.

A) FRAUDE INFORMATICO.- El fraude informático solo está limitado por la imaginación del autor, su capacidad técnica y las medidas de seguridad de la instalación. Se pueden clasificar en cuatro grupos: 1.- Intervención en los datos de entrada al sistema; 2.- Incorporación de modificaciones no autorizadas en los programas; 3.- Modificación fraudulenta de la información almacenada en el sistema. 4.- Intervención en las líneas de transmisión de datos.

B) ACCESO NO AUTORIZADO.- El uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

C) DESTRUCCION DE DATOS.- Son daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático.-

D) INFRACCION DE LOS DERECHOS DE AUTOR.- Es la interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red.

E) INFRACCION DEL COPYRIGHT DE BASES DE DATOS.- Aún no existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet.

F) INTERCEPCION DE E-MAIL.- Constituye una violación de correspondencia, y la intercepción de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

G) ESTAFAS ELECTRONICAS.- La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra.

H) TRANSFERENCIA DE FONDOS.- Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático.- Como se puede observar, muchas de estas conductas no son irreales, es decir, las encontramos de una manera palpable, y cualquier persona que tenga conocimientos básicos de informática puede llegar a cometerlos.

4.8 CASOS VERIDICOS SOBRE DELITOS INFORMÁTICOS.

"Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de «Shadowhawk», fue el primer sentenciado bajo el cargo de Fraude Computacional y Abuso en 1986. Zinn tenia 16 y 17 cuando violo el acceso a AT&T y los sistemas del Departamento de Defensa.

Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US $174,000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publico contraseñas y instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US $10,000. Se estima que Zinn hubiera podido alcanzar una sentencia de 13 años de prisión y una fianza de US$800,000 si hubiera tenido 18 años en el momento del crimen".[195]

[195] http://WWW. Monografias.com/legisdelinf

"Smith, David, programador de 30 años, detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo, «Melissa». Entre los cargos presentados contra él, figuran el de «bloquear las comunicaciones publicas» y de «dañar los sistemas informáticos».

Acusaciones que en caso de demostrarse en el tribunal podrían acarrearle una pena de hasta diez años de cárcel".[196]

Por el momento y a la espera de la decisión que hubiese tomado el juez, David Smith esta en libertad bajo fianza de 10.000 dólares. Melissa en su «corta vida» había conseguido contaminar a más de 100,000 ordenadores de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas estadounidenses como la del Gobierno del Estado de Dakota del Norte y el Departamento del Tesoro.

En España su «éxito» fue menor al desarrollarse una extensa campaña de información, que alcanzo incluso a las cadenas televisivas, alertando a los usuarios de la existencia de este virus.

La detención de David Smith fue fruto de la colaboración entre los especialistas del FBI y de los técnicos del primer proveedor de servicios de conexión a Internet de los Estados Unidos, América On Une. Los ingenieros de América On Line colaboraron activamente en la investigación al descubrir que para propagar el virus, Smith había utilizado la identidad de un usuario de su servicio de acceso.

Además, como otros proveedores el impacto de Melissa había afectado de forma sustancial a buzones de una gran parte de sus catorce millones de usuarios.

Fue precisamente el modo de actuar de Melissa, que remite a los cincuenta primeros inscritos en la agenda de direcciones del cliente de correo electrónico «Outlook Express», centenares de documentos *«Office»* la clave para encontrar al

[196] http://WWW. Monografias.com/legisdelinf.

autor del virus. Los ingenieros rastrearon los primeros documentos que fueron emitidos por el creador del virus, buscando encontrar los signos de identidad que incorporan todos los documentos del programa informático de Microsoft *«Office»* y que en más de una ocasión han despertado la alarma de organizaciones en defensa de la privacidad de los usuarios. Una vez desmontado el puzzle de los documentos y encontradas las claves se consiguió localizar al creador de Melissa. Sin embargo, la detención de Smith no significa que el virus haya dejado de actuar.

Compañías informáticas siguen alertando que aún pueden quedar miles de usuarios expuestos a sus efectos, por desconocimiento o por no haber instalado en sus equipos sistemas antivíricos que frenen la actividad de Melissa u otros virus, que han venido apareciendo últimamente como Happy99 o Papa.

"Diciembre de 1992 Kevin Poulsen, un pirata infame que alguna vez utilizo el alias de «Dark Dante» en las redes de computadoras es acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana o Se acusa a Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y encara hasta 10 años en la cárcel".[197]

Siguió el mismo camino que Kevin Mitnick, pero es más conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a «ganar» un Porsche en un concurso radiofónico, si su llamada fuera la 102, Y así fue.

Poulsen también crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional.

Esto fue lo que lo llevó a su estancia en la cárcel, 5 años, fue liberado en 1996, supuestamente «reformado». Que dicho sea de paso, es el mayor tiempo de estancia en la cárcel que ha comparecido un hacker.

---

[197] http://WWW. Monografias.com/legisdelinf.

"Holland, Wau y Wenery, Steffen, de visita en la NASA «Las dos de la madrugada, Hannover, ciudad Alemana, estaba en silencio. La primavera llegaba a su fin, y dentro del cuarto cerrado el calor ahogaba. Hacía rato que Wau Holland y Steffen Wernery permanecían sentados frente a la pantalla de una computadora, casi inmóviles, inmersos en una nube de humo cambiando ideas en susurros. - Desde acá tenemos que poder llegar. -murmuró Wau. - Mse. Hay que averiguar cómo - contestó Steffen". [198]

Probemos algunos. Siempre eligen nombres relacionados con la astronomía, ¿No? - Tengo un mapa estelar: usémoslo. Con el libro sobre la mesa, teclearon uno a uno y por orden, los nombres de las diferentes constelaciones.

«Acceso Denegado» -leyó Wau-; maldición, tampoco es - Quizá nos esté faltando alguna indicación. Calma.

Pensemos. «Set» y «host» son imprescindible-obvio; además, es la fórmula. Probemos de nuevo ¿Cuál sigue? - Las constelaciones se terminaron. Podemos intentar con las estrellas. A ver... ¿Castor, una de las dos más brillantes de Géminis? - Set Host Castor deletreó Wau mientras tecleaba.

Cuando la computadora comenzó a ronronear, Wau Holland y Steffen Wernery supieron que habían logrado su objetivo. Segundos más tarde la pantalla mostraba un mensaje: «Bienvenidos a las instalaciones VAX del cuartel general, de la NASA». Wau sintió un sacudón y atinó a escribir en su cuaderno: «Lo logramos, por fin... Sólo hay algo seguro, la infinita inseguridad de la seguridad».

El 2 de mayo de 1987, los dos hackers alemanes, de 23 y 20 años respectivamente, ingresaron sin autorización al sistema de la central de investigaciones aerospaciales más grande del mundo.- ¿Por qué lo hicieron? - Preguntó meses después un periodista norteamericano. Porque es fascinante. En

[198] http://www.Monografias.com/legisdelinf.

este mundo se terminaron las aventuras. Ya nadie puede salir a cazar dinosaurios o a buscar oro. La única aventura posible -respondió Steffen, está en la pantalla de un ordenador. Cuando advertimos que los técnicos nos habían detectado, les enviamos un telex: «Tememos haber entrado en el peligroso campo del espionaje industrial, el crimen económico, el conflicto este-oeste y la seguridad de los organismos de alta tecnología.

Por eso avisamos, y paramos el juego». El juego puede costar muchas vidas ¡Ni media vida! La red en que entramos no guarda información ultra secreta; en este momento tiene 1,600 subscriptores y 4,000 clientes flotantes.

Con esos datos, Steffen anulaba la intención de presentarlos como sujetos peligrosos para el resto de la humanidad». (Hackers, la guerrilla informática - Raquel Roberti).

"Murphy lan, Captain Zapo, en julio de 1981 Lan Murphy, un muchacho de 23 años que se autodenominaba «Captain Zap», gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o de la casa blanca. En ese entonces Lan Murphy de 24 años de edad, conocido en el mundo del hacking como «Captain Zap".[199]

Mostró la necesidad de hacer mas clara la legislación cuando en compañía de un par de amigos y usando una computadora y una línea telefónica desde su hogar viola los accesos restringidos a compañías electrónicas, y tenía acceso a órdenes de mercancías, archivos y documentos del gobierno. «Nosotros usamos los a la Casa Blanca para hacer llamadas a líneas de bromas en Alemania y curiosear archivos militares clasificados» Explico Murphy. «El violar accesos nos resultaba muy

[199] Monografias com/legisdelinf

divertido». La Banda de hackers fue finalmente puesta a disposición de la ley». Con cargos de robo de propiedad, Murphy fue multado por US $1000 y sentenciado a 2 años de prueba.[200]

4.9 ESTADÍSTICAS SOBRE DELITOS INFORMÁTICOS.

Desde hace aproximadamente cinco años, en los Estados Unidos existe una institución que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos a través de las computadoras.

Esta entidad es El Instituto de Seguridad de Computadoras (CSI), quien anunció los resultados de su quinto estudio anual denominado «Estudio de Seguridad y Delitos Informáticos» realizado a un total de 273 Instituciones principalmente grandes Corporaciones y Agencias del Gobierno.

Este Estudio de Seguridad y Delitos Informáticos es dirigido por CSI con la participación Agencia Federal de Investigación (FBI) de San Francisco, División de delitos informáticos. El objetivo de este esfuerzo es levantar el nivel de conocimiento de seguridad, así como ayudar a determinar el alcance de los Delitos Informáticos en los Estados Unidos de Norteamérica.

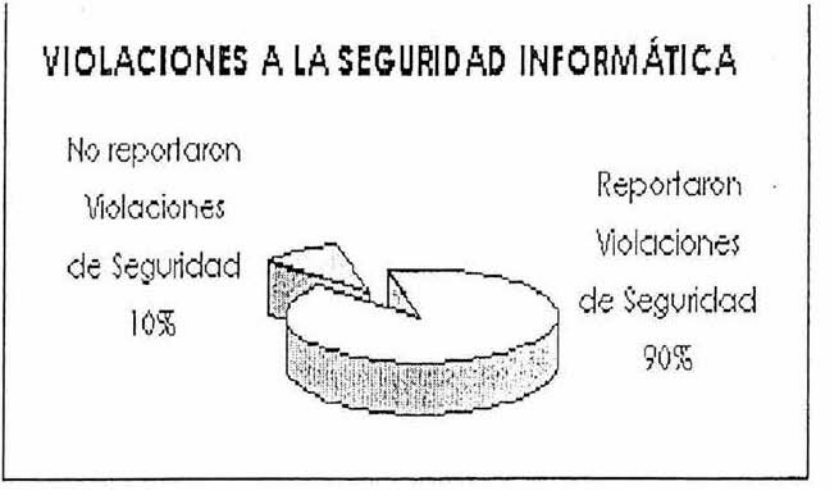
Entre lo más destacable del Estudio de Seguridad y Delitos Informáticos realizados en el año dos mil, se puede incluir lo siguiente:

---

[200] [illegible] Monografias.com/legisdelinf.

Violaciones a la seguridad informática.

Respuestas	(%)
No reportaron Violaciones de Seguridad	10%
Reportaron Violaciones de Seguridad	90%



90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.

70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados - por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

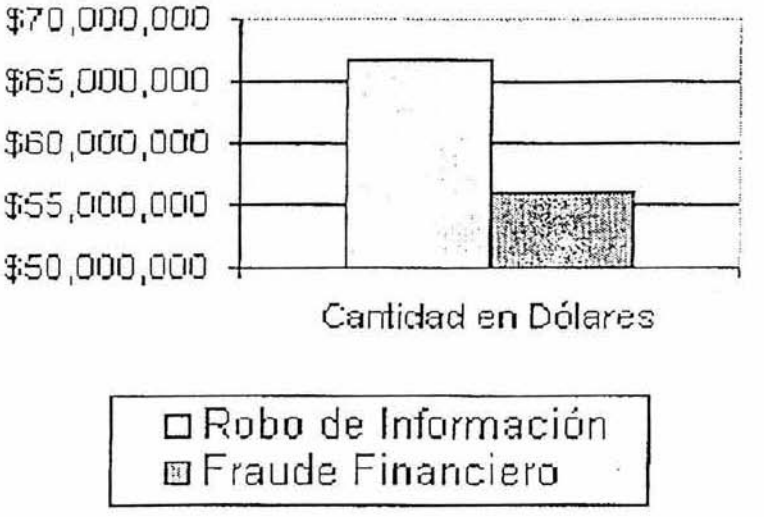
PÉRDIDAS FINANCIERAS.

74% reconocieron pérdidas financieras debido a las violaciones de las computadoras.

Las pérdidas financieras ascendieron a $265, 589,940 (el promedio total anual durante los últimos tres años era $120, 240,180).

61 encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27, 148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10, 848,850.

PÉRDIDAS POR SABOTAJE INFORMÁTICO.

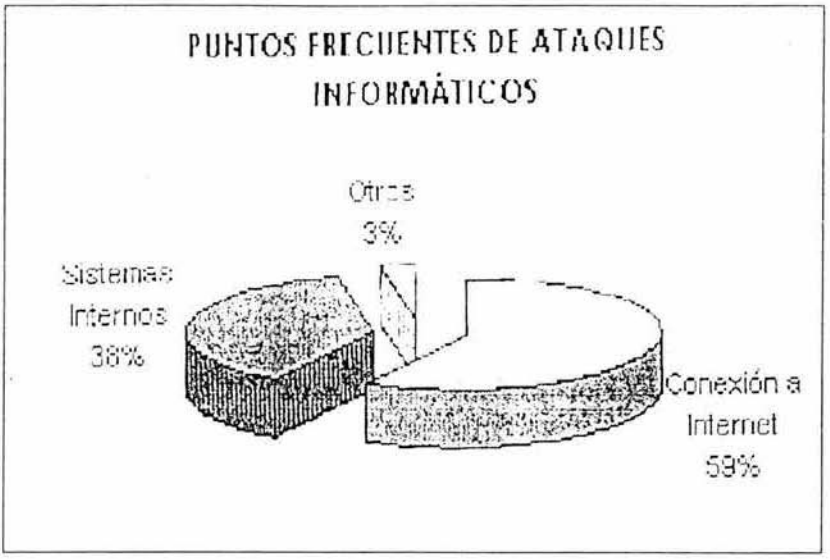


Cantidad en Dólares

Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66, 708,000) Y el fraude financiero (53 encuestados informaron $55, 996,000).

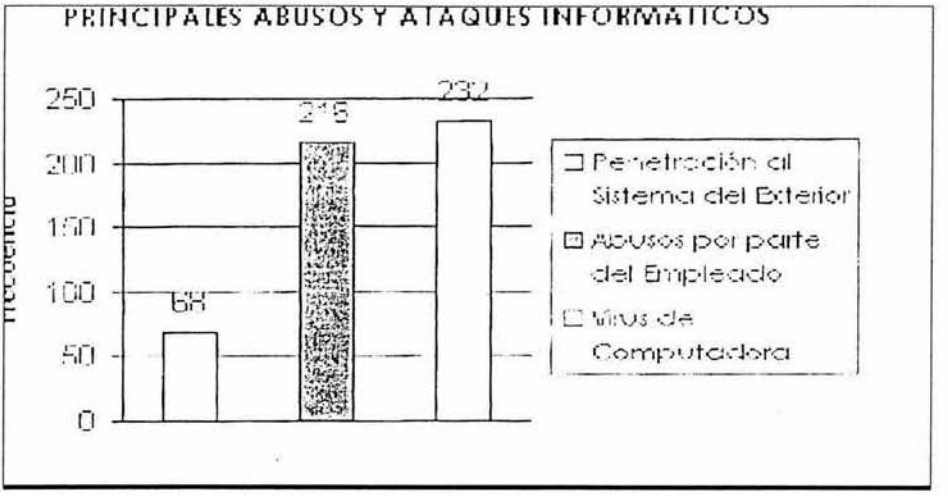
Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

PUNTOS FRECUENTES DE ATAQUES INFORMÁTICOS



71 % de los encuestados descubrieron acceso desautorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuesta dos (59%) mencionó su conexión de Internet como un punto frecuente de ataque, los que citaron sus sistemas interiores como un punto frecuente de ataque fue un 38%.

Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del «Estudio de Seguridad y Delitos Informáticos 2000 confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo.



Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) Y el fraude financiero (53 encuestados informaron $55,996,000).

Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

Los encuestados detectaron una amplia gama a de ataques y abusos. Aquí están algunos otros ejemplos:

25% de encuestados descubrieron penetración al sistema del exterior.

79% descubrieron el abuso del empleado por acceso de Internet (por ejemplo, transmitiendo pornografía o pirateó de software, o uso inapropiado de sistemas de correo electrónico).

85% descubrieron virus de computadoras. Comercio electrónico.

Por segundo año, se realizaron una serie de preguntas acerca del comercio electrónico por Internet. Aquí están algunos de los resultados:

93% de encuestados tienen sitios de WWW.

43% maneja el comercio electrónico en sus sitios (en 1999, sólo era un 30%).

19% experimentaron accesos no autorizados o inapropiados en los últimos doce meses.

32% dijeron que ellos no sabían si hubo o no, acceso no autorizado o inapropiado.

35% reconocieron haber tenido ataques, reportando de dos a cinco incidentes.

19% reportaron diez o más incidentes.

64 % reconocieron ataques reportados por vandalismo de la Web.

8% reportaron robo de información a través de transacciones.

3% reportaron fraude financiero.

Conclusión sobre el estudio del Instituto de Seguridad de Computación:

Las tendencias que el estudio de CSI/FBI ha resaltado por años son alarmantes. Los «Cyber crímenes» y otros delitos de seguridad de información se han extendido y diversificado. El 90% de los encuestados reportaron ataques.

Además, tales incidentes pueden producir serios daños. Las 273 organizaciones que pudieron cuantificar sus pérdidas, informaron un total de $265, 589,940. Claramente, la mayoría fueron en condiciones que se apegan a prácticas legítimas, con un despliegue de tecnologías sofisticadas, y lo más importante, por personal adecuado y entrenando, practicantes de seguridad de información en el sector privado y en el gobierno.

Otras estadísticas:

- La «línea caliente» de la Internet Watch Foundation (IWF), abierta en diciembre de 1996, ha recibido, principalmente a través del correo electrónico, 781 informes sobre unos 4.300 materiales de Internet considerados ilegales por usuarios de la Red. La mayor parte de los informes enviados a la «línea caliente» (un 85%) se refirieron a pornografía infantil. Otros aludían a fraudes financieros, racismo, mensajes maliciosos y pornografía de adultos.

- Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.

- Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson «Acecho cibernético: delito, represión y responsabilidad personal en el mundo online», publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.

•En Singapur.- El número de delitos cibernéticos detectados en el primer semestre del 2000, en el que se han recibido 127 denuncias, alcanza ya un 68 por ciento del total del año pasado, la policía de Singapur prevé un aumento este año en los delitos por Internet de un 38% con respecto a 1999.

•En relación con Internet y la informática, la policía de Singapur estableció en diciembre de 1999 una oficina para investigar las violaciones de los derechos de propiedad y ya ha confiscado copias piratas por valor de 9,4 millones de dólares.

•En El Salvador, existe más de un 75% de computadoras que no cuentan con licencias que amparen los programas (software) que utilizan. Esta proporción tan alta ha ocasionado que organismos Internacionales reacciones ante este tipo de delitos tal es el caso de BSA (Bussines Software Alliance).

Robert Morris, un inventor del sistema operativo Unix y más tarde principal técnico de la agencia nacional de seguridad en los Estados Unidos de América, fue precursor en el descubrimiento de cómo introducirse sin autorización en una computadora y también como protegerla.

Con el advenimiento de la tecnología computacional ya enraizada en las instituciones financieras, muy probablemente se hayan enfrentado los bancos o empresas algún tipo de delincuente informático, aún cuando esta figura no existe formalmente en nuestros códigos punitivos todavía.

No existe información exacta que determine cuantas organizaciones o personas han sido víctimas de ilícitos informáticos.

Sin embargo, las estimaciones conocidas de distintas fuentes estadísticas establecen que las víctimas morales o físicas prefieren no reportar estos hechos por temor a la publicidad negativa, a situaciones vergonzosas o por ambas circunstancias. Pero una cosa es cierta, los delitos informáticos se están incrementando. Las sociedades modernas dependen cada vez más del uso de la tecnología, por lo tanto los criminales también están expandiendo su arsenal delictivo incluyendo la tecnología informática.

En los Estados Unidos de América, el departamento de justicia estableció como una definición básica el crimen por computadoras en la forma siguiente:

"Cualquier acto ilegal por cuyo conocimiento de la tecnología computacional, ésta es utilizada para cometer el hecho" obviamente es una definición muy escueta, sin embargo también puede ser muy amplia, dependiendo de la interpretación que quiera darse.

Una de las formas para tratar de establecer la incidencia delictiva en materia de ilícitos informáticos ha sido el uso de encuestas. Las siguientes estimaciones corresponden a un diagnóstico de seguridad de delitos por computadoras realizado en 1999 en los Estados Unidos de América por el Instituto Nacional Computacional conjuntamente con el FBI. Del 100% de empresas que contestaron se tiene que:

- 62% sufrieron violaciones a la seguridad informática.
- 30% reportó penetración por hackers externos.
- 57% reportó intrusión en conexiones de Internet.
- 32% reportó negación de servicios por ataques masivos.
- 19% experimentó sabotaje en redes de datos.
- 14% reportó ser víctima de fraude financiero.
- 90% tuvo incidentes de contaminación por virus.
- 55% reportó accesos no autorizados de empleados.
- 97% reportó abuso interno de privilegios de Internet.

- 69% reportó pérdida y robo de laptops.
- 26% mencionó robo de información de su propiedad.
- 32% reportó los incidentes a las autoridades de justicia.
- Las pérdidas estimadas en 3 años consecutivos superaron los 100 millones de dólares.
- Del 51% de empresas que reconocieron sus pérdidas solo el 31% pudo establecer el monto del daño.[201]

[201] http: WWW. Legal infosel com.

CAPITULO V.

5.1 Fundamentos para la tipificación de los delitos informáticos en el código penal federal.

CAPITULO V. FUNDAMENTACIÓN PARA LA TIPIFICACIÒN DE LOS DELITOS INFORMATICOS EN EL CÒDIGO PENAL FEDERAL.

Los siguientes fundamentos, son una propuesta de reforma y adiciones al Código Penal Federal, correspondiente en la creación de tipos penales en materia de informática, propuesta con la que se pretende que sea presentada como una propuesta legislativa al Congreso de la Unión, ya que se pretende prever que los delitos informáticos, que no son otra cosa que las conductas antisociales, cometidas teniendo como objeto del delito o como medio de comisión a los sistemas informáticos, las conductas a combatir pueden ser muy amplias y revestir muy variadas formas.

Por lo que haré mención de las principales conductas antisociales que tuve en mente al formular los nuevos tipos penales, como lo son:

1. Constituyendo conductas antisociales preponderantemente contra lo bienes patrimoniales.

- Adquisición no autorizada de información.
- Daño a programas.
- Substracción de efectivo
- Beneficios indebidos por el uso inadecuado de bancos de datos.
- Piratería de programación o su adquisición ilegal.
- Fraudes.
- Robo de dinero.
- Apoderamiento no autorizado de información, discos o programas.

2. constituyendo conductas antisociales preponderantemente a los derechos de las personas como lo es la intimidad.

- Violación a la privacidad.
- Adquisición ilegal de información.

3. constituyendo conductas antisociales preponderantemente a los delitos contra la moral pública y las buenas costumbres.

- Pornografía infantil a través de los sistemas informáticos.

4. constituyendo conductas antisociales preponderantemente contra la falsedad.

- Falsificación de documentos a través de los scanner de computadoras.

5. Entre otros.

Los bienes jurídicos a proteger por los nuevos tipos penales, el cual es el objetivo de esta reforma, deberá garantizar por una parte la confiabilidad, seguridad e invulnerabilidad de los sistemas informáticos y por otra parte los derechos de las personas en su vertiente moral y patrimonial, entre otros.

ADICIONES Y REFORMAS AL CÓDIGO PENAL FEDERAL.

Los delitos propuestos formaran parte del Código Penal Federal, en primer término en relación al bien jurídico tutelado a proteger en los delitos informáticos es fundamentalmente el patrimonio, la privacidad e intimidad.

Por lo que se propone:

Adicionar la fracción III, del Titulo Vigésimo Segundo de los delitos en contra de las personas en su patrimonio, Capítulo I, Artículo 368 del Código Penal Federal.

ARTICULO 368.- Se equiparan al robo y se castigarán como tal:

I.- El apoderamiento o destrucción dolosa de una cosa propia mueble, si ésta se halla por cualquier título legítimo en poder de otra persona y no medie consentimiento; y

II. El uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

III. El aprovechamiento de la información contenida en un sistema informático o de sus claves de acceso, ejecutando sin derecho y sin consentimiento de la persona que legalmente pueda disponer de ella.

Reforma la fracción XVI, derogado el 24 de diciembre de 1996, del Título Vigésimo Segundo de los delitos en contra de las personas en su patrimonio, Capítulo III, Artículo 378 del Código Penal Federal.

ARTÍCULO 387.- Las mismas penas señaladas en el artículo anterior, se impondrán:

I.- Al que obtenga dinero, valores o cualquiera otra cosa ofreciendo encargarse de la defensa de un procesado o de un reo, o de la dirección o patrocinio en un asunto civil o administrativo, si no efectúa aquélla o no realiza ésta, sea porque no se haga cargo legalmente de la misma, o porque renuncie o abandone el negocio o la causa sin motivo justificado;

II.- Al que por título oneroso enajene alguna cosa con conocimiento de que no tiene derecho para disponer de ella, o la arriende, hipoteque, empeñe o grave de

cualquier otro modo, si ha recibido el precio, el alquiler, la cantidad en que la gravó, parte de ellos, o un lucro equivalente;

III.- Al que obtenga de otro una cantidad de dinero o cualquiera otro lucro, otorgándole o endosándole a nombre propio o de otro, un documento nominativo, a la orden o al portador contra una persona supuesta o que el otorgante sabe que no ha de pagarle;

IV.- Al que se haga servir alguna cosa o admita un servicio en cualquier establecimiento comercial y no pague el importe;

V.- Al que compre una cosa mueble ofreciendo pagar su precio al contado y rehuse después de recibirla, hacer el pago o devolver la cosa, si el vendedor le exigiere lo primero dentro de quince días de haber recibido la cosa del comprador;

VI.- Al que hubiere vendido una cosa mueble y recibido su precio, si no la entrega dentro de los quince días del plazo convenido o no devuelve su importe en el mismo término, en el caso de que se le exija esto último.

VII.- Al que vende a dos personas una misma cosa sea mueble o raíz y recibe el precio de la primera o de la segunda enajenación, de ambas o parte de él, o cualquier otro lucro con perjuicio del primero o del segundo comprador.

VIII.- Al que valiéndose de la ignorancia o de las malas condiciones económicas de una persona, obtenga de ésta ventajas usuarias (sic) por medio de contratos o convenios en los cuales se estipulen réditos o lucros superiores a los usuales en el mercado.

IX.- Al que para obtener un lucro indebido, ponga en circulación fichas, tarjetas u otros objetos de cualquier materia como signos convencionales en substitución de la moneda legal;

X.- Al que simulare un contrato, un acto o escrito judicial, con perjuicio de otro o para obtener cualquier beneficio indebido.

XI.- Al que por sorteos, rifas, loterías, promesas de venta o por cualquiera otro medio, se quede en todo o en parte con las cantidades recibidas, sin entregar la mercancía u objeto ofrecido.

XII.- Al fabricante, empresario, contratista, o constructor de una obra cualquiera, que emplee en la construcción de la misma, materiales en cantidad o calidad inferior a la convenida o mano de obra inferior a la estipulada, siempre que haya recibido el precio o parte de él;

XIII.- Al vendedor de materiales de construcción o cualquiera especie, que habiendo recibido el precio de los mismos, no los entregare en su totalidad o calidad convenidos;

XIV.- Al que venda o traspase una negociación sin autorización de los acreedores de ella, o sin que el nuevo adquirente se comprometa a responder de los créditos, siempre que estos últimos resulten insolutos. Cuando la enajenación sea hecha por una persona moral, serán penalmente responsables los que autoricen aquella y los dirigentes, administradores o mandatarios que la efectúen;

XV.- Al que explote las preocupaciones, la superstición o la ignorancia del pueblo, por medio de supuesta evocación de espíritus, adivinaciones o curaciones.

XVI.- Al que con engaño o aprovechándose del error en que otro se halla, actuando en calidad de usuario, intermediario, empresa proveedora de información, banco o cualquier empresa comercializadora, utilice el intercambio electrónico de datos, con animo de lucro, aprovechándose de un acceso a los sistemas de redes computacionales, adquiriendo, enajenando,

transfiriendo, depositando, o dando en garantía productos y servicios de toda índole

XVII.- Al que valiéndose de la ignorancia o de las malas condiciones económicas de un trabajador a su servicio, le pague cantidades inferiores a las que legalmente le corresponden por las labores que ejecuta o le haga otorgar recibos o comprobantes de pago de cualquier clase que amparen sumas de dinero superiores a las que efectivamente entrega.

XVIII.- Al que habiendo recibido mercancías con subsidio o franquicia para darles un destino determinado, las distrajere de este destino o en cualquier forma desvirtúe los fines perseguidos con el subsidio o la franquicia.

XIX.- A los intermediarios en operaciones de traslación de dominio de bienes inmuebles o de gravámenes reales sobre éstos, que obtengan dinero, títulos o valores por el importe de su precio, a cuenta de él o para constituir ese gravamen, si no los destinaren, en todo o en parte, al objeto de la operación concertada, por su disposición en provecho propio o de otro.

Para los efectos de este delito se entenderá que un intermediario no ha dado su destino, o ha dispuesto, en todo o en parte, del dinero, títulos o valores obtenidos por el importe del precio o a cuenta del inmueble objeto de la traslación de dominio o del gravamen real, si no realiza su depósito en Nacional Financiera, S. A. o en cualquier Institución de Depósito, dentro de los 30 días siguientes a su recepción a favor de su propietario o poseedor, a menos que lo hubiese entregado, dentro de ese término, al vendedor o al deudor del gravamen real, o devuelto al comprador, o al acreedor del mismo gravamen.

Las mismas sanciones se impondrán a los gerentes, directivos, mandatarios con facultades de dominio o de administración, administradores de las personas

morales que no cumplan o hagan cumplir la obligación o (sic) que se refiere el párrafo anterior.

El depósito se entregará por Nacional Financiera, S. A. o la Institución de Depósito de que se trate, a su propietario o al comprador.

Cuando el sujeto activo del delito devuelva a los interesados las cantidades de dinero obtenidas con su actuación, antes de que se formulen conclusiones en el proceso respectivo, la pena que se le aplicará será la de tres días a seis meses de prisión.

XX.- A los constructores o vendedores de edificios en condominio que obtengan dinero, títulos o valores por el importe de su precio o a cuenta de él, si no los destinaren, en todo o en parte, al objeto de la operación concertada, por su disposición en provecho propio o de otro.

Es aplicable a lo dispuesto en esta fracción, lo determinado en los párrafos segundo a quinto de la fracción anterior.

XXI.- Al que libre un cheque contra una cuenta bancaria, que sea rechazado por la institución o sociedad nacional de crédito correspondiente, en los términos de la legislación aplicable, por no tener el librador cuenta en la institución o sociedad respectiva o por carecer éste de fondos suficientes para el pago. La certificación relativa a la inexistencia de la cuenta o a la falta de fondos suficientes para el pago, deberá realizarse exclusivamente por personal específicamente autorizado para tal efecto por la institución o sociedad nacional de crédito de que se trate.

No se procederá contra el agente cuando el libramiento no hubiese tenido como fin el procurarse ilícitamente una cosa u obtener un lucro indebido.

Las Instituciones, sociedades nacionales y Organizaciones Auxiliares de Crédito, las de Fianzas y las de Seguros, así como los organismos Oficiales y Descentralizados, autorizados legalmente para operar con inmuebles, quedan exceptuados de la obligación de constituir el depósito a que se refiere la fracción XIX.

Adicional el Capítulo III BIS del Titulo Vigésimo Segundo de los delitos en contra de las personas en su patrimonio.

CAPÍTULO III BIS.
DELITOS INFORMÁTICOS.

ARTÍCULO 399 ter.- Se aplicará la pena de prisión de dos a cinco años, y de 100 a trescientos días de multa al que:

I.- Sin estar autorizado, se apodere, altere, utilice o modifique, en perjuicio de un tercero, datos reservados de carácter personal, familiar o de negocios que se hallen registrados en ficheros programas, códigos, comandos, soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

II.- Difunda, revele o ceda a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren el apartado anterior.

III.- Con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realice la conducta descrita en el párrafo anterior.

IV.- Teniendo la calidad de encargado o responsable de los ficheros, programas, códigos, comandos o soportes informáticos, electrónicos o telemáticos, archivos o registros, incurra en lo descrito en los apartados 1 y II, se le impondrá la pena de prisión de tres a seis años de prisión.

V.- Afecte con los hechos descritos en los apartados anteriores datos de carácter personal, que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad, se impondrán las penas de cuatro a siete años de prisión.

VI.- Realice los hechos descritos de la fracción I a la III con fines lucrativos, se le impondrán penas de cinco a diez años de prisión.

VII.- Siendo proveedor de acceso a Internet, que proporcione servicios informativos que contengan material apto solo para mayores de edad, o que puedan afectar la integridad de la familia, o herir la sensibilidad de algún sector de la población, omita identificarse totalmente, incluyendo nombre o razón social, domicilio, y número telefónico, y no especifique claramente en su página de entrada la siguiente advertencia: " estas páginas contienen materiales aptos solo para adultos, si usted tiene menos de 18 años, deberá salir de esta página, si usted es un adulto que está interesado en evitar que menores de edad que manejan su equipó de cómputo, tengan acceso a estas páginas, póngase en contacto con el proveedor de la información para su cancelación."

VIII.- Siendo proveedor de acceso a Internet, solicite de los usuarios el derecho de uso de sus datos personales para determinados fines como inscripción para obtener un servicio, o comprar o vender un producto, y los utilice para fines distintos sin su aprobación.

ARTÍCULO 399 Cuater.- Las mismas penas señaladas en el artículo anterior se impondrán:

I.- Al que, sin autorización utilice una tarjeta electrónica o el que utilice indebidamente tecnologías de información, se hace ilícitamente de alguna

cosa o alcanza un lucro indebido, sin asumir el compromiso de pago de la contra prestación debida.

II.- Al que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la información contenidas en una tarjeta electrónica o en cualquier instrumento destinado a los mismos fines; o al que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos.

III.- Al que sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas electrónicas o instrumentos destinados al mismo fin, o de la información contenidas en ellos o en un sistema.

IV.- El que se apropie de una tarjeta electrónica o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario autorizado o entidad emisora.

V.- Al que a sabiendas de que una tarjeta electrónica o instrumento destinado a los mismos fines, se encuentre vencido, revocado, se haya indebidamente obtenido, retenido, falsificado, alterado, provea a quien los presente dinero, bienes o servicios o cualquier otra cosa de valor económico.

También considero necesario adicionar la fracción VIII, del Articulo 246 del Código Penal Federal.

ARTÍCULO 246.- También incurrirá en la pena señalada en el artículo 243:

I.- El funcionario o empleado que, por engaño o sorpresa, hiciere que alguien firme un documento público, que no habría firmado sabiendo su contenido;

II.- El Notario y cualquier otro funcionario público que, en ejercicio de sus funciones, expida una certificación de hechos que no sean ciertos, o da fe de lo que no consta en autos, registros, protocolos o documentos;

III.- El que, para eximirse de un servicio debido legalmente, o de una obligación impuesta por la ley, suponga una certificación de enfermedad o impedimento que no tiene, como expedida por un médico cirujano, sea que exista realmente la persona a quien la atribuya, ya sea ésta imaginaria o ya tome el nombre de una persona real, atribuyéndoles falsamente la calidad de médico o cirujano;

IV.- El médico que certifique falsamente que una persona tiene una enfermedad u otro impedimento bastante para dispensarla de prestar un servicio que exige la ley, o de cumplir una obligación que ésta impone, o para adquirir algún derecho;

V.- El que haga uso de una certificación verdadera expedida para otro, como si lo hubiere sido en su favor, o altere la que a él se le expidió;

VI.- Los encargados del servicio telegráfico, telefónico o de radio que supongan o falsifiquen un despacho de esa clase, y

VII.- El que a sabiendas hiciere uso de un documento falso o de copia, trascripción o testimonio del mismo, sea público o privado.

VIII.- Al que altere o falsificare datos de los documentos almacenados en forma computarizada, ya sea personal o comercial.

Asimismo, considero de gran importancia adicional la fracción III, al artículo 424 BIS, del Código Penal Federal:

ARTÍCULO 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

III. El que se apropie, descargue o usare, indebidamente la información contenida en un sistema informático.

Se genera por medio de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red.

Conocido también como "Pirateo Informático", consiste en entrar sin autorización a una computadora y explorar su interior.

No existe aparentemente límite pudiendo acceder por vía remota a servicios de noticias, servicios financieros, información financiera, instalaciones universitarias, correo electrónico, computadoras oficiales.

Por otra parte se propone adicionar la fracción IV, del artículo 200 de ley en mención.

ARTÍCULO 200.- Se aplicará prisión de seis meses a cinco años o sanción de trescientos a quinientos días multa o ambas a juicio del juez:

I.- Al que fabrique, reproduzca o publique libros, escritos, imágenes u objetos obscenos, y al que los exponga, distribuya o haga circular;

II.- Al que publique por cualquier medio, ejecute o haga ejecutar por otro, exhibiciones obscenas (sic), y

III.- Al que de modo escandaloso invite a otro al comercio carnal.

En caso de reincidencia, además de las sanciones previstas en este artículo, se ordenará la disolución de la sociedad o empresa.

No se sancionarán las conductas que tengan un fin de investigación o divulgación científico, artístico o técnico.

IV. El que por medio de una computadora o sistema de computación, exhiba, transmita o comercie material pornográfico relativo a la persona o a la imagen de un menor de edad, aunque mediare el consentimiento de la víctima.

Finalmente, adicionar un tercer párrafo al artículo 211 Bis-1, del Código Penal Federal.

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

El que maliciosamente destruyere, inutilizare, modificare, borrare, hiciera inaccesible o de cualquier modo y por cualquier medio, obstaculizare el funcionamiento normal de un sistema o dato informático, por medio de virus, gusanos o bombas lógicas.

Finalmente se observa la importancia del estudio de la teoría del delito para el estudio individualizado de cada conducta que al aceptarse este proyecto de reforma serían considerados como delitos.

Los delitos mencionados se persiguen algunos por **querella de parte y otros de oficio.**

El Ministerio Público recibirá la denuncia o querella sobre los hechos que pudieran constituir delitos; investigará los conducente para la demostración de que se integraron o no los elementos del tipo penal y se acreditó la probable responsabilidad del inculpado; ejercitará la acción penal; dictará las medidas precautorias correspondientes; concederá libertad provisional a los sujetos a proceso cuando proceda; aportará a la autoridad jurisdiccional las pruebas que tiendan al esclarecimiento de los hechos motivo de la acción penal; Y las demás atribuciones que señalen las leyes y reglamentos correspondientes.

Sólo en caso de flagrancia y con observancia de lo prescrito por el arto 16 Constitucional es posible la detención de una persona.

La comprobación de los Elementos del Tipo Penal.- Para ello se estará a lo dispuesto por los, idénticos, artículos 168 del Código Federal de Procedimientos Penales:

ARTÍCULO 168. El Ministerio Público acreditará el cuerpo del delito de que se trate y la probable responsabilidad del indiciado, como base del ejercicio de la acción penal; y la autoridad judicial, a su vez, examinará si ambos requisitos están acreditados en autos.

Por cuerpo del delito se entiende el conjunto de los elementos objetivos o externos que constituyen la materialidad del hecho que la ley señale como delito, así como los normativos, en el caso de que la descripción típica lo requiera.

La probable responsabilidad del indiciado se tendrá por acreditada cuando, de los medios probatorios existentes, se deduzca su participación en el delito, la comisión dolosa o culposa del mismo y no exista acreditada a favor del indiciado alguna causa de licitud o alguna excluyente de culpabilidad.

El cuerpo del delito de que se trate y la probable responsabilidad se acreditarán por cualquier medio probatorio que señale la ley.

El Agente del Ministerio Público deberá tomar en consideración lo previsto en los artículos 7°, 8°,9°, 12, 13, 15 Y 17 del Código Penal Federal.

Sólo en el caso de que se verifique o compruebe fehacientemente que se han integrado los elementos del tipo penal del delito de que se trate, se podrá proceder a determinar el ejercicio de la acción penal.

El pliego de consignación hará referencia a los medios de prueba de los elementos del tipo, y acerca de la probable responsabilidad. Asimismo, si hubiera derecho a la libertad provisional del inculpado.

METODOLOGÍA PARA ACREDITAR LOS ELEMENTOS DEL TIPO PENAL Y LA PROBABLE RESPONSABILIDAD DEL INCULPADO

Para obrar de conformidad con lo exigido por el Art. 19 Constitucional, se deberá analizar:

1 °. COMO ACREDITAR LOS ELEMENTOS DEL TIPO PENAL;

2°. COMO DETERMINAR LA PROBABLE RESPONSABILIDAD DEL INCULPADO.

Con la finalidad anterior se propone a continuación una matriz sistemática para acreditar los elementos del tipo penal y la probable responsabilidad penal de las personas indiciadas al procedimiento de averiguación previa.

MATRIZ PARA LA ACREDITACIÓN DE LOS ELEMENTOS DEL TIPO PENAL Y PARA DETERMINAR LA PROBABLE RESPONSABILIDAD DEL INCULPADO.

I. ELEMENTOS DEL TIPO PENAL

A) ELEMENTOS OBJETIVOS

1. **LA CONDUCTA.**- activa u omisiva.

2. **EL SUJETO ACTIVO.**- Su forma de intervención.

3. **EL SUJETO PASIVO.**- Su identidad; el daño sufrido.

4. EL BIEN JURÍDICO PROTEGIDO. LAS LESIONES O LA PUESTA EN PELIGRO DEL MISMO.- Su definición.

5. EL OBJETO MATERIAL

6. LOS MEDIOS UTILIZADOS

7. CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO Y OCASIÓN

8. ELEMENTOS NORMATIVOS

9. EL RESULTADO

B) ELEMENTOS SUBJETIVOS

1. GENERALIDADES. Se analiza si se realiza una conducta dolosa o culposa en la acción u omisión.

2- EL DOLO radica en:

A) El conocimiento

B) La voluntad

Artículo 9 del Código Penal Federal.- "obra dolosamente el que conociendo los elementos del tipo penal, o previendo como posible el resultado típico, quiere o acepta la realización del hecho descrito por la ley; y Obra culposamente, el que produce el resultado típico que o previó siendo previsible o previo confiando en que no se produciría, en virtud de la violación a un deber de cuidado, que debía y podía observar según las circunstancias y condiciones personales".

El dolo requiere ser probado en sus dos elementos: el conocimiento, y la voluntad. Para efectos del dolo se requiere que el sujeto activo tenga conocimiento de los elementos objetivos del tipo penal ya sean descriptivos o normativos. La voluntad por su parte en el dolo se manifiesta cuando el sujeto activo *"quiere o acepta"* la realización del hecho descrito por la ley *(dolo directo* o *dolo eventual),* abrazando esa conducta.

Debe verificarse que el indiciado no se encontraba en las circunstancias previstas por el artículo 15 del Código Penal Federal, que se refiere a las causas de exclusión del delito por haber realizado la acción u omisión bajo un error invencible sobre alguno de los elementos que integran el tipo penal, lo que constituiría un error de tipo y por lo tanto una causa de atipicidad. Si es error no invencible, no puede excluirse a la culpa, y aunque no pueda configurarse la tipicidad dolosa, se configura la tipicidad culposa.

ELEMENTOS SUBJETIVOS ESPECÍFICOS.

LA DETERMINACIÓN DE LA PROBABLE RESPONSABILIDAD DEL INCULPADO EL AGENTE DEL MINISTERIO PÚBLICO DEBERÁ:

Acreditar la probable culpabilidad, para lo cual se deberá acreditar: la conciencia de antijuridicidad del sujeto activo; la exigibilidad de otra conducta.

Comprobar y acreditar si el sujeto activo era imputable al momento de cometer el hecho tipico.

Determinar en consecuencia la probable culpabilidad del indiciado.

Para la determinación de la probable responsabilidad del inculpado, responder si no existe alguna causa exclusión del delito referente a la falta de los elementos del tipo penal, objetivos o subjetivos.

CONCLUSIONES.

La finalidad de la elaboración de esta tesis, es la elaboración de un proyecto de reforma al Código Penal Federal, para la preservación del bien común, para crear un poco de conciencia en nuestros legisladores, en relación a que en la actualidad existe un desafió permanente al exigir una adecuación a los nuevos fenómenos que la vida social va presentando de manera que se encuentra preparada la sociedad a insertarlos dentro de sus ámbitos de conocimiento y acción la utilización de dichos medios informáticos, al ser destinados al servicio de la sociedad, requieren de una inminente regulación jurídica con respecto a su utilización, y analizar las conductas delictivas que puede generar el gran avance tecnológico, sobre todo en el campo de la informática.

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades, sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquélla. En ese entendido, el presente trabajo se dirige al análisis de las posibles medidas preventivas, ya sean de carácter administrativo o penal que deben ser tomadas en cuenta para evitar que la comisión de este tipo de infracciones o delitos alcance en México los niveles de peligrosidad que se han registrado en otros países.

No parece adecuado hablar del delito informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal federal para que pueda existir un delito.

Por tanto, al no estar tipificado el delito informático, acudiremos al principio de legalidad en materia penal indicador de la ley como creadora de delitos y penas, al conocido principio *nullus crimen, nulla poena, sine lege,* e indicaremos que no habiendo Ley que tipifique y consecuentemente, indique la conducta delictiva y no habiendo ley que determine cual es la pena, no existe delito ni pena por la acción, por dolosa que sea, que en esta tesis analizamos como delitos informáticos.

Esta prevención del delito debe contar con la legislaciones penales federales adecuadas a las conductas antisociales que se generan dia con dia, y las Instituciones especiales tendientes a combatir y configurar las acciones del país que permitan tener resultados concretos en la disminución de los altos indices delictivos que actualmente tenemos en nuestro país, y para que exista una convivencia social hoy en día.

Por lo que se sugiere que exista una legislación adecuada sobre la protección de los sistemas informáticos, creando una nueva regulación sólo en aquellos aspectos en los que en base a las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos pueden proporcionar datos e informaciones sobre miles de personas, físicas y morales, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, provisionales y de identificación de las personas, y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares, se comprenderá que están en juego o podrían llegar a estarlo de modo dramático,

algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

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

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, dadas las caracteristicas 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.

Uno de los derechos más defendidos en los paises en los que ha habido una gran implantación de los sistemas informáticos en la gestión de los datos de los ciudadanos por parte de la administración, ha sido el derecho a la persona a que su intimidad no sea vulnerada por un abuso de estos medios. La protección de éste derecho ha generado preceptos de rango constitucional en muchos paises.

En nuestro país se regulan administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero aún no contemplan en sí los delitos informáticos. El tratamiento administrativo se realiza a través de la Ley Federal del Derecho de Autor, y el penal se ha establecido en el Título Vigésimo Sexto del Código Penal para el Distrito Federal en materia de Fuero Común y para toda la República en materia de Fuero Federal. Sobre el particular, debe aclararse que ley no regula delitos informáticos ya que su competencia es la de sancionar administrativamente conductas ilícitas cuyo bien jurídico a tutelar es la propiedad intelectual Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997.

Para finalizar se incluye una propuesta, sustentada en el estudio comparativo antes mencionado, que trata de adecuar a la realidad existente en México, pero previendo que nuestro país no está exento de la velocidad del desarrollo tecnológico y de los vicios que éste genera.

Propuesta en la que se analizó la gravedad que implican los delitos informáticos, es necesario que el Código Penal Federal incluya figuras delictivas que contengan los delitos informáticos ya que de no hacerlo, la ausencia de figuras concretas que se puedan aplicar en esa materia daría lugar a que los autores de esos hechos quedaran impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos.

BIBLIOGRAFIA

1. AMOROSO Fernández, Yarina. LA INFORMATICA COMO OBJETO DE DERECHO. Revista de Ciencias Jurídicas N.1, Habana Cuba, 1991. 43 p.

2. ARTEAGA S. EL DELITO INFORMATICO, Revista de la Facultad de Ciencias Jurídicas y Políticas. N. 68, Universidad de Venezuela, 1987. 115 p.

3. BARRIOS Garrido Gabriela, MUÑOZ de Alba M Marcia, PÉREZ Bustillos Camilo INTERNET Y DERECHO EN MEXICO. EDT. MC Graw Hill. México 1998.pp.180.

4. BECCARIA. TRATADO DE LOS DELITOS Y DE LAS PENAS. Editorial Porrùa. S.A. México1995. pp.408.

5. BETANCOURT López, Eduardo. TEORIA DEL DELITO. Editorial Porrùa. S.A. México1994.pp.304.

6. CASTELLANOS, Fernando, LINEAMIENTOS ELEMENTALES DEL DERECHO PENAL, México 2002, Editorial. Porrùa.

7. DAVARA Rodriguez, Miguel ángel. DERECHO INFORMATICO. México. Editorial Aranzadi, 1993.

8. DEL PONT K., Luis Marco y NADELSTICHER Mitrania, Abraham, DELITOS DE CUELLO BLANCO Y REACCIÒN SOCIAL, Instituto Nacional de Ciencias Penales. México, 1981.

9. DÍAZ Aranda, Enrique. DERECHO PENAL PARTE GENERAL, Ed. Porrúa, México 2003.

10. DÍAZ Aranda, Enrique. DOLO, Ed. Porrúa, México 2004.

11. EUGENIO, Cuello Calón. DERECHO PENAL I, 8° Edición, p.8.

12. GOLDSTEIN, Raúl, DICCIONARIO DE DERECHO PENAL Y CRIMINOLOGÍA, Buenos Aires, Argentina, 3ª, 1993, pp. 293.

13. GONZÁLEZ de la Vega, Francisco. DERECHO PENAL MEXICANO. Editorial Porrùa. S.A. México 1996. pp. 473.

14. GONZÁLEZ Quintanilla, José Arturo. DERECHO PENAL MEXICANO. (PARTE GENERAL).Editorial Porrùa .S.A. México1993. pp.503.

15. HANCE, Olivier, LEYES Y NEGOCIOS EN INTERNET, Mèxico, Editorial De Mc Gram Hill, 1996.

16. JIMÉNES DE ASÚA, Luis, PRINCIPIOS DEL DERECHO PENAL, LA LEY Y EL DELITO, Editorial sudamericana, Buenos Aires, 1990, p.210.

17. JIMÉNES Martinez, Javier, INTRODUCCIÓN A LA TEORÍA GENERAL DEL DELITO, Ed. Ángel, México.2003.

18. LIMA DE LA LUZ, Maria. DELITOS ELECTRONICOS. En Crimenalia. México, Academia Mexicana de Ciencias Penales, Editorial Porrùa.1984. 100 p.

19. MAGGIORE, DERECHO PENAL I, Editorial Temis, Bogotá, 1954, p.3.

20. MANUAL DEL JUSTICIABLE EN MATERIA PENAL, Poder Judicial de la Federación, México 2004.

21. MALO Camacho, Gustavo. DERECHO PENAL MEXICANO. Editorial Porrùa. S.A. México. 1998.

22. MIR PUIG, DELINCUENCIA INFORMÀTICA, Promociones y Publicaciones Universitarias. Barcelona, 1992.

23. MUÑÓZ Conde Francisco, TEORÍA GENERAL DEL DELITO, Ed. Temis, Bogota Colombia 2002.

24. PORTE, Petit Candaudao, Celestino, APUNTES DE LA PARTE GENERAL DEL DERECHO PENAL, Editorial Porrùa, 1983, p 419-420.

25. TELLEZ Valdés, Julio. DERECHO INFORMÀTICO, segunda edición, México, Editorial De MC Gram Hill, 1996, 103-104 p.

26. VILLALOBOS, Ignacio. DERECHO PENAL MEXICANO. Editorial Porrùa. S.A. México 1975. pp. 650.

27. ZAVALA, Antelmo. EL IMPACTO SOCIAL DE LA INFORMÀTICA JURÌDICA EN MÈXICO. Tesis. Mèxico UNAM. 1996.

HEMEROGRAFÌA

26. NOVEDADES, México, Jueves 20 de agosto de 1992.
27. JORNADFA, México, Sábado 12 de abril de 1997.
28. EL SOL DE MÈXICO, Lunes 21 de abril 1997.
29. EL UNIVERSAL, México, Martes 29 de abril de 1997.

LEGISLACIÒN.

30. C.D ROM COMPILACIÓN DE LEYES, Suprema Corte de Justicia de la Nación, 2004.
31. C-D ROM Informática y Derecho.
32. C-D ROM Justicia Cibernética.
33. Código Penal para el Distrito Federal del Fuero Común y Federal.
34. Código Penal y de Procedimientos Penales del Estado de Sinaloa.
35. Ley Federal de Derechos de Autor.
36. Tratado de Libre Comercio parte 3, Diario Oficial de la Federación, Lunes 20 de abril de 1997.

OTRAS.

37. http: WWW. Monografías. Com.
38. http: WWW. Legal infosel. Com.
39. http: WWW. delitosinformáticos. Com.
40. http: WWW. Fiscalia. Org/informático. Com.