UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

LICENCIATURA EN DERECHO.

"ANÁLISIS JURÍDICO DEL DELITO DE ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA PREVISTO EN EL CAPÍTULO SEGUNDO DE EL TÍTULO NOVENO DE EL CÓDIGO PENAL FEDERAL".

TESIS

Que para obtener el título de
Licenciado en Derecho presenta:

ALUMNO: BERNAL PEDRAZA LUIS
CTA: 09903562-6
TEL. 26-26-34-70

ASESOR: LIC. DAVID TORRES DURÁN.

MAYO DE 2011

AGRADECIMIENTOS.

A DIOS, por todo las bendiciones que me ha dado, y que me han permitido culminar mis estudios profesionales.

A MI MADRE, SANTA PEDRAZA AUSTRIA, por ser el ángel que ha estado a mi lado a lo largo de mi vida y que me ha hecho lo que soy. Todo esto es y será por siempre gracias a ti mamita. Lo logramos!

A MI PADRE, LIC. LUIS RAMÓN BERNAL TAPIA, por alentarme siempre a terminar mis estudios y orientarme con su ejemplo a ser un profesional del Derecho.

A MI HERMANO, LIC. EN PSIC. RAMÓN BERNAL PEDRAZA, por que sin su apoyo, no hubiera sido posible la realización de esta meta.

Al amor de mi vida, MI ESPOSA VIANEY, por todo su cariño y compresión.

A MI HIJO LUIS EDUARDO, el cual constituye todas mis razones y motivos para salir adelante y seguir en esta vida. Te amo hijo.

A TODOS Y CADA UNO DE LOS INTEGRANTES DE MI FAMILIA, por todo el aliento y el apoyo brindado siempre.

De manera muy especial deseo agradecer al LICENCIADO DAVID TORRES DURÁN, asesor de la presente tesis, por todo el generoso apoyo que me ha brindado en múltiples momentos trascendentales de mi vida, sin el cual no hubiera sido posible la conclusión de mis estudios profesionales.

AL DOCTOR EN DERECHO GABINO EDUARDO CASTREJÓN GARCÍA, por sus conocimientos aportados a mi formación profesional, por haber tenido el privilegio de ser su alumno, y por toda la experiencia compartida dentro del aula.

AL MAESTRO JAVIER PÉREZ JIMÉNEZ, por el privilegio de haber sido su alumno, por todos los conocimientos y experiencia transmitidos, invaluables en mi carrera profesional.

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, por haberme permitido formar parte de la máxima casa de estudios de nuestra nación.

A LA FACULTAD DE ESTUDIOS PROFESIONALES ACATLÁN, por haberme concedido el honor y el prestigio de haber cursado mis estudios en sus aulas.

Con particular afecto al PROFESOR JORGE J. ESTEVA VELASCO, por todo el apoyo recibido durante el desarrollo de mi carrera profesional.

AL LIC. VICTOR A. VIVEROS VILLA, por dar continuidad mediante su tutela y patrocinio, a mi formación profesional afuera de las aulas.

TÍTULO.

“ANÁLISIS JURÍDICO DEL DELITO DE ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA PREVISTO EN EL CAPÍTULO SEGUNDO DE EL TÍTULO NOVENO DE EL CÓDIGO PENAL FEDERAL”.

Í N D I C E.

Página.

Página.

CAPITULO III.- DELITOS INFORMÁTICOS.

CAPITULO IV.- EL DELITO DE ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA PREVISTO EN EL CAPÍTULO SEGUNDO DEL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL.

OBJETIVO.

El PRESENTE TRABAJO TIENE POR OBJETO ANALIZAR LA NATURALEZA JURÍDICA DE EL DELITO DE ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA PREVISTO EN EL CAPÍTULO SEGUNDO DE EL TÍTULO NOVENO DE EL CÓDIGO PENAL FEDERAL, DENTRO DE EL CONTEXTO DE EL DERECHO INFORMÁTICO Y EL DERECHO PENAL.

P R Ó L O G O.

El uso indebido de las computadoras y otros equipos de informática ha propiciado la aparición de nuevas conductas delictivas que comúnmente se han tratado de encuadrar en figuras típicas de carácter tradicional como el robo, el fraude, la falsificación o el sabotaje; sin embargo, recientemente fue reformado el Capitulo II del Título Noveno de el Código Penal Federal, mediante el cual se establece como delito el acceso ilícito a sistemas y equipos de informática, ya sea que estén protegidos por algún mecanismo de seguridad, o bien se consideren propiedad del Estado, de las instituciones que integran el Sistema Financiero o las corporaciones de Seguridad Pública del país, dando con este hecho origen a la necesidad de realizar un análisis jurídico detallado de esta figura, mismo que sirva como base de un estudio posterior.

Para tal efecto hemos divido el presente estudio en cuatro capítulos, tomando como punto de referencia en primer término al Derecho Informático, el cual constituye una rama del derecho de reciente desarrollo mediante la cual se trata de regular y agrupar en una única materia aquellos aspectos relacionados con la informática de los que derivan consecuencias jurídicas.

Así tenemos que en este primer capítulo pretendemos otorgar al lector una base teórica que sirva de introducción a la noción de Derecho Informático más actual, así como de sus aspectos más relevantes. Asimismo dentro del desarrollo de la investigación de éste capítulo se intento destacar la importancia económica y jurídica que puede llegar a poseer la información contenida en medios electrónicos y la creciente necesidad de regulación de su flujo por parte del derecho.

Por otra parte, debido a que el tema específico motivo del presente trabajo es el análisis de una figura delictiva en particular, en el segundo capítulo de este

proyecto se retomo el estudio de la teoría del delito, el cual consideramos constituye el pilar fundamental para el correcto análisis e interpretación de la ley penal sustantiva materia del presente estudio.

Así encontramos que el tercer capítulo del presente trabajo constituye un esfuerzo por integrar la doctrina penal tradicional a aquellas conductas ilícitas en las que inciden las nuevas tecnologías, dando como resultado el estudio de una nueva clase de ilícitos catalogados como “delitos informáticos”, a la cual consideramos pertenece el denominado “acceso ilícito a sistemas y equipos de informática”, objeto del presente análisis, siendo este estudio previo de los llamados delitos informáticos de especial relevancia, toda vez que constituye una categoría delictiva de la que actualmente no existe un estudio tan profuso como el que tenemos la posibilidad de encontrar en otras materias.

Dentro del cuarto capítulo de el presente trabajo nos dedicaremos al estudio particular de el delito de acceso ilícito a sistemas y equipos de informática, previsto en los artículos 211 bis-1 al 211 bis-7, presentes en el Capítulo II del Título Noveno del Libro Segundo del Código Penal Federal, comenzando por analizar las diversas conductas que integran el tipo penal, para continuar con un estudio detallado de los diversos conceptos que contiene como el requisito de que dichos sistemas ó equipos estén protegidos por algún mecanismo de seguridad, para lo cual trataremos de brindar un concepto general acerca de lo que podemos entender por sistemas y equipos de informática así como de los diversos mecanismos de seguridad que existen en la actualidad para la protección de la información que contienen estos equipos.

Por otra parte también se consideró relevante el análisis de los diversos sujetos pasivos en los que recae la dicha conducta, debido a que constituyen un factor que incide directamente en la penalidad.

CAPITULO I.- EL DERECHO INFORMÁTICO.

1.1 Orígenes del Derecho Informático.

1.2 Características y elementos del Derecho Informático.

1.3 El Derecho de la Información.

1.4 Regulación jurídica del Bien Informacional.

1.5 Principales características del Derecho Informático y la Informática Jurídica.

1.6 Desarrollo del Derecho Informático en el ámbito internacional actual.

1.7 Principales avances legislativos en México en materia de Derecho Informático.

CAPITULO I.- EL DERECHO INFORMÁTICO.

1.1 ORIGENES DEL DERECHO INFORMÁTICO.

Panorama actual de la informática.

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, a través del desarrollo de la informática; tecnología que de una manera muy general se define como la "creación, procesamiento, almacenamiento y transmisión de datos."[1]

Los progresos mundiales de los equipos informáticos, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips 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".

La informática esta hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se relacionan con los progresos tecnológicos, y comienzan a utilizar los sistemas de Información para ejecutar tareas que en otros tiempos se 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 de millones de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporados a sistemas informáticos

[1] http://www.definiciones.com.mx/definicion/I/informatica/

que, en la práctica cotidiana, de una forma muy sencilla y accesible, son capaces de recopilar y entregarnos una gran variedad de información que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre realizaba todo el trabajo y las máquinas existentes tenían la función limitada de imprimir los resultados.

Es por tales motivos que "la revolución tecnológica ha redimensionado las relaciones del hombre con los demás hombres, las relaciones entre el hombre y la naturaleza, así como las relaciones del ser humano con su contexto o marco de convivencia. Pero en el curso de estos últimos años pocas cuestiones han suscitado tan amplia y heterogénea inquietud como las referentes a las relaciones del hombre con las nuevas Tecnologías del la Información y la Comunicación (TIC)."[2]

La sociedad de la Información.

En la actualidad la evolución de los equipos de cómputo así como su abaratamiento han hecho posible que el fenómeno informático tenga un alcance mucho mayor en la población, lo que ha dado origen al término "sociedad de la información".

La sociedad de la información, es un nuevo término que hace referencia a "el ambiente donde la sociedad está inmersa que comprende el uso masivo de las Tecnologías de la Información y Comunicación (TIC) para difundir el conocimiento y los intercambios de información en una sociedad."[3]

Esta evolución de la sociedad en el uso de las TIC ha dado como resultado un enorme incremento en el volumen y manejo de los flujos de información entre los

[2] Pérez Luño, Antonio Enrique. *Ensayos de Informática Jurídica,* Distribuciones Fontamara S.A. de C.V. Primera Edición, México 1996. Pág. 7

[3] Téllez Valdés, Julio, *Derecho informático*. McGraw-Hill Interamericana, México, 2004. Pág. 6

diferentes sujetos de la sociedad, aumentando el número de equipos interconectados así como de las actividades de los usuarios, cambiando las exigencias y expectativas a las que deben responder los gobiernos, empresas, y la sociedad civil en general.

En este entorno la sociedad se desarrolla de nuevas formas y modifica las relaciones entre sus actores; la relación ciudadano – Estado, las relaciones empresariales, las actividades comerciales, la educación y la difusión del conocimiento, la labor de los medios de comunicación, e inclusive las relaciones personales de los propios individuos.

Un aspecto de la informática que ha jugado un papel fundamental en la evolución de las formas en las que se relacionan actualmente los seres humanos ha sido sin duda la expansión y masificación del acceso a Internet y el aumento en la variedad de servicios que están disponibles desde esta red.

El desarrollo del Internet y la creación del ciberespacio.

"Internet es un sistema de intercomunicación global, cuya tecnología permite vincular millones de computadoras entre sí, y acceder desde cualquier sitio del planeta a la información o servicios que se ofrezcan el ella desde cualquier lugar remoto".[4] Esta red permite el libre intercambio de información. Para lograr que sea posible intercambiar información entre diferentes computadoras ubicadas en distintas partes del mundo se utiliza un lenguaje común a todos los equipos interconectados que sirve como estándar. Este lenguaje o sistema de identificación se conoce como "protocolo de comunicación o protocolo de red"[5], y es lo que hace posible fundamentalmente el funcionamiento de Internet.

---

[4] Aboso, Gustavo, Zapata, María. *Cibercriminalidad y Derecho Penal.* Ed. B de F Ltda. Buenos Aires, 2006. Pág. 6

[5] http://es.wikipedia.org/wiki/Internet

*(FTP) File Transfer Protocol. *http://www.masadelante.com/faqs/ftp*

A su vez, este intercambio de información crea un universo virtual, diferente del universo físico conocido. Este espacio artificial o ciberespacio no tiene la localización fija, esto es, no se puede ubicar el lugar en donde se asienta.

Una de las características de este ciberespacio es que está formado por información contenida en medios electrónicos de almacenamiento y que estos medios de almacenamiento sí pertenecen al ámbito físico, por lo que en última instancia esa información esa ubicada en cierto lugar físico territorial, pero puede ser accedida desde cualquier parte del mundo.

Dentro del ciberespacio o del espacio virtual, es decir dentro de la red, existen diferentes métodos de comunicación, cada uno de ellos acorde con una finalidad. Así tenemos el correo electrónico que funciona como un correo tradicional, y el FTP* que funciona como el sistema de intercambio de libros de una biblioteca. Pero dentro de todos estos servicios existe uno que sobresale y que ha cobrado más fuerza que los demás y es el servicio denominado WEB, el cual consiste en una “página” en la que se coloca cierto tipo de información sobre algún tema en particular.

Importancia Jurídica del desarrollo del Internet.

El Internet en la actualidad no solo es utilizado como un vehículo de información, sino también para llevar a cabo diferentes actividades que producen diversos efectos jurídicos como lo son actos de comercio como compra-venta, contratos, el pago de contribuciones y servicios, operaciones bancarias, etc., lo que ha propiciado una revolución en el mundo entero, de ahí que sea comparado por algunos autores como el tercer movimiento de cambio de la humanidad, los dos primeros fueron el manejo de la agricultura y el segundo la revolución industrial; por ello se le ha considerado un prodigio para el desarrollo de un gran número de actividades del ser humano, todo esto disponible a través de corriente eléctrica y un equipo de cómputo personal de bajo costo, aunque actualmente hay

tantas innovaciones tecnológicas que el Internet fluye incluso a través del teléfono celular; sin embargo, el Internet también representa un gran reto y problema, ya que también ha sido utilizado cono vehículo para llevar a cabo conductas ilícitas que han propiciado en el menor de los daños intromisión a la privacidad de las comunicaciones y de las personas, causándoles en otras ocasiones graves daños en su patrimonio e incluso también ha dado pauta, a que individuos conformen bandas de delincuencia organizada que aprovechando el nivel de tecnificación del internet han llevado a cabo conductas delictivas muy difíciles de perseguir por las instituciones de impartición de justicia, asunto que ha tomado por sorpresa a muchos gobiernos como el nuestro, y que a pesar de los intentos por lograr un consenso entre los diversos países a fin de tipificar los delitos informáticos, este se ha dado a un ritmo muy lento en comparación con las actividades delictivas que día a día están presentando innovaciones y variantes, lo que ha propiciado que a los esfuerzos de los diversos Estados, se sumen incluso algunas veces acciones de instituciones particulares para tratar de agilizar y controlar mejor el flujo de la información y brindar seguridad a los usuarios, así como de protegerlos en la medida de lo posible de este tipo de conductas a través de mecanismos tecnológicos. Un ejemplo muy claro de lo anterior son los esfuerzos de las empresas e instituciones privadas por “blindar” sus sistemas de acceso a la información y así evitar fugas o desvíos de fondos, siendo las instituciones de crédito las que tradicionalmente han puesto especial énfasis en esa autoprotección de su información y la de sus clientes.

1.2 CARACTERÍSTICAS Y ELEMENTOS DEL DERECHO INFORMÁTICO.

El Derecho Informático.

Como ya se ha analizado con anterioridad el Derecho Informático nace como una rama jurídica de reciente desarrollo, que surge a consecuencia de los cambios sociales derivados de la evolución de la computación en general y su impacto dentro de la sociedad de la información. Así encontramos que, en el caso del Derecho Informático no hubo que transcurrir un largo periodo de gestación de los cambios sociales, sino que el cambio fue brusco y en poco tiempo, lográndose sociedades altamente dependientes de la informática, que sin la ayuda actual que ésta les brinda en todas sus actividades muy probablemente colapsarían.

En este orden de ideas, el Derecho Informático surge en una primera instancia como una relación interdisciplinaria entre diversas ramas del derecho tradicional que han atendido las problemáticas jurídicas que emanan de la implementación de nuevas tecnologías dentro de la sociedad de la información. Aunque el Derecho Informático tal vez no cuenta con tanta trayectoria y legislación que comprenden otras ramas del Derecho, si existe en el Derecho Informático doctrina basada en leyes, tratados y convenios internacionales, además de los distintos proyectos que se llevan a cabo en los entes legislativos de gran número de naciones, con la finalidad del control y aplicación lícita de los instrumentos informáticos.

Concepto de Derecho Informático.

Aunque todavía no existe un criterio uniforme mediante el cual se pueda conceptualizar con precisión al Derecho Informático, el maestro Javier Téllez Valdés lo define como “una rama de las ciencias jurídicas que considera a la informática como instrumento y objeto de estudio”.[6]

[6] Téllez Valdés, Julio, *Óp. Cit.* Pág. 17

Tenemos entonces que el Derecho Informático es una rama del derecho especializado en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales.

A su vez Julio Núñez Ponce establece que "El Derecho Informático es la aplicación del derecho a la informática, permitiendo que se adopten o creen soluciones jurídicas a los problemas que surgen en torno al fenómeno informático"[7].

En un sentido más amplio, Antonio Pérez Luño define al Derecho Informático como "el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones legales dirigidas a la regulación de las nuevas tecnologías de la Información y la Comunicación."[8]

Fuentes del Derecho Informático.

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

Asimismo en cuanto a la jurisprudencia, doctrina y literatura sobre el tema, existe ya toda una amplia variedad de teorías y artículos respecto a los problemas jurídicos suscitados por la informática.

[7] Núñez Ponce, Julio. *Nociones básicas del derecho de la Informática.* Ed. Tecnos, Madrid 1996. Pág.22
[8] Pérez Luño, Antonio. *Óp. Cit.* Pág. 12

Por otra parte, en cuanto a las fuentes interdisciplinarias existen aquellas provistas por ciencias y técnicas del conocimiento humano como la Contabilidad, Sociología, Economía, Estadística, Comunicación y desde luego la Informática.

Naturaleza Jurídica del Derecho Informático.

Existe actualmente un debate teórico acerca de la naturaleza jurídica del Derecho Informático que se basa fundamentalmente en el carácter interdisciplinario que lo distingue, ya que puede equipararse a un conjunto de normas dispersas pertenecientes a diferentes disciplinas jurídicas tradicionales, o bien como proponen diversos autores debe ser copilado como un conjunto unitario de normas, dirigidas a regular un objeto bien delimitado, enfocándose desde una metodología propia, constituyéndose así como una disciplina jurídica autónoma.

Desde sus inicios en la década de los ochentas, han surgido problemas a la hora de catalogar al Derecho Informático como rama jurídica autónoma del Derecho o simplemente si el Derecho Informático debe diluirse entre las distintas ramas del Derecho, asumiendo cada una de estas la parte que le corresponde.

Como un intento por establecer la naturaleza jurídica del Derecho Informático en América Latina, se celebró en 1998 en Montevideo, Uruguay, el “VI Congreso Iberoamericano de Derecho e Informática”, en donde diversos teóricos expusieron las razones por las cuales el Derecho Informático debiera ser considerado actualmente como una rama autónoma del Derecho. Desde aquel momento surgieron diferentes criterios, algunos afirmaban que el Derecho Informático nunca comprendería una rama autónoma del Derecho, debido a que dependía en su esencia de otras ramas del Derecho, mientras que otros catalogaban únicamente al Derecho Informático como una rama potencial del Derecho, debido a su insuficiente contenido y desarrollo. Asimismo originó una vertiente cada vez más amplia de estudiosos del Derecho que señalan la necesidad de ubicar al Derecho Informático como una rama autónoma del Derecho, debido a que no debe

considerarse por su propia naturaleza al Derecho Informático como una rama típica, pero sin embargo constituye conocimientos y estudios específicos que se encuentran entre la relación Derecho e Informática, y que claramente, aunque tal vez no tan desarrollada como otras ramas del Derecho, cuenta con una serie de conocimientos específicos del saber humano, el cual constituye un elemento que caracteriza a una rama del Derecho como autónoma.

Para hablar propiamente de la autonomía de una rama del derecho se necesitan ciertas características: “la existencia de campo normativo, docente, institucional y científico, con la finalidad de que se dé un tratamiento específico de estos conocimientos determinados”[9], por lo que, según el maestro Téllez Valdés, si existen condiciones para establecer la autonomía del Derecho Informático, ya que aunque si bien no cuenta con la existencia de un cuerpo normativo copilado por el legislador en un único compendio legal, sí existe un variedad de normas jurídicas como objeto particular de su estudio, además de ser creciente el número de instituciones académicas que la aceptan como tal y que incluso han modificado sus programas y planes de estudio para incluirlo en la como una asignatura independiente de las tradicionales áreas del Derecho.

Con respecto a las instituciones jurídicas que podemos mencionar como propias del Derecho Informático ya que no se encuentran en otras áreas del Derecho (campo institucional); se encuentra el contrato informático, el documento electrónico, el comercio electrónico, los delitos informáticos, la firma digital, la libertad informática, entre otras, que llevan a la necesidad de un estudio particular de la materia (campo docente), dando como resultado las investigaciones, y doctrinas que traten la materia (campo científico). En efecto, se pueden conseguir actualmente grandes cantidades de investigaciones, artículos, libros, e inclusive jurisprudencia referente al Derecho Informático, creando poco a poco sus propios

[9] Téllez Valdés, Julio, *Óp. Cit.* Pág. 17

principios e instituciones, como se ha constatado en los Congresos Iberoamericanos de Derecho e Informática.

Asimismo actualmente se implementan día a día centros de investigación que se dedican al estudio de la relación entre el Derecho y la Informática en todo el mundo.

Por lo tanto, ni siquiera en un país donde el grado de informatización sea bajo, hay inconvenientes para que surja la posibilidad de hablar del Derecho Informático como rama jurídica autónoma del Derecho, si bien podemos mencionar también, no sólo la integración de las normas jurídicas, sino también la heteroaplicación, cuando en un sistema jurídico existan vacíos legales al respecto, porque es de tomar en cuenta que ante el aumento de las ciencias jurídicas, el Derecho es un todo unitario, puesto que las normas jurídicas están estrechamente vinculadas entre sí ya sea por relaciones de coordinación o de subordinación, con lo que se concluye que para la solución de una controversia, se puede a través de la experiencia jurídica buscar su solución en la integración de normas constitucionales, administrativas, financieras, entre otros o llegar incluso a la aplicación de convenios o tratados internacionales.

El Derecho Informático como una rama de derecho público o privado.

Para analizar la naturaleza pública o privada del derecho informático comenzaremos por mencionar por un lado la estrecha y tan importante relación que existe entre el Derecho Informático y el Estado; en este punto tenemos por ejemplo su relación con el Derecho Constitucional dentro de la regulación del Derecho de Petición y el acceso a la información de la Administración Pública Federal, asimismo se inscriben en el ámbito del Derecho Público: El problema de la regulación del flujo internacional de datos informatizados, que interesa al derecho internacional público, la Libertad Informática, o defensa de las libertades frente a eventuales agresiones perpetradas por las tecnologías de la información y

la comunicación, objeto de especial atención por parte del Derecho Constitucional y Administrativo. Otro ejemplo es su relación con el Derecho Penal en el estudio de los delitos informáticos objeto del presente trabajo, por lo que considero que si es factible hablar de la existencia de el Derecho Informático Público; ó en otras palabras, el Derecho Informático de carácter Público.

Ahora bien, si tomamos en cuenta que el uso de la tecnología constituye la esencia de la necesidad jurídica de regulación que da origen al Derecho Informático, podemos considerar que de una u otra manera el Derecho Informático es tan amplio que necesariamente penetra en muchas más áreas del derecho, así como la Informática ha penetrado en todos los ámbitos. Por lo que también se puede hacer referencia al Derecho Informático Privado; es decir, al Derecho Informático de carácter Privado, ya que existen innumerables situaciones que son de carácter privado, como por ejemplo, los derechos de autor, el contrato electrónico, el comercio electrónico, etc., y así un sin número de figuras jurídicas pertenecientes al ámbito particular o privado.

Se concluye entonces, que la naturaleza jurídica del Derecho Informático, tomando en cuenta que éste constituye una rama atípica del Derecho y que nace como consecuencia del desarrollo e impacto que la tecnología tiene en la sociedad; así como la tecnología penetra en todos los sectores, tanto en el Derecho Público como en el privado, igualmente sucede con el Derecho Informático, éste penetra tanto en el sector público como en el sector privado, para dar soluciones a conflictos o planteamientos que se presenten en cualquiera de ellos.

1.3 DERECHO DE LA INFORMACIÓN.

La palabra “información”, proviene del latín *in-formare* (dar forma) es una noción abstracta, no obstante que posee una connotación vinculada a una de nuestras más grandes libertades: la opinión y expresión de informaciones e ideas por cualquier medio que sea[10] , por lo tanto podemos considerar a la información como cualquier conjunto de datos que los seres humanos hemos sido capaces de reconocer por medio de signos o combinación de signos, y que además, somos capaces también de transmitir por medio de procesos físicos o mecánicos.

Características de la Información.

La información a su vez, se diferencia de otros datos porque presenta las siguientes características:

A) *Clara e inteligible*. Esto se refiere a que el contenido de la información debe de estar dentro de las normas y la lógica de la comunicación, usadas de manera individual o socialmente.
B) *Relevante*. Significa que para que algo sea considerado información debe tener alguna importancia efectiva en el algún proceso de decisión en el que intervenga.
C) *Completa*. Quiere decir que la información debe de ser útil para el mayor rango de posibilidades que se presenten en la situación que se le requiera.
D) *Oportuna*. Que sea accesible en el momento que sea solicitada.
E) *Confiable.* Se dice que una información puede ser catalogada como confiable, cuando cumple los satisfactoriamente con todas las características anteriormente señaladas.

Clasificación de la Información.

De manera muy breve, comentaré también la clasificación más común de la cual ha sido objeto la información atendiendo esencialmente a los siguientes criterios:

[10] *Declaración Universal de los Derechos del Hombre,* París 1948, Art 19.

A) Según su contenido: Esto clasifica la información dependiendo de él área del conocimiento a la que se refiera su contenido: jurídica, médica, histórica, política, deportiva, etc.
B) Según su carácter cronológico: O sea el tiempo en el que fue emitida, pasada, presente, o futura.
C) Según sus fuentes: Puede ser oficial, privada, clandestina, confidencial, etc.
D) Según el fin para la que fue creada: Formativa, persuasiva, recreativa, etc.
E) Según el medio de su procesamiento: Manual, semiautomática, y automática. [11]

Importancia económica de la información.

En la actualidad, la información es valorada por sujetos e instituciones tanto del sector público como del privado, como un elemento fundamental para la toma de decisiones, llegando a ser equiparado inclusive como un factor de la producción, como lo son las materias primas o la energía, y puede ser en ocasiones tan relevante que de ella puede depender total o parcialmente el éxito de algún proyecto o empresa.

Por lo tanto podemos mencionar que la información posee una importancia de carácter económico en un sinnúmero de aspectos; por una parte permite planear y ejecutar planes y programas de desarrollo; tanto económicos, políticos o técnicos, sin la cual no existiría la posibilidad de conocer, transformar, corregir o planear.

Ahora bien si consideramos de esta forma a la información como un bien inmaterial susceptible de apropiación, con un inherente valor patrimonial, encontramos que la información reviste una gran trascendencia social, razón por la cual debe ser regulada en todos y cada uno de sus aspectos por el Derecho, debido a que da lugar a diversas obligaciones y derechos, que van desde la

[11] Téllez Valdés, Julio, *Óp. Cit.* Pág. 43

simple relación de propiedad entre autor e información, hasta la de la relación de transferencia entre emisores y receptores de información.

Derecho a la información.

En nuestro país encontramos que el derecho a la información está garantizado por parte del Estado como se establece en el artículo 6 de nuestra Carta Magna, el cual emana a su vez de la Declaración Universal de los Derechos del Hombre de 1948, y constituye un sustituto para derechos anteriormente existentes pero más restringidos, como lo son el derecho de expresión e imprenta, que resultaban insuficientes para abarcar y dar respuesta al complejo y creciente desarrollo de la información.

El derecho a la información comprende así, a todas las libertades informativas, pero aporta algo más, pues en un intento de respuesta global al proceso informativo, plantea el acceso y participación de los individuos y los grupos sociales en una corriente bilateral entre emisor y receptor en los términos de un fenómeno de interrelación, por lo que el derecho a la información , comprende un conjunto de tres facultades vinculadas entre sí como son, difundir, investigar y recibir información, todas ellas agrupadas en dos vertientes fundamentales: el derecho a informar, y el derecho a ser informado.[12]

El derecho a informar.

El derecho informar contiene a la libertad de expresión, la cual constituye la libertad de investigar y difundir, pero a su vez dicha libertad no es suficiente por sí misma para abarcar la totalidad del proceso informativo, ni los mecanismos jurídicos de protección que de ella emanan son suficientes para asegurar en la actualidad el flujo de la información de una manera libre e inclusive hasta democrática.

[12] Téllez Valdés, Julio, *Óp. Cit.* Pág. 47

El derecho a ser informado.

Este segundo aspecto se refiere básicamente al derecho que poseen los individuos de estar informados de los sucesos públicos relevantes y en general de todas las informaciones que pudieran afectar su existencia, con el objetivo de que puedan obtener un criterio objetivo de la situación y esto sea un factor que le permita contar con elementos suficientes para dirigir sus acciones y así sea capaz de interactuar con el medio en donde se desarrolla, como por ejemplo, participar en la vida política de su comunidad.

El derecho a no informar ó confidencialidad de datos personales.

Algunos autores consideran la existencia de un derecho de auto tutela de la identidad y la privacidad de los datos personales, en donde los individuos poseen el derecho de controlar (agregar, quitar, gestionar y conocer) los datos o información de carácter personal recabados o inscritos en cualquier base de datos pública o privada, debido principalmente a que dada la actual situación tecnológica propia de la sociedad contemporánea, todos los ciudadanos, desde su nacimiento, otorgan una gran variedad de datos personales diversos bancos de información o bases de datos lo cual da origen al riesgo de que esa información sea manipulada de tal forma que exponga a los individuos a abusos y violaciones de su intimidad.

En una sociedad como la que vivimos actualmente, en la que la información es poder, y en la que ese poder se torna decisivo cuando, por medio de la informática, las informaciones parciales y dispersas se convierten en informaciones masivas y organizadas, la reglamentación jurídica de la informática reviste un interés prioritario.[13]

[13] Pérez Luño, Antonio. *Óp. Cit.* Pág. 13

1.4 REGULACIÓN JURÍDICA DEL BIEN INFORMACIONAL.

Tutela jurídica del bien informacional.

Como ya hemos analizado en el apartado anterior la información es un producto de la actividad humana que puede poseer un carácter económico y a su vez puede también ser un bien susceptible de apropiación, partiendo desde su propio origen, es así como el autor que la hace disponible obtiene el derecho real sobre la misma para los diversos fines de la que pueda ser objeto. Tal es el caso por ejemplo de las obras artísticas, las cuales reconocen un derecho sobre su creador, lo que le otorga una protección privativa oponible frente a terceros conformando un derecho de propiedad intelectual. Por lo que podemos considerar que "los derechos sobre la información proceden de una operación intelectual de creación o formulación, aún así sean utilizados instrumentos de técnicos o tecnológicos como lo son hoy en día las computadoras para tal efecto".[14]

Por otra parte cabe mencionar que una vez creada la información pasa a formar parte de un cierto número de procesos más ó menos complejos dentro de los que se encuentran su transformación y explotación, convirtiéndola en muchos casos incluso en materia contractual, reafirmando por lo tanto, la necesidad de un control jurídico de la misma.

Así encontramos que en esencia el bien jurídicamente tutelado es la propiedad. Para continuar con este análisis podemos recordar la definición tradicional de patrimonio la cual nos dice que "se constituye como la suma de todos los valores pecuniarios de una persona", el cual incluye los bienes materiales e inmateriales, con la necesidad de que sean apreciables económicamente. Podemos incluir por ende entonces los derechos reales, la posesión, la tenencia, y los créditos.

[14] Fernández Delpech, Fernando. *Internet: su problemática jurídica.* Ed. Abeledo-Perrot. Argentina, 2001 pág. 124

Por lo tanto, en cuanto a los delitos cometidos contra la propiedad de la información, el ámbito y el alcance de tutela consiste en los intereses pecuniarios de carácter personal, es decir, es un modelo de protección a los derechos individuales, abarcando indirectamente la función social que cumple el patrimonio en la sociedad moderna.[15]

El problema fundamental que presenta el uso abusivo de computadoras y sistemas informáticos con la finalidad de cometer algún delito por medio de una manipulación malintencionada de la información, nace al contraponerlo al concepto clásico de propiedad, ya que se proyecta sobre el objeto inmaterial mediante el cual se basa el funcionamiento de estos sistemas. Así tenemos que debido a la naturaleza tecnológica de los medios de almacenamiento de datos que revisten los equipos informáticos, aunque el bien jurídicamente afectado sea la propiedad, el ámbito de esta se manifiesta en un plano virtualmente inmaterial. Por ejemplo, algunas formas por medio de las cuales los delincuentes logran afectar el patrimonio de las personas pueden darse por medio de la eliminación de un saldo favorable en una cuenta bancaria, el traspaso del dinero de una cuenta a otra, el uso fraudulento de una máquina para obtener dinero, el uso ilegitimo del servicio de un sistema de telecomunicaciones que finalmente genera un saldo negativo en la cuenta del usuario; son solamente algunos de los ejemplos que nos permiten demostrar que la mayoría de los delitos informáticos cometidos contra el patrimonio sin alterar físicamente la existencia de la cosa, cualidad que pasa a un segundo plano debido a las múltiples posibilidades que existen en la actualidad de afectar la propiedad ajena sin necesidad de involucrar dicha corporeidad.

Por lo tanto como ya hemos comentado con anterioridad es de especial relevancia el desarrollo del Derecho Informático como una rama de la ciencia jurídica, mediante el cual sea posible sancionar aquellas conductas que constituyan un medio para obtener ilegalmente beneficios o ventajas de la propia

[15] Aboso, Gustavo Eduardo. *Cibercriminalidad y Derecho Penal.* Ed. B de F. Argentina, 2006. Pág. 76

tecnología que ha inundado la vida cotidiana y económica tanto de personas físicas, así como de las actividades económicas y corporativas de las empresas, así como también sea capaz de proteger los movimientos de sectores clave como por ejemplo el de la Banca ó la información confidencial de las mismas autoridades, ya que desafortunadamente, estos avances tecnológicos ya son utilizados día a día para cometer delitos que en el mejor de los casos, ya están tipificados en ley o bien, cuando no; para ejecutar o concretar comportamientos ilícitos que afectan derechos ajenos y que permanecen impunes por no existir norma penal que los sancione en específico.

Un ejemplo común es cuando una persona tiene acceso remoto desde una computadora a información contenida en otro equipo por medio de alguna red (por ejemplo: internet) con el objetivo de modificar información que potencialmente pueda ocasionar daños a bases de datos, redes o servidores. Estas actividades pueden ser llevadas a cabo totalmente de una forma virtual, porque la información se encuentra en forma digital y el aunque ocasionan un daño real no tiene consecuencias físicas que puedan distinguirse tangiblemente sobre los daños causados sobre los ordenadores o servidores. Esto presenta un problema fundamental sobre todo en algunos sistemas judiciales que no admiten que la propiedad intangible pueda ser robada y requieren para su acreditación judicial que el daño deba ser visible. De manera personal considero que esta postura puede llegar a ser una limitante que debe ser superada, ya que sí lo analizamos desde otra perspectiva podemos encontrar que un ordenador o computadora puede ser incluido en un momento dado como una fuente de evidencia ya que aunque el ordenador no haya sido directamente utilizado para cometer el crimen, es un excelente artefacto que debido a su naturaleza tecnológica es capaz de guardar de manera automática todo tipo de registros y datos que incluyen desde información de la actividad del usuario, hasta detalles de sus comunicaciones y movimientos efectuados por medio de ese equipo, además de los archivos informáticos realizados por el usuario que pueda contener en su disco duro, lo cual brinda una confiabilidad muy notable que reside especialmente en su posibilidad

de codificar los datos. Esto ha hecho que los datos codificados de un ordenador o servidor actualmente ya tengan valor probatorio en varias Cortes alrededor del mundo.

Inviolabilidad de las comunicaciones privadas.

En el Diario Oficial de la Federación del 3 de julio de 1996, se publicó el decreto mediante el cual se declararon reformados los artículos 16, 20, fracción I y penúltimo párrafo, 22 y 73, fracción XXI, de la Constitución Política. Por lo que concierne al artículo 16, la reforma le adicionó dos párrafos, que pasan a ser el noveno y el décimo, por lo que también recorrió en orden progresivo los tres últimos párrafos.

La primera parte del párrafo noveno establece, como regla general, el carácter inviolable de cualquier tipo de comunicación privada, dentro de las cuales quedan incluidas las telefónicas y radiotelefónicas que se mencionan expresamente en la exposición de motivos. La inviolabilidad de las comunicaciones privadas forman parte del derecho a la intimidad o a la privacidad, que ya se encontraba implícito en el primer párrafo del artículo 16 de la Constitución, en cuanto prevé la inviolabilidad del domicilio y de la correspondencia; y que también ha sido incluido expresamente por los artículos 17 del Pacto Internacional de Derechos Civiles y Políticos, y el artículo 11 de la Convención Americana sobre Derecho Humanos. El primero de estos preceptos dispone: “Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación”. El artículo 11 de la Convención Americana es casi idéntico.

El mismo párrafo noveno del artículo 16 de nuestra Carta magna establece la posibilidad de que la autoridad Judicial Federal autorice la intervención de cualquier comunicación privada.

Esta autorización debería haber quedado prevista como una excepción frente a la regla general de la inviolabilidad de las comunicaciones privadas. Sin embargo, como hemos comentado ampliamente dentro de las aulas de nuestra facultad, la redacción del párrafo no resulta del todo precisa, pues no regula la autorización de la intervención como una verdadera excepción, sino como una muy amplia posibilidad sujeta a lo que dispongan las leyes ordinarias.

El párrafo noveno sólo indica que pueden solicitar la autorización:

1) la autoridad federal que faculte la ley, y

2) el titular del Ministerio Público de la entidad federativa correspondiente.

Inicialmente se estimó que por la amplitud de la redacción del párrafo, dentro de la expresión "autoridad federal que faculte la ley" pueden quedar no sólo los agentes del Ministerio Público Federal, sino prácticamente cualquier autoridad Federal, con la única condición de que la faculte la ley para tal fin, lo que se descartó con motivo de que es al Ministerio Público a quien corresponde la investigación y persecución de los delitos. La facultad para otorgar la autorización se atribuye exclusivamente a la "Autoridad Judicial Federal", es decir, a los órganos del Poder Judicial de la Federación.

En cuanto al tema del derecho a la no intromisión de las comunicaciones privadas Julio Núñez Ponce sostiene que: "las conductas y contenidos a restringir deben estar tipificadas legalmente, haciendo compatible las conductas sin valor con el mayor y más amplio de los respetos a la libertad de expresión y al derecho –hoy fundamental– de tener acceso a la información, con lo que a su juicio se pretende que el ciudadano visualice al Estado como aliado en la lucha contra los riesgos que sufren los beneficios de la expansión de la actividad informática y no como una amenaza a sus derechos a la intimidad y libertad."[16]

[16] Núñez Ponce, Óp. Cit. Pág. 36

1.5 PRINCIPALES CARACTERÍSTICAS DEL DERECHO INFORMÁTICO Y LA INFORMÁTICA JURÍDICA.

"El Derecho Informático es el sector normativo de los sistemas, dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telemática"[17]. Asimismo integran el Derecho Informático las proposiciones normativas, es decir, los razonamientos de los teóricos del Derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y la telemática. Las fuentes y estructura temática del Derecho Informático involucran varias de las ramas del Derecho tradicionales.

Por otra parte debido a la similitud de términos suele confundirse al Derecho Informático con la Informática Jurídica, la cual constituye una rama del mismo que estudia el tratamiento automatizado de: las fuentes del conocimiento jurídico a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (informática jurídica documental); las fuentes de producción jurídica, a través de la elaboración informática de los factores lógico-formales que concurren en el proceso legislativo y en la decisión judicial (informática jurídica decisional); y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho (informática jurídica de gestión).

Informática Jurídica Documental.

La Informática Jurídica Documental tiene por objeto la automatización de los sistemas de información relacionados con las fuentes del conocimiento jurídico como lo son la legislación, la jurisprudencia, y la doctrina. En la actualidad el adecuado acceso a los sistemas de documentación jurídica informatizada es una herramienta que optimiza el desempeño de los profesionales del Derecho.

Por su parte el maestro Pérez Luño considera que "el flujo incesante de leyes y decisiones jurisprudenciales, cuyo exacto y puntual es imprescindible para él

[17] Ídem, pág. 46

correcto funcionamiento del sistema jurídico, hace materialmente imposible su discernimiento, interpretación y aplicaciones por los operadores jurídicos"[18].

Podemos identificar entonces la existencia de una aglomeración de información y documentación en el Derecho de las sociedades tecnológicamente avanzadas, producida a su vez por volúmenes inmensos de legislación, jurisprudencia, y doctrina generada de forma masiva día con día, que solo puede ser, a su vez, contrarrestada con una respuesta en igual proporción por parte del sistema jurídico, a través del adecuado empleo de la tecnología informática y los sistemas de tele documentación. Solo así el jurista; y en concreto el abogado, se hallan en condiciones de tener un equilibrio entre el incesante flujo de datos jurídicos y su capacidad para asumirlos y aprovecharlos.

Informática Jurídica Decisional.

La informática jurídica meta-documental o decisional "se halla integrada por los procedimientos dirigidos a la sustitución o reproducción de las actividades del jurista; a proporcionarle decisiones o dictámenes, es decir a ofrecer soluciones de problemas y no mera información sobre problemas"[19]. Actualmente uno de los sectores más dinámicos y en constante evolución de la informática jurídica decisional es el que se refiere a la aplicación al Derecho de la Inteligencia Artificial (IA) y los denominados Sistemas Expertos (SE). La Inteligencia Artificial alude al conjunto de actividades informáticas que si fueran realizadas por el hombre se considerarían producto de su inteligencia[20]. La propia amplitud de estas operaciones abarca desde la comprensión de lenguajes naturales y el reconocimiento de imágenes y sonidos, hasta una amplia variedad de aplicaciones y simulaciones, las cuales han determinado una necesidad de acotar y delimitar su ámbito. A ello también ha contribuido la contradicción que supone predicar de entidades ajenas al hombre el rasgo humano por excelencia o sea la

[18] Pérez Luño, Óp. Cit. Pág. 42
[19] Ibídem. Pág.42
[20] "Inteligencia artificial." Microsoft® Student 2009 [DVD]. Microsoft Corporation, 2008.

inteligencia.[21] De ahí que hoy se aluda preferentemente a lo que es el sector más importante de la inteligencia artificial el que se refiere a los Sistemas Expertos.

Tales sistemas incorporan, de una manera práctica y operativa, el conocimiento que posee un experto en la materia que se trate. Consisten en programas que reproducen las actuaciones que ha previsto el programador que los diseña, utilizando los conocimientos y las reglas analíticas definidas por los expertos en dicho campo. Los expertos solucionan los problemas utilizando una combinación de conocimientos basados en hechos y en su capacidad de razonamiento.[22]

Entre los sistemas expertos más notorios de nuestros días se encuentran los dirigidos al diseño artístico o arquitectónico, la localización de yacimientos minerales y el diagnostico médico. Actualmente el Derecho no ha sido la excepción en cuanto a la aplicación práctica de esta tecnología ya que también han proliferado en estos años una serie de proyectos y prototipos de sistemas expertos jurídicos en materias tales como:

A) Liquidaciones tributarias
B) Cálculo de indemnizaciones por accidentes laborales o de tránsito,
C) Predicción de las consecuencias jurídicas de impactos medioambientales,
D) Condiciones de adquisición de la nacionalidad y derechos de familia, etc.

Estos sistemas pueden prestar un importante servicio al abogado al informarle sobre la normativa aplicable a determinados supuestos, así como las consecuencias jurídicas derivadas de aplicar dicha normativa a situaciones de ese tipo. No obstante, en la medida en la que las máquinas pueden procesar informaciones y establecer diferencia lógicas pero no pueden comprender la multiplicidad de circunstancias que concurren en las conductas humanas, debemos mencionar también que en la actualidad aún no es posible, de ninguna

[21] Téllez Valdés, Óp. Cit. Pág. 24
[22] “Sistema experto." Microsoft® Student 2009 [DVD]. Microsoft Corporation, 2008

forma; la existencia de una substitución plena del razonamiento jurídico del juez o abogado por el cálculo informático de las computadoras. “Solo en aspectos de la experiencia jurídica rutinarios, estandarizados, formalizables, con variables predeterminadas cerradas; es posible recurrir a sistemas expertos capaces de ofrecer soluciones operativas”.[23] Pero incluso en estos casos el juez o el abogado no pueden someter su decisión o su dictamen para delegarla en el ordenador.

Informática Jurídica de Gestión.

Otro de los sectores que han registrado un amplio desarrollo en los últimos años es el que se refiere a la Informática Jurídica de Gestión, la cual se refiere a todos los avances orientados a la automatización de las tareas rutinarias que se llevan a cabo en cualquier oficina (ofimática) y por tanto, también en las oficinas o despachos jurídicos. Se trata de la realización de soportes informáticos de operaciones destinadas a recibir y transmitir comunicaciones de cualquier tipo, de leer y escribir textos, de formar y organizar y actualizar archivos y registros, exigir y recibir pagos, estipular condiciones y controlar su cumplimiento[24]. Los avances de la ofimática permiten con respecto a la gestión de la justicia y la abogacía, automatizar todas aquellas operaciones estandarizadas que obedecen a pautas regulares y constantes por ejemplo en la escritura, el registro, la transcripción, la contabilidad, la documentación, la comunicación y la certificación. Gracias a la gestión automatizada implementada en las oficinas del Poder Judicial y los despachos jurídicos de los juristas se tienden a lograr resultados más uniformes, imparciales, transparentes, rápidos y económicos. Esto se debe principalmente a que el uso de estas herramientas tecnológicas permite a su vez que la actividad de los profesionales del Derecho por ejemplo el Juez o el abogado, puedan dedicarse así de manera exclusiva, a labores que exijan una actividad creativa, o que precisen de una iniciativa personal, o deban ser decididos con un criterio muy particular.

[23] Pérez Luño, Óp. Cit. Pág. 43
[24] Ibídem. Pág. 43

1.6 DESARROLLO DEL DERECHO INFORMÁTICO EN EL ÁMBITO INTERNACIONAL ACTUAL.

Un análisis de las legislaciones en materia de Derecho Informático que existen en la actualidad en diversos países nos muestra 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 la comisión de dichas conductas.

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En la mayoría de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma de preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.[25]

El desarrollo del Derecho Informático en nuestro país tiene alrededor de escasos diez años; sin embargo, en los Estados Unidos de Norteamérica, la primera propuesta formal de legislar con este respecto, fue presentada por el senador A. Ribicoff, ante el Congreso Federal de esa nación en el año de 1977.[26]

Años después, en 1983 en París, la OCDE* designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en los códigos penales. El dictamen de esta organización, recomendó a los países miembros la modificación de su legislación penal, de forma que se integraran los nuevos delitos informáticos.

---

[25] Núñez Ponce, Óp. Cit. Pág. 42
[26] Téllez Valdés, Óp. Cit. Pág. 28
* (OCDE) Organización para la Cooperación y el Desarrollo Económico.

En 1989, el Consejo de Europa convocó a otro comité de expertos, que en la Recomendación emitida el 13 de septiembre de ese año, presentaron una lista mínima de los delitos que debían necesariamente agregarse a las legislaciones de cada país miembro, junto con una lista opcional.

También se llegó a discutir sobre estos temas en el "*Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado de Montreal en 1990*", en el "*Octavo Congreso Criminal de las Naciones Unidas*" celebrado en el mismo año, y en la "*Conferencia de Wurzburgo*", en Alemania, en 1992.

En 1996, se estableció por el "*Comité Europeo para los Problemas de la Delincuencia*", un nuevo comité de expertos para que abordaran el tema de los delitos informáticos.

Con el fin de combatir los delitos informáticos, sobre todo los cometidos a través de las redes de telecomunicaciones, en Internet, como pueden ser las transacciones de fondos ilegales, la oferta de servicios ilegales, la violación de los derechos de autor, así como también los delitos que violan la dignidad humana y la protección de los menores, se encargó la tarea de elaborar un borrador del instrumento legal obligatorio al recién formado "*Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras".*

El veintitrés de noviembre de dos mil uno, el Consejo de Ministros de Europa, compuesto por los ministros del interior de los estados que conforman la Unión Europea, conjuntamente con Estados Unidos, Sudáfrica, Canadá y Japón, firmaron en Budapest, la "*Convención sobre Delitos Informáticos*", cuyos objetivos fundamentales fueron los siguientes:[27]

1. Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático.

[27] Cassou Ruiz, Jorge Esteban. "Delitos Informáticos en México". *Revista de Derecho Informático*, núm. 028, Consejo de la Judicatura Federal, México, Septiembre de 2006.

2. Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas, y
3. Establecer un régimen dinámico y efectivo de cooperación internacional.

Asimismo de forma unilateral varios países desarrollados alrededor del mundo sostienen diversos progresos en materia de Derecho Informático como son los siguientes:[28]

Alemania.

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

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

Austria.

Recientemente se promulgo en este país la *"Ley de reforma del Código Penal"*, la cual sanciona en el artículo 148 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". Además contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

Gran Bretaña.

Debido a un caso de hacking* en 1991, comenzó a regir en este país la *"Computer Misuse Act*" (Ley de Abusos Informáticos), mediante esta ley el intento, exitoso o

[28] Ídem, pág. 24

* (Hacking) Actividad de ingresar a un sistema informático con el fin de eludir o desactivar las medidas de seguridad del mismo. http:// www.wikipedia.org.hacker.mht

no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene también un apartado que específica 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.

Holanda.

En este país entró en vigencia El 1º de Marzo de 1993 la *"Ley de Delitos Informáticos"*, en la cual se penaliza el *hacking* (acceso no autorizado a un sistema o base de datos), el *phreaking* (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*. Cabe destacar que en el ordenamiento en comento la distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño de forma intencional ya que 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.

Francia.

En enero de 1988, este país emitió la *"Ley relativa al fraude Informático"*, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta ley establece en su artículo 462-3 "una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos". Por su parte el artículo 462-4 también incluye en su tipo penal "una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión".

También la legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena "cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema" (sabotaje).

Por último, esta ley en su artículo 462-2, sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente "si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema".

España.

En el "*Nuevo Código Penal de España"*, se establece el art. 263 que "el que causare daños en propiedad ajena, se aplicará la pena de prisión de uno a tres años y multa... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe 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 delictiva (*Violación de secretos, Espionaje y Divulgación*), aplicando pena de prisión y multa, agravándolas cuando existe una intensión dolosa, y cuando el hecho es cometido por parte funcionarios públicos; se penaliza con inhabilitación.

En materia de "*estafas electrónicas"*, el nuevo Código Penal de España, en su artículo 248, 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.

1.7 PRINCIPALES AVANCES LEGISLATIVOS EN MÉXICO EN MATERIA DE DERECHO INFORMÁTICO.

Constituyen en nuestro sistema jurídico, el principal avance en materia de Derecho Informático, las reformas que se realizaron al Código Penal Federal, publicadas en el Diario Oficial de la Federación el diecisiete de mayo de mil novecientos noventa y nueve.

Así tenemos que en la actualidad en México existen los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática; ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero, hechos que son sancionables por el *Código Penal Federal* en el titulo noveno capítulo I y II.

Asimismo el artículo 167 fr.VI del *Código Penal Federal* sanciona también con prisión y multa al que “dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos”.

Por otro lado tenemos un avance legislativo importante en lo que respecta a la “reproducción no autorizada de programas informáticos o piratería”, la cual está regulada actualmente en el Título IV, de la *Ley Federal del Derecho de Autor.*

Por su parte la *Ley de Instituciones de Crédito* en mayo de 1999 en su artículo 112 bis, incorporó algunas normas más o menos similares a las contenidas en el artículo 240 bis del Código Penal, por cuanto hace a la fabricación de instrumentos de pago (cheques, tarjetas de crédito) o su comercio ilícito. En la misma disposición se añaden dos fracciones que versan sobre un uso indebido de medios informáticos a través de dos supuestos:

A) Primero: Alterar el medio de identificación electrónica y acceder a los equipos electromagnéticos del sistema bancario con el propósito de disponer indebidamente de recursos económicos.

B) Segundo: Obtener o usar indebidamente información sobre clientes u operaciones del Sistema Bancario sin contar con autorización. La pena que se fija es prisión de 3 a 9 años y multa 30,000 a 300,000 días de salario mínimo, con una calificativa del 50% más si es consejero, funcionario o empleado de la institución.

También existen actualmente diversos proyectos para modificar leyes locales como el *Código Penal del Distrito Federal*, y algunos como el *Código Penal del Estado de Sinaloa,* el cual desde agosto de 2006 cuenta con un capítulo exclusivo para los delitos informáticos, el cual constituye el más emprendedor avance legislativo local en materia de este tipo de ilícito en nuestro país, brindando inclusive, en su artículo 217, un intento por establecer una definición de delito informático, mismo que analizaremos más adelante en el presente trabajo.

CAPITULO II.- LA TEORIA DEL DELITO

2.1 Concepto de delito y clasificación.

2.2 La Conducta y su ausencia.

2.3 Omisión y comisión por omisión.

2.4 El Tipo penal y la ausencia del tipo.

2.5 Antijuricidad y causas de licitud.

2.6 Imputabilidad y causas de inimputabilidad.

2.7 Culpabilidad y causas de inculpabilidad.

2.8 Condiciones objetivas de punibilidad, falta de condiciones objetivas de punibilidad.

2.9 Tentativa.

2.10 Concurso de delitos.

2.11 Autoría y participación penal

CAPÍTULO II.- LA TEORIA DEL DELITO.

2.1 CONCEPTO DE DELITO Y CLASIFICACIÓN.

Concepto de delito.

Para iniciar un estudio del delito, comenzaré por recordar que desde los orígenes del derecho, el hombre ha regulado su conducta a través de las normas, y éstas han sido clasificadas en:

a) Éticas

b) Morales

c) Sociales

d) Naturales

e) Jurídicas.

Hablando de las normas jurídicas y del derecho como tal, encontramos el derecho penal que es el que precisamente se encarga de salvaguardar el orden social y puede definirse brevemente como el "conjunto de normas jurídicas promulgadas por el Estado para castigar los delitos e imponer las penas y medidas de seguridad a los infractores de éste".[29]

Por otra parte, antes de comenzar con el concepto de delito, debemos mencionar que la palabra delito se deriva del vocablo latino *Delinquere*, que significa "abandonar o apartarse del buen camino, alejarse del sendero señalado por la Ley."[30]

[29] Instituto de Investigaciones Jurídicas. *Diccionario Jurídico Mexicano*. Editorial Porrúa, S.A., Octava Edición, México 1995. Pág. 262

[30] Nicoltello, Nelson. *Diccionario del Latín Jurídico.* Julio César Faira, Editor. Argentina, 2004. Pág. 220

El diccionario jurídico mexicano refiere al concepto formal del delito de la siguiente forma: “En derecho penal, acción u omisión ilícita y culpable expresamente descrita por la ley bajo la amenaza de una pena o sanción criminal”.[31]

Por su parte, Jiménez de Asúa nos dice que: “el delito es el acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal”.[32]

El maestro Cuello Calón, tomando en cuenta el aspecto formal, ha definido al delito como: “la acción prohibida por la Ley bajo la amenaza de una pena”.[33]

Asimismo también podemos encontrar el concepto de delito definido por nuestra legislación penal vigente:

El Código Penal para el Estado de México, contempla la definición del delito en su artículo 6, de la forma siguiente:

LIBRO PRIMERO

TITULO SEGUNDO

DELITO Y RESPONSABILIDAD

CAPITULO I

EL DELITO Y SUS CLASES

---

[31] Instituto de Investigaciones Jurídicas. Óp. Cit. Pág. 865

[32] Jiménez de Asúa, Luis. *La Ley y el Delito*. Editorial Sudamericana, décimo segunda edición, Argentina 1981. Pág. 206.

[33] Cuello Calón, Eugenio. *Derecho Penal*, Editorial Nacional, novena edición, México, 1961. Pág. 289.

Artículo 6.- El delito es la conducta típica, antijurídica, culpable y punible.

Así tenemos que el delito es esencialmente una conducta, activa u omisiva, cuyas consecuencias se conminan con la imposición de la pena, pero para llegar a tal aplicación deben existir los elementos tradicionales del delito.

Con relación a este aspecto encontramos que el Maestro López Betancourt nos menciona que: “La aportación de diversos estudiosos de nuestra ciencia ha traído en número de siete los elementos del delito y su respectivo aspecto negativo. Es decir, a partir de la disposición de todos y cada uno de los predicados de la conducta o hecho, se estudia al delito en dos esferas; una referente a la existencia e inexistencia del hecho delictivo (aspectos positivos y negativos), otra relativa a las formas de aparición (a la vida del delito)”.

En la primera esfera a cada aspecto positivo le corresponde su respectivo negativo en la forma en que a continuación se exponen. Cabe mencionar que cuando se trate del primero (aspecto positivo), estaremos ante la existencia del delito; y cuando se trate del segundo, de su inexistencia.

Por otro lado, según el número de elementos que se acepten para la formación del mismo, podemos ubicarlo dentro de la teoría atomizadora, en una postura que va desde la dicotómica o biatómica, hasta la heptatómica, pasando por la triédrica, tetratómica, pentatómica y hexatómica.

De esta forma la segunda esfera se conforma por:

1.- El iter criminis o camino del delito.

2.- El concurso de delitos.

3.- La participación criminal."[34]

Haciendo un estudio breve de la primera esfera, podemos mencionar que dichos elementos de acuerdo a la doctrina tradicional, se ubican de acuerdo con el siguiente esquema:

	Aspectos Positivos	Aspectos Negativos
1)	Acto, acción o conducta	Falta de acción o Conducta
2)	Tipicidad	Ausencia de tipo o Atipicidad
3)	Antijuricidad	Causas de justificación
4)	Imputabilidad	Causas de inimputabilidad
5)	Culpabilidad	Causas de Inculpabilidad
6)	Condicionalidad objetiva	Falta de Condición Objetiva
7)	Punibilidad	Excusas absolutorias.

Así tenemos que para poder definir el delito desde el punto de vista jurídico formal, tenemos que remitirnos a las conductas típicas que traen como resultado una penalidad. Es decir, que la propia ley amenaza imponiendo alguna pena a la acción u omisión llevada a cabo por el individuo, siempre y cuando con esa conducta se comprometan los valores jurídicos protegidos por la propia ley, otorgándoles así la forma de delitos.

[34] López Betancourt, Eduardo. *Teoría del Delito*. Editorial Porrúa, S.A. décima edición, México 2002. Págs. 65 y 66.

Clasificación del delito.

Es importante mencionar la enorme la existencia de una gran variedad de criterios de clasificación del delito, por lo que en este estudio nos limitaremos a aportar lo que consideramos las clasificaciones más aceptadas por la Doctrina:

DELITOS DE ACCION: que son los que se cometen mediante un comportamiento positivo. Porte Petit hace referencia a dos delitos de acción, cuando la conducta se manifiesta a través de un movimiento corporal o conjunto de movimientos corporales. Ambos coinciden en ser conducto o comportamiento orientados a un "hacer". En los delitos de acción se contraviene una norma prohibitiva, ya que el sujeto realiza algo que la norma prohíbe hacer.

DELITOS DE OMISION. Según Pavón Vasconcelos son: "aquellos en los cuales la conducta constituye una inactividad, es decir, un no hacer de carácter voluntario".[35] La omisión puede ser material o espiritual, la primera da lugar a los delitos de simple omisión (propios delitos de omisión) y a los de comisión por omisión (impropios delitos de omisión), y la segunda da lugar a los especialmente llamados así.

Asimismo Fernando Castellanos Tena establece en su obra, que los delitos de omisión materiales se subdividen en:

DELITOS DE SIMPLE OMISION (Verdadero delito de omisión): siendo estos los que esencialmente consisten en una falta de una actividad jurídicamente establecida, con AUTONOMÍA del resultado material que produzcan. Encontramos un ejemplo cuando la ley castiga al que requerido por las autoridades, no de

[35]Pavón Vasconcelos, Francisco. Manual de Derecho Penal Mexicano, Editorial Porrúa, S.A. sexta edición. México 1984. Pág. 224.

auxilio para la averiguación previa de los delitos o para la persecución de los delincuentes; y

DELITOS DE COMISION POR OMISION (Falsos delitos de omisión, impropios): son aquellos en los que el sujeto decide no actuar, y por esa inacción se provoca el resultado material. En este tipo de delitos el resultado se produce como consecuencia de la omisión del movimiento corporal y llega a un resultado prohibitivo, por ejemplo, la madre que no alimenta a su hijo recién nacido para causarle la muerte, esto es, mediante un no hacer u omisión de la acción, en cuyo caso hay violación de dos normas: una preceptiva y otra prohibitiva.

A su vez, Cuello Calón señala que los delitos de omisión: "consisten en la aparición de un resultado delictivo de carácter positivo, por inactividad".[36]

Otra clasificación que encontramos del delito atiende al RESULTADO que éste produce. Así tenemos que bajo este criterio los delitos pueden clasificarse en:

FORMALES: siendo éstos en los que se agota el tipo penal en el movimiento corporal o en la omisión del agente, sin que sea preciso para su integración la producción de un resultado exterior; y

MATERIALES: que son aquellos en los cuales para su integración resulta necesario la producción de un resultado objetivo o material (homicidio, robo, etc.)

Para Cuello Calón los delitos también se clasifican de la siguiente manera, según los siguientes aspectos:

[36] Cuello Calón, Eugenio. Óp. Cit. Pág. 274.

“Por el DAÑO que causan, dividiéndose en:

DELITOS DE LESION: siendo éstos los que consumados causan un daño directo o efectivo en intereses jurídicamente tutelados por la norma violada.

DELITOS DE PELIGRO a los que el mismo Cuello Calón alude como: “aquellos cuyo hecho constitutivo no causa un daño efectivo y directo en intereses jurídicamente tutelados, pero crean para éstos una situación de peligro, entendiéndose por éste, como la posibilidad de la producción más o menos próxima de un efecto perjudicial”.[37]

Por otra parte, podemos clasificar al delito tomando en cuenta el factor de su DURACION, por lo que pueden ser:

INSTANTÁNEOS: Siendo estos los que se establecen por la acción que los consuma, es decir que se perfecciona en un solo momento.

INSTANTANEOS CON EFECTOS PERMANENTES: son aquellos cuya conducta destruye o disminuye el bien jurídico tutelado en forma instantánea pero subsisten las consecuencias perjudiciales del mismo.

CONTINUADOS, en este tipo de delitos, se llevan a cabo varias acciones delictivas que producen a su vez una sola lesión jurídica.

[37] Ibídem. Óp. Cit. Pág. 289.

PERMANENTES. Son aquellos dentro de los cuales persiste el efecto del delito y el estado mismo de la consumación, como es el caso del, secuestro, etc.

A su vez, nuestra legislación vigente también nos otorga una clasificación formal del delito como podemos nos establece el *Código Penal para el Estado de México,* de acuerdo a los siguientes artículos:

LIBRO PRIMERO

TITULO SEGUNDO

DELITO Y RESPONSABILIDAD

CAPITULO I

EL DELITO Y SUS CLASES.

Artículo 7.- Los delitos pueden ser realizados por acción y por omisión.

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

Artículo 8.- Los delitos pueden ser:

I. Dolosos;

El delito es doloso cuando se obra conociendo los elementos del tipo penal o previendo como posible el resultado típico queriendo o aceptando la realización del hecho descrito por la ley.

II. Culposos;

El delito es culposo cuando se produce un resultado típico que no se previó siendo previsible o confiando 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.

III. Instantáneos;

Es instantáneo, cuando la consumación se agota en el mismo momento en que se han realizado todos sus elementos constitutivos.

IV. Permanentes;

Es permanente, cuando la consumación se prolonga en el tiempo.

V. Continuados.

Es continuado, cuando existe unidad de propósito delictivo, pluralidad de conductas e identidad de sujeto pasivo y se viola el mismo precepto legal.

Por otro lado, tenemos también que el delito puede clasificarse de acuerdo con el ELEMENTO INTERNO O CULPABILIDAD:

Estos se subdividen en: DOLOSOS, CULPOSOS y algunos agregan a los DELITOS PRETERINTENCIONALES.

DOLOSO: cuando se obra con conocimiento de los elementos del tipo penal o previendo como posible el resultado típico pretendiendo o aceptando la ejecución del hecho descrito por la ley.

CULPOSO: cuando se causa un resultado típico que no se previó siendo previsible o confiando en que no se produciría, en virtud de la desobediencia a un

deber de cuidado, que debía y era posible observarse según las circunstancias y condiciones personales.

El Delito PRETERINTENCIONAL es cuando se causa un daño que va más allá de la intención y que no ha sido previsto ni deseado, siempre y cuando el medio empleado no sea el idóneo para producir el resultado. Como ejemplo de este tipo de delito, tenemos cuando alguien golpea a otro con la sola intención de golpearlo, pero éste al caer se golpea la cabeza y muere.

En función de su COMPOSICION O ESTRUCTURA:

SIMPLES: siendo aquellos en los cuales la lesión jurídica es única, por ejemplo el homicidio; y

COMPLEJOS: que son aquellos en los cuales la figura jurídica consta de la unificación de dos violaciones, cuya fusión da nacimiento a una figura delictiva nueva, superior en gravedad a las que la componen, tomadas aisladamente. Tenemos de esta manera que un ejemplo clásico de estos delitos lo constituye el caso del robo cometido en casa habitada.

POR EL NÚMERO DE ACTOS INTEGRANTES DE LA ACCION TIPICA: subdividiéndose en:

UNISUBSISTENTES: cuando la acción se agota en un solo acto. Por ejemplo en el caso de la disposición en el abuso de confianza, la cual integra la acción, siendo esta disposición un acto único.

PLURISUBSISTENTES: que son cuando la acción demanda, para su agotamiento, de varios actos.

Sebastián Soler, establece la diferencia entre el delito plurisubsistente del complejo, pues en el primero cada uno de los actos integrantes de una sola figura no constituye, a su vez, un delito autónomo.

Por otra parte también podemos clasificar al delito atendiendo a la UNIDAD O PLURALIDAD DE SUJETOS QUE INTERVIENEN PARA EJECUTAR EL HECHO DESCRITO EN EL TIPO dividiéndose para tal efecto en:

UNISUBJETIVOS: cuando basta la actuación de un solo sujeto cuya conducta sea acorde a la descripción legal.

PLURISUBJETIVOS: cuando se requiere forzosamente de la concurrencia de dos o más conductas para integrar el tipo, siendo un ejemplo de éstos el delito de asociación delictuosa.

También encontramos que POR LA FORMA DE SU PERSECUCION, los delitos pueden ser:

PRIVADOS o de QUERELLA NECESARIA, cuya persecución sólo es factible si se cumple con el requisito previo de la parte ofendida; y

PERSEGUIBLES de OFICIO que son todos aquellos en los que la autoridad está obligada y facultada para actuar por mandato legal, persiguiendo y castigando a los responsables, con independencia de la voluntad de los ofendidos.

Podemos también clasificar al delito EN FUNCION DE LA MATERIA de la que se trate, y ésta se compone en:

DELITOS COMUNES: siendo estos los que se formulan en leyes dictadas por las legislaturas locales.

DELITOS FEDERALES: siendo aquellos que se constituyen en leyes expedidas por el Congreso de la Unión.

DELITOS OFICIALES que son los que realiza un empleado o funcionario público en ejercicio de sus funciones, incluyendo inclusive a los altos funcionarios de la Federación.

DELITOS DEL ORDEN MILITAR: siendo estos los que afectan la disciplina del Ejército y las Fuerzas Armadas de nuestro país.

DELITOS POLÍTICOS: Son aquellos cometidos contra la seguridad del Estado, ya que él mismo tiene una organización política como forma y tiene que protegerla, prohibiendo y condenando como delito político, todo acto que la desconozca en sí misma o en sus órganos o representantes y tienda a alterar o imponer determinados regímenes o determinadas personas por medio del uso de la violencia, el fraude o en otras formas no autorizadas por la ley.

2.2 LA CONDUCTA Y SU AUSENCIA.

LA ACCION O CONDUCTA. Este término constituye de acuerdo a la Doctrina, en su acepción más amplia, el movimiento corporal externo y voluntario, así como el no hacer, o inactividad voluntaria.

De esta forma el maestro Luis Jiménez de Asúa, establece: "que es la manifestación de voluntad que, mediante acción, produce un cambio en el mundo exterior o que por no hacer lo que se espera, deja sin mudanza ese mundo externo cuya modificación se aguarda. Dicho esto de otra manera, es la manifestación de voluntad que por medio de acción u omisión, causa un cambio en el mundo exterior".[38]

Fernando Castellanos Tena adopta el concepto de conducta, pues señala: "Dentro de él se puede incluir cabalmente tanto el hacer positivo como el negativo y, al efecto, apunta su concepto de conducta como el comportamiento humano voluntario, positivo o negativo encaminado a un propósito".[39]

Para el maestro Eugenio Cuello Calón, "la acción es la conducta exterior voluntaria encaminada a la producción de un resultado".[40]

Por su parte Raúl Carrancá y Trujillo opina que "la conducta es un hecho material, exterior, positivo o negativo, producido por el hombre".[41]

---

[38] Jiménez de Asúa, Luis. Óp. Cit. Pág. 227

[39] Castellanos Tena, Fernando. *Lineamientos Elementales de Derecho Penal, Parte General*. Ed. Porrúa, S.A. trigésima quinta edición, México 1994. Pág. 149.

[40] Cuello Calón, Eugenio. Óp. Cit. Pág. 319.

[41] Carrancá y Trujillo, Raúl. *Derecho Penal Mexicano, Parte General*. Ed. Porrúa, S.A. tercera edición, México 1996. Pág. 126.

Aunque hay diferencias en las expresiones utilizadas por los autores, todos coinciden en que se trata de una acción propiamente dicha y de una omisión integrados en un solo vocablo, llámese acción, conducta, actividad o manifestación de voluntad, etc., por lo tanto, podemos concluir que todos los autores determinan que la acción como forma de conducta es el primer elemento del delito.

En resumen el primer carácter del delito es ser un acto. Acto supone la existencia de un ser dotado de voluntad que lo ejecuta. Este acto no es otra cosa sino una conducta humana voluntaria que produce un resultado, ya que esta conducta debe ser voluntaria, dicho de otra forma, sin voluntad no hay conducta; el Derecho no regula hechos en general, sino sólo la conducta humana.[42]

De esta forma podemos concluir que la conducta es el primer elemento básico del delito, precisando a la conducta para tal efecto como el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito. Esto debido fundamentalmente a que sólo los seres humanos pueden cometer conductas positivas o negativas, ya sea una actividad o inactividad respectivamente. Afirmamos que es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito, y porque tiene una finalidad al realizarse la acción u omisión. Dentro del concepto de conducta pueden comprenderse la acción y la omisión; es decir, el hacer positivo y el negativo; el actuar y el abstenerse de obrar.

[42] Castellanos Tena, óp. Cit. Pág. 149.

2.3 OMISIÓN Y COMISIÓN POR OMISIÓN.

"La acción radica en un acto de voluntad, su exteriorización por medio de un hacer o mediante inactividad, y el resultado será la modificación producida en el mundo exterior o el peligro creado con dicha conducta. De lo que se desprende el nexo causal entre la acción y el resultado.

En sentido estricto consiste en un movimiento corporal voluntario orientado a la producción de un resultado, consistente en la alteración del mundo exterior o en peligro de que se produzca. La acción (como hacer activo) exige además de voluntad en el agente, una actividad corporal. Nuestro Derecho Positivo Mexicano se ocupa de estos actos y debemos entender la acción en sentido amplio, percibiéndola en su aspecto positivo como tal y en su aspecto negativo como omisión".[43]

La conducta o el acto lato sensu, reviste dos formas:

1.- La acción estricto sensu y;

2.- La omisión; y la omisión a su vez comprende;

a) La omisión simple

b) La omisión impropia

c) La comisión por omisión.

[43] López Betancourt, Eduardo. Óp. Cit. Págs.85 y 86.

Por lo tanto, podemos establecer que “la acción en estricto sentido, es un hacer efectivo, corporal y voluntario”.[44]

En los delitos de acción se viola una norma prohibitiva, ya que el sujeto realiza algo que la norma prohíbe hacer.

Por su parte, “la omisión es un no hacer activo, corporal y voluntario, cuando se tiene el deber de hacer, cuando ése hacer es esperado y se tiene el deber de omitirlo”.[45]

De acuerdo con Eugenio Cuello Calón, “la omisión consiste en una inactividad voluntaria cuando la Ley Penal impone la obligación de ejecutar un hecho determinado”.[46]

En cuanto a los delitos de simple omisión (verdadero delito de omisión), éstos concurren cuando hay incumplimiento de una orden positiva de la ley, y causan un resultado exclusivamente jurídico o típico, pues no hay resultados materiales.

[44] Carrancá y Trujillo, Raúl. Óp. Cit. Pág. 263.
[45] Ibídem. Pág. 265.
[46] Cuello Calón, Eugenio. Óp. Cit. Pág.273.

2.4 EL TIPO PENAL Y LA AUSENCIA DEL TIPO.

La Tipicidad.

Se dice que para que una acción sea delictuosa, requiere de ciertos elementos, uno de ellos es justamente la tipicidad, cuyo fundamento se encuentra consagrado en el art. 14 constitucional en cuyo texto se lee: “En los juicios del 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".

Al respecto, Fernando Castellanos Tena, menciona que “la tipicidad es la adecuación de una conducta concreta con la descripción legal formulada en abstracto”.[47]

Para Fernando Pavón Vasconcelos, en su libro "Manual de Derecho Penal Mexicano ", “la tipicidad puede definirse como la adecuación de la conducta o del hecho a la hipótesis legislativa”.[48]

Por su parte el maestro Celestino Porte Petit establece que “la tipicidad consistirá en la adecuación o conformidad a lo prescrito por el tipo”.[49]

Por lo tanto y en concordancia con las definiciones anteriores podemos mencionar que el tipo penal para Ignacio Villalobos en su libro “Derecho Penal

[47] Castellanos Tena, Fernando. Óp. Cit. Pág. 165.
[48] Pavón Vasconcelos, Francisco. Óp. Cit. Pág. 283.
[49] Porte Petit, Celestino. *Apuntamientos de la parte general de Derecho Penal*, Editorial Porrúa, S.A. México 1984. Pág. 471.

Mexicano", consiste en: "la descripción esencial, objetiva de un acto que, si se ha cometido en condiciones ordinarias, la ley considera delictuoso".[50]

Asimismo, el maestro Francisco Pavón Vasconcelos señala que el tipo es: "la descripción concreta dispuesta por la ley de una conducta a la que en ocasiones se suma su resultado, estima como delictuosa, al conectarse a ella una sanción penal".[51]

Para Jiménez de Asúa, en su obra "La Ley y el Delito", el tipo legal es: "la abstracción especifica que ha trazado el legislador, descartando los detalles innecesarios para la definición del hecho que se cataloga en la ley como delito".[52]

Después de haber hablado del tipo y de la tipicidad, hemos de decir que del primero existe una clasificación y dentro de ella, encontramos el tipo y asimismo, optamos por transcribir la hecha por el maestro Fernando Castellanos Tena, y que divide al tipo de las siguientes formas:[53]

Por su COMPOSICION pueden ser:

a) NORMALES: Estos se circunscriben a hacer una descripción objetiva, y

b) ANORMALES: Son los que además de tener elementos objetivos, contienen también subjetivo y/o normativos.

[50] Villalobos, Ignacio. Óp. Cit. Pág. 266.
[51] Pavón Vasconcelos, Francisco. Óp. Cit. Pág. 283.
[52] Jiménez de Asúa, Luis. Óp. Cit. Pág. 235.
[53] Castellanos Tena, Fernando. Óp. Cit. Pág.171.

Por su AUTONOMIA o INDEPENDENCIA pueden ser:

a) AUTÓNOMOS o INDEPENDIENTES: Siendo estos los que tienen vida por sí solos,

b) SUBORDINADOS: Siendo dependientes de otro tipo.

Por su FORMULACIÓN pueden ser:

a) CASUISTICOS: Estos prevén varias hipótesis que a veces se integran el tipo de una de ellas, ejemplo: el delito de adulterio o el de lesiones; y otras veces se integran con la correlación de todas ellas, como el caso de la vagancia y mal vivencia.

b) AMPLIOS: Son los que refieren una hipótesis única, que puede ejecutarse por cualquier medio, como en el caso del robo.

Por el DAÑO que causan se dividen en:

a) DE DAÑO (o de lesión): Que son los que protegen la deducción o pérdida del bien (homicidio, fraude).

b) DE PELIGRO: Estos tutelan los bienes jurídicos contra la posibilidad de ser dañados.

Por su ORDENACIÓN METODOLÓGICA se dividen en:

a) ESPECIALES: Se conforman agregando otros requisitos al tipo fundamental, al cual subsumen, por ejemplo: parricidio.

b) COMPLEMENTADOS: Se constituyen paralelamente de un tipo básico y una circunstancia o característica distinta, ejemplo: homicidio calificado.

c) BÁSICOS o FUNDAMENTALES: Estos constituyen la naturaleza o fundamento de otros tipos (Robo).

El maestro Jiménez Huerta señala que conforman tipos básicos: “aquellos en que cualquier lesión del bien jurídico basta por sí sola para integrar un delito. Los tipos básicos constituyen la espina dorsal del sistema de la parte especial del Código”.[54]

Por otro lado, Luis Jiménez de Asúa nos dice que son tipos básicos: “los que tienen plena independencia”.[55]

Hemos observado que los autores citados conciertan en que esta clase de tipos son fundamentales e independientes y que son base del Código.

Para la creación de un delito, como el referido en el artículo 211 del Código Penal Federal, que es materia de estudio en el presente trabajo de tesis, es de gran importancia tener en cuenta lo anterior para que su aplicación sea llevada a cabo lo más acertadamente posible a fin de no caer en errores o fallas que puedan comprometer su legalidad y eficiencia.

Después de analizar el concepto de tipo, es preciso introducirnos un poco en él y analizar los elementos que lo conforman para que de esta forma, tengamos un conocimiento más amplio y completo del tipo y de cómo se integra un delito.

[54] Jiménez Huerta Mariano. Derecho Penal Mexicano, Editorial Porrúa, S.A. tercera edición, México 1980. Pág. 189
[55] Jiménez de Asúa, Luis. Óp. Cit. Pág. 259.

La mayoría de los autores coinciden en señalar que el tipo corresponde a la descripción de una conducta en los preceptos legales y que esta descripción puede estar determinada por diversos elementos subjetivos, objetivos y normativos, a los que nos referiremos a continuación:

a) ELEMENTOS SUBJETIVOS. Sobre este tipo de elementos, Jiménez de Asúa señala en su libro “La Ley y el Delito”, que son: “aquellos que se refieren a estos anímicos del autor en orden a lo injusto”.[56]

Ignacio Villalobos, por su parte, considera que los elementos subjetivos: “son los que residen y deben estudiarse en el agente del delito”.[57]

Y Fernando Castellanos Tena claramente indica que los elementos subjetivos: “constituyen referencias típicas a la voluntad del agente o al fin que persigue”.[58]

Los citados autores concuerdan en que estos elementos subjetivos determinarán al delito tomando como base, el estado de ánimo o la voluntad del sujeto autor del ilícito.

b) ELEMENTOS OBJETIVOS. Para el jurista Mariano Jiménez Huerta: “la mayoría de los tipos de la parte especial de un Código tienen como contenido una simple descripción objetiva de una conducta, representación que se realiza

[56] Jiménez de Asúa, Luis. Óp. Cit. Pág. 225.
[57] Villalobos, Ignacio. Óp. Cit. Pág. 278.
[58] Castellanos Tena, Fernando. Óp. Cit. Pág. 173.

mediante simples referencias a un movimiento corporal o a un resultado material o tangible que produce".[59]

Estos elementos objetivos, al contrario de los subjetivos, establecerán al delito con la sola descripción de la conducta, sin atender necesariamente al estado anímico, a la voluntad del sujeto o alguna otra circunstancia.

b) ELEMENTOS NORMATIVOS. Estos elementos que también concurren en las figuras típicas, pueden establecer algún delito en forma preponderante dada la importancia que para él mismo revista.

El maestro Mariano Jiménez Huerta en su libro "Derecho Penal Mexicano" menciona que: "los auténticos elementos normativos que contienen los tipos penales, son aquellos que por estar cargados de desvalor jurídico, resaltan específicamente la antijuricidad de la conducta".[60]

Ignacio Villalobos señala que: "los elementos normativos son aquellos cuya afluencia, en su caso concreto, solo puede ser establecida mediante una valoración".[61]

Por otra parte Francisco Pavón Vasconcelos menciona en su obra "Manual de Derecho Penal Mexicano" que: "se les denomina normativos por implicar una valoración de ellos por el aplicador de la ley".[62]

[59] Jiménez Huerta Mariano. Óp. Cit. Pág. 270.
[60] Jiménez Huerta Mariano.Óp. Cit. Pág. 86.
[61] Villalobos, Ignacio. Óp. Cit. Pág. 278.
[62] Pavón Vasconcelos, Francisco. Óp. Cit. Pág. 279.

En los supuestos anteriores se habla de valoración, siendo ésta la base de estos elementos, ya que por medio de dicha valoración, el que aplique la ley podrá manifestar de manera acertada la dirección que se ha querido imprimir a un cierto tipo.

Las diferencias que de la tipicidad radican en que la tipicidad es parte elemental del delito pues para éste exista, primeramente debe establecerse el tipo legal, es decir, el precepto de la ley que ha de contener la conducta que se penalizará en caso de concordar con la descripción de la misma.

Lo anterior queda establecido en una forma más clara en el dogma NULLUM CRIMEN SINE LEGE, lo que corrobora que sin la tipicidad, una acción no podría ser definida como un crimen.

2.5 ANTIJURICIDAD Y CAUSAS DE LICITUD.

Antijuricidad.

Este elemento como los anteriores varía en la noción de los diferentes autores. Así tenemos por ejemplo que Javier Alba Muñoz enuncia en su prólogo a la tesis de R. Higuera Gil: "El contenido último de la antijuricidad que interesa al penalista es, lisa y llanamente, la contradicción objetiva de los valores estatales... en el núcleo de la antijuricidad como en el núcleo mismo de todo fenómeno penal, existe solo el poder primitivo del Estado valorando el proceso material de la realización prohibida implícitamente".[63]

Por su parte Carrancá y Trujillo establece que la antijuricidad "es la oposición a las normas de cultura, reconocidas por el Estado".[64] Carrancá hace referencia a la oposición a las normas de cultura ya que para él, después de hacer un estudio, es posible dividir a las leyes en dos órdenes: las físicas y las culturales, siendo a éstas últimas a las que pertenecen las normas jurídicas; por expresar el deber y tomar en cuenta la valoración de la conducta humana.

Porte Petit define a la antijuricidad como "una conducta adecuada al tipo cuando no se pruebe la existencia de una causa de justificación". El maestro al elaborar su concepto, toma en cuenta las causas de absolución que, en un momento dado, pueden excluir una conducta determinada de la descripción legal impuesta por el Estado.

[63] Castellanos Tena, Fernando. Óp. Cit. Pág. 175.
[64] Carrancá y Trujillo, Raúl. Óp. Cit. Pág. 337.

Causas de licitud.

El aspecto negativo de la antijuricidad lo constituyen las causas de justificación, que son las razones o circunstancias que el legislador consideró para invalidad la antijuricidad de la conducta realizada, al considerarla lícita.

En otras palabras, cuando aparece alguna causa de justificación, desaparece lo antijurídico, y por ende, se desvanece el delito.

Los criterios que fundamentan las causas de justificación son: el consentimiento y el interés preponderante.

Según Edmund Mezger, dice que: “el consentimiento del lesionado no excluye el injusto en todos los hechos punibles”, y agrega: “El consentimiento debe ser serio y voluntario y corresponder a la verdadera voluntad del que consiente”.[65]

En otras palabras, para que el consentimiento tenga eficacia, se necesita que el titular objeto de la acción y el objeto de protección sean de una misma persona.

El interés preponderante nace cuando se está en presencia de dos bienes jurídicos y no se pueden salvar ambos, por lo cual se tiene que sacrificar o arriesgar uno para salvar al otro. Por ejemplo, se justifica que se prive de la vida a alguien para salvar la propia.

[65] Oronoz, Santana, Carlos. *Manual de Derecho Procesal Penal.* Limusa Noriega Editores. 4ta Edición, México 2003, Pág. 113

CAUSAS DE JUSTIFICACIÓN.

La legislación penal mexicana contempla las siguientes:

- Legítima defensa
- Estado de necesidad
- Ejercicio de un derecho
- Cumplimiento de un deber
- Obediencia jerárquica
- Impedimento legítimo.

Como conclusión podemos de esta manera señalar para tal efecto, que la mayoría de los autores coinciden en sugerir que la antijuricidad consiste en la contrariedad de una conducta hacia el Derecho y ésta a su vez tiene su aspecto negativo en las causas de justificación.

2.6 IMPUTABILIDAD Y CAUSAS DE INIMPUTABILIDAD.

Imputabilidad.

El significado de este término de conformidad con el diccionario jurídico de Rafael de Pina Vara es: “la capacidad general atribuible al sujeto para cometer cualquier clase de infracción penal”.

Otro concepto es el de “atribuir o achacar algo a alguien, hacerle responsable”. Es decir, imputarle un delito es atribuírselo para hacerle sufrir las consecuencias, pero para que esa imputación surta efectos legales, el sujeto debe contar con cierta capacidad para poder responder. “La imputabilidad viene a ser la capacidad de ser penalmente responsable”.[66]

La doctrina coincide en que la imputabilidad es “la capacidad de entender y querer en el campo del derecho penal”.

Esto quiere decir que el sujeto activo debe comprender la ilicitud de su acto. Por lo tanto, la imputabilidad está condicionada por la salud mental y por el desarrollo de su autor, dependiendo de la aptitud de discernir sobre el alcance de sus actos, y así determinar si es o no penalmente responsable, o sea, para que el Estado pueda incorporar al sujeto activo en una situación jurídica concreta al cometer un acto contrario a derecho. Esto es, el sujeto activo que es imputable se ve obligado a responder por su proceder ante los tribunales del Estado.

[66] De Pina, Rafael.- Diccionario de Derecho, Editorial Porrúa, S.A., Décima Segunda Edición, México 1996. Pág. 294.

Fernando Castellanos Tena expresa: “que el individuo debe tener capacidad de determinarse en función de lo que conoce, luego la aptitud intelectual y volitiva constituye “el presupuesto básico de la culpabilidad”. La imputabilidad, concluye, “es la posibilidad condicionada por la salud mental y por el desarrollo del autor, para obrar según el justo conocimiento del deber existente. Es la capacidad de obrar en Derecho Penal, es decir, de realizar actos referidos al Derecho punitivo que traigan consigo las consecuencias penales de la infracción”.[67]

Por su parte, Pavón Vasconcelos infiere “que la noción de imputabilidad requiere no sólo el querer del sujeto, sino además su capacidad de entendimiento, pues únicamente quien por su desarrollo y salud mental es capaz de representar el hecho, conocer su significación y mover su voluntad al fin concreto de la violación de la norma, puede ser reprochado en el juicio integrante de la culpabilidad”.[68]

La imputabilidad, según Mayer, es la posibilidad, condicionada por la salud y madurez espirituales del autor, de valorar correctamente los deberes y de obrar conforme a ese conocimiento. O como señala Villalobos “referido a la capacidad del sujeto para dirigir sus actos dentro del orden jurídico; la capacidad de obrar con discernimiento y voluntad, así como para ajustarse a las normas jurídicas o apartarse de ellas culpablemente.”

Podemos concluir entonces que la imputabilidad es la obligación que tiene el sujeto activo de responder de sus actos cuando de manera consciente por su capacidad de actuar, ha vulnerado la norma jurídica previamente establecida por el Estado.

[67] Castellanos Tena, Fernando. Óp. Cit. Pág. 126
[68] Pavón Vasconcelos, Óp. Cit. Pág. 283

Inimputabilidad.

Consiste en la ausencia de capacidad para querer y entender en el ámbito del derecho penal.

CAUSAS DE INIMPUTABILIDAD.

- Trastorno mental.
- Desarrollo intelectual retardado.
- Miedo grave.
- Minoría de edad.

1.- Trastorno Mental.

Incluye cualquier alteración o mal funcionamiento de las facultades psíquicas, siempre y cuando impidan al agente comprender el carácter ilícito del hecho o conducirse acorde con esa comprensión.

Puede ser transitorio o permanente, por la ingestión de alguna sustancia nociva o por un proceso patológico interno. Sólo se excluye el caso en que el propio sujeto haya provocado esa incapacidad, ya sea intencional o imprudencialmente.

Conforme a la legislación mexicana, la fracción II del artículo 15 del Código Penal Federal, señala como circunstancia excluyente de responsabilidad (ausencia de imputabilidad):

“padecer el inculpado, al cometer la infracción, trastorno mental o desarrollo intelectual retardado que le impida comprender el carácter ilícito del hecho o conducirse de acuerdo con esa comprensión, excepto en los casos en que el

propio sujeto activo haya provocado esa incapacidad intencional o imprudencialmente."

2.- Desarrollo intelectual retardado.

Es un proceso tardío de la inteligencia, que provoca incapacidad para entender y querer. En este sentido la sordomudez será causa de inimputabilidad sólo si el sujeto carece de capacidad para entender y querer.

3.- Miedo grave.

Contemplado en la fracción VI del art. 15 del Código Penal del Distrito Federal, es un proceso psicológico mediante el cual el sujeto cree estar en un mal inminente y grave. Es algo de naturaleza interna, a diferencia del temor, que tiene su origen en algo externo; por tanto el temor fundado es causa de inculpabilidad.

4.- Minoría de edad. Se considera que los menores de edad carecen de madurez y, por tanto, de capacidad de querer y entender. De lo anterior se deduce que el menor no comete delitos, sino infracciones a la ley.

2.7 CULPABILIDAD Y CAUSAS DE INCULPABILIDAD.

Culpabilidad.

Para muchos juristas, este es el elemento quizá de mayor importancia, pues en el campo del Derecho Penal, una de las tareas más difíciles consiste en comprobar la culpabilidad o inculpabilidad del ejecutor de un acto.

Sin embargo, aunque gran parte de los autores la consideran un elemento del delito, los conceptos de culpabilidad existentes, son muy variados.

Eugenio Cuello Calón en su obra "Derecho Penal", menciona como “culpable la conducta cuando a causa de las relaciones psíquicas existentes entre ella y su autor, debe serle jurídicamente reprochada”.[69]

Para Celestino Porte Petit la culpabilidad constituye “el nexo intelectual y emocional que liga al sujeto con el resultado de su acto”.[70]

Por su parte Ignacio Villalobos se refiere a la culpabilidad como “el desprecio del sujeto por el orden jurídico y por los preceptos y prohibiciones que tienden a constituirlos y conservarlo”.[71]

Asimismo el profesor Villalobos se refiere a la culpabilidad de manera general como el desprecio por parte de un sujeto hacia las leyes encaminadas al orden social. El sujeto al romper con estas normas, antepone sus intereses personales, emocionales, etc., a los intereses sociales.

---

[69] Cuello Calón, Eugenio. Óp. Cit. Pág. 240.
[70] Porte Petit, Celestino. Óp. Cit. Pág. 49
[71] Villalobos, Ignacio. Óp. Cit. Pág. 282.

Por otro lado Luis Jiménez de Asúa opina que la culpabilidad es “el conjunto de presupuestos que fundamentan la reprochabilidad personal de la conducta antijurídica”.[72]

Algunos autores se refieren a la imputabilidad y a la culpabilidad, como Raúl Carrancá y Trujillo, y se expresan de la primera como una situación psíquica en abstracto y a la segunda como la concreta capacidad de imputación legal.

En relación a la culpabilidad, diversos autores analizan al dolo, al que consideran como elemento subjetivo y principal de la culpabilidad.

Al respecto solo haremos una breve mención de lo que es el dolo. Así tenemos que para tal efecto Cuello Calón nos dice que: “el dolo consiste en la voluntad consciente dirigida a la ejecución de un hecho delictuoso”.[73]

Luis Jiménez de Asúa menciona que: “existe el dolo cuando se produce un resultado típicamente antijurídico, con conciencia de que se infringe el deber, con conocimiento de las circunstancias de hecho y del curso esencial de la relación 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”.[74]

Podemos resumirlo entonces como el acto manifestado voluntaria y razonadamente encaminado a crear consecuencias antijurídicas y típicas y así como la responsabilidad obtenida por el simple hecho de realizarlo.

[72] Jiménez de Asúa, Luis. Óp. Cit. Pág. 352.
[73] Castellanos Tena, Fernando. Óp. Cit. Pág. 239.
[74] Jiménez de Asúa, Luis. Óp. Cit. Pág. 365.

Inculpabilidad.

La inculpabilidad la podemos definir como la ausencia de culpabilidad, significa la falta de reprochabilidad ante el derecho penal, por faltar la voluntad o el conocimiento del hecho. Esto tiene una relación estrecha con la imputabilidad; así, no se puede ser culpable de un delito quien no es imputable.

Por lo anterior, cabe agregar que el delito es una conducta típica, antijurídica imputable y culpable.

CAUSAS DE INCULPABILIDAD.

Las causas de inculpabilidad son las circunstancias que anulan la voluntad o el conocimiento, siendo las siguientes:

a).- Error esencial del hecho invencible.

b).- Eximentes punitivas.

c).- No exigibilidad de otra conducta.

d).- Temor fundado.

e).- Caso fortuito.

Clases de error.

El error puede ser de derecho o de hecho y éste a su vez, ser esencial (vencible e invencible) o accidental (*aberratio ictus, aberratio in persona y aberratio delicti*).

a).-Error.- Es la falsa concepción de la realidad; no es la ausencia del conocimiento, sino un conocimiento deformado, o incorrecto.

b).- Ignorancia.- Es el desconocimiento absoluto de la realidad o la ausencia de conocimiento.

Error de derecho.- Ocurre cuando el sujeto tiene una falsa concepción del derecho objetivo. No puede decirse que es inculpable quien comete un hecho ilícito por error de derecho, ni puede serlo por ignorar el derecho, pues su desconocimiento no excusa de su cumplimiento.

Error de hecho.- El error recae en condiciones del hecho; así, puede ser de tipo o de prohibición: El primero es un error respecto a los elementos del tipo; el segundo, el sujeto cree que no es antijurídico obrar.

Error esencial.- Es un error sobre un elemento de hecho que impide que se dé el dolo.

Error esencial vencible.- Cuando subsiste la culpa a pesar del error.

Error esencial invencible.- Cuando no hay culpabilidad. Este error constituye una causa de inculpabilidad.

Error accidental.- Cuando recae sobre circunstancias accesorias y secundarias del hecho.

Aberratio ictus.- Es el error en el golpe. De todas formas se contraría la norma. Ejemplo, alguien quiere matar a una persona determinada pero a quien priva de la vida es a otra a causa de imprecisión o falta de puntería en el disparo.

Aberratio in persona.- Es el error sobre el pasivo del delito: igual que en el anterior, se mata, pero en este caso, por confundir a una persona con otra.

Aberratio in delicti.- Es el error en el delito. Se produce otro ilícito que no era el querido.

2.8 CONDICIONES OBJETIVAS DE PUNIBILIDAD, FALTA DE CONDICIONES OBJETIVAS DE PUNIBILIDAD.

Punibilidad.

Fernando Castellanos Tena considera que: “la punibilidad consiste en la estimación de una pena en función de la realización de cierta conducta. Un comportamiento es punible cuando se hace acreedor a la pena”.[75]

Es decir, en el momento en que se fije una pena para una determinada conducta, existirá la punibilidad.

El maestro López Betancourt al referirse a la punibilidad se refiere a la punibilidad como: “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 establecidas en nuestro Código Penal”.[76]

Por su parte Jiménez de Asúa considera que lo esencialmente característico del delito es ser punible. Por lo tanto: “la punibilidad es el carácter específico del crimen”.[77]

Al respecto, Cuello Calón expone: “que el delito es fundamentalmente acción punible, dando por tanto a la punibilidad, el carácter de requisito esencial en la formación de aquél”.[78]

---

[75] Ibídem. Óp. Cit. Pág. 267.
[76] López Betancourt, Eduardo. Óp. Cit. Pág. 263.
[77] Jiménez de Asúa, Luis. Óp. Cit. Pág. 426.
[78] Cuello Calón, Eugenio. Óp. Cit. Pág. 281.

Por otra parte encontramos un punto de vista opuesto a los anteriores autores, lo señala Ignacio Villalobos, quien dice que: “no se puede considerar a la punibilidad como elemento integral, dado que la exigencia concreta de una pena no es sino la reacción del Estado respecto al ejecutar de un delito, siendo por tanto algo externo al mismo”.[79]

Podemos mencionar entonces que la punibilidad no constituye un elemento esencial, pero sí un elemento que debe considerarse porque también es cierto que la pena es una característica del delito, ya que de no ser por las excusas absolutorias, existe la posibilidad de estipular a la punibilidad como elemento esencial.

Aspecto negativo: Excusas absolutorias.

Las excusas absolutorias constituyen la razón o fundamento que el legislador consideró para que un delito, a pesar de haberse integrado en su totalidad, carezca de punibilidad.

En la legislación penal mexicana existen casos específicos en los que ocurre una conducta típica, antijurídica, imputable y culpable, pero, por disposición legal expresa, no es punible. Esta ausencia de punibilidad obedece a diversas causas, como se verá en cada caso concreto.

Excusa por estado de necesidad**.**

Aquí la ausencia de punibilidad se presenta en función de que el sujeto activo se encuentra ante un estado de necesidad. Por ejemplo, el robo de famélico art. 379 Código Penal Federal) y el aborto terapéutico (art. 334 del Código Penal Federal).

[79] Ibídem. Óp. Cit. Pág. 254

Excusa por temibilidad mínima.

En función de la poca peligrosidad que representa el sujeto activo, tal excusa puede existir en el robo por arrepentimiento (art. 375 del Código Penal Federal).

Excusa por ejercicio de un derecho.

El caso típico se presenta en el aborto, cuando el embarazo es producto de una violación (art. 333 del Código Penal Federal).

Excusa por imprudencia.

Un ejemplo de este tipo de excusa en el aborto causado por imprudencia de la mujer embarazada (art. 333 del Código Penal Federal.)

Excusa por no exigibilidad de otra conducta.

Uno de los ejemplos más comunes es el encubrimiento de determinados parientes y ascendientes y de otras personas (art. 400 del Código Penal Federal).

Excusa por innecesaridad de la pena.

Esta excusa es aquella en la cual cuando el sujeto activo sufrió consecuencias graves en su persona, por su senilidad o por su precario estado de salud hacen notoriamente innecesaria e irracional la aplicación de la pena (art. 55 del Código Penal Federal).

Condicionalidad objetiva y su aspecto negativo.

Aunque en este caso se trata de otro elemento del delito, dada su naturaleza controvertida, pues la mayoría de los autores niegan que se trate de un verdadero elemento del delito, se ha incluido en el tema de la punibilidad por su relación estrecha con ésta.

También considero importante aclarar que al igual que la punibilidad, la condicionalidad objetiva no es propiamente parte integrante y necesaria del delito, ya que éste puede existir sin aquellas.

Está constituida por requisitos que la ley señala eventualmente para que se pueda perseguir el delito. Algunos autores dicen que son requisitos de procedibilidad o perseguibilidad, mientras que para otros son simples circunstancias de hechos adicionales, exigibles, y para otros más constituyen un auténtico elemento del delito.

Jiménez de Asúa, quien los denomina *condiciones objetivas de punibilidad*, afirma que: “son presupuestos procesales a los que a menudo se subordinan la persecución de ciertas figuras de delito”.

Fernando Castellanos Tena, señala que: “estas condiciones objetivas son parte integral del tipo”.[80] Y si bien es cierto que en varios casos así ocurre, también es cierto que son parte independiente del tipo, por ejemplo, en el caso de delincuentes que hayan cometido infracción en el extranjero y deban ser penados en la República, para lo cual es requisito que la infracción de que se les acuse, tenga el carácter de delito en el país en que se ejecutó y en la República.

[80] Castellanos Tena, Fernando. Óp. Cit. Pág. 270.

Las condiciones objetivas de penalidad, expresa el maestro Jiménez de Asúa, son adventicias e inconstantes, asimismo Castellanos Tena nos dice que "no constituyen un elemento esencial porque son exigibles solo por excepción".

Por su parte el maestro Sebastián Soler parece darnos la visión más clara al respecto, señalando que: "estas condiciones objetivas de punibilidad se diferencian de los presupuestos o elementos esenciales porque éstos anteceden al delito y aquellas otras, después de efectuado el delito". [81]

Así tenemos que en realidad, las condiciones objetivas son, elementos del tipo; a veces están relacionados con la intencionalidad del sujeto, otras con aspectos referentes a la perseguibilidad, etc.

Un ejemplo de condición objetiva es el siguiente: para que la circunstancia atenuante establecida en el art. 310 del Código Penal Federal, opere en beneficio del cónyuge ofendido por infidelidad conyugal, se requiere que él no haya favorecido a la corrupción de su cónyuge.

Ausencia de condicionalidad objetiva.

La ausencia de condicionalidad objetiva llega a ser el aspecto negativo de las condiciones objetivas de punibilidad. La carencia de ellas hace que el delito no se castigue.

[81] Soler, Sebastián. Óp. Cit. Pág. 279.

2.9 TENTATIVA.

Para Luis Jiménez de Asúa la tentativa consiste en: “la ejecución incompleta de un delito”.[82]

Por su parte, Sebastián Soler establece en su obra que: “la tentativa radica en iniciar la acción principal en la cual el delito consiste; para ello es ilustrativo pensar en el verbo que la expresa”.[83]

Asimismo Fernando Castellanos Tena menciona al respecto: “entendemos, pues, por tentativa, los actos ejecutivos (todos o algunos), encaminados a la realización de un delito, si éste no se consuma por causas ajenas al querer del sujeto”.[84]

Por lo tanto el delito será tentativo cuando el autor dolosamente haya dado comienzo a la ejecución, pero no logre consumarlo por circunstancias ajenas a su voluntad. Este concepto es válido tanto para el caso en que la consumación no se produzca porque la acción no resultaba adecuada para la realización integra del tipo, como para el caso de que la acción tuviera materialmente posibilidad de consumar el delito, por ejemplo en el delito de robo que no se consuma por circunstancias ajenas a la voluntad del autor, tanto cuando no encuentra la cosa de la que esperaba apoderarse en el lugar donde supuso erróneamente que estaría, así como cuando el autor es sorprendido con la cosa, antes de salir del ámbito de custodia del dueño.

Así encontramos que en la tentativa no se cumple totalmente el tipo objetivo. Por otra parte podemos observar que debe existir totalmente el tipo subjetivo (dolo).

---

[82] Jiménez de Asúa, Luis. Óp. Cit. Pág. 595.
[83] Soler, Sebastián. Óp. Cit. Pág. 217.
[84] Castellanos Tena, Fernando. Óp. Cit. Pág. 287.

En consecuencia, si el tipo consumado admite el dolo eventual es factible la tentativa de ese delito con dolo eventual.

Así tenemos que la tentativa puede analizarse a través de sus distintos elementos y que de acuerdo a la doctrina consisten en:

a) Que el tipo objetivo no se haya ejecutado totalmente. El defecto del tipo objetivo puede referirse a cualquiera de sus elementos. Puede tratarse cuando falta una característica del sujeto pasivo, por ejemplo la víctima de estupro tiene más de 18 años como lo requiere el artículo 180 del Código Penal para el Distrito Federal, ó como que no realice cambios en el mundo exterior, en los delitos de resultado, por ejemplo errar el disparo por lo que no se produce la muerte en el delito de homicidio.

b) Que el tipo subjetivo concurra totalmente. De acuerdo a la ley por la tentativa se exterioriza la intención de cometer un delito, lo que muestra que debe existir el dolo de efectuarlo.

c) Que haya por lo menos inicio en la ejecución. El comienzo de ejecución es lo que diferencia la tentativa de los actos preparatorios.

Por lo tanto es necesario hacer un análisis del comienzo de ejecución, ya que de acuerdo a la doctrina encontramos la delimitación entre actos preparatorios y tentativa.

Para resolver esta cuestión se han enunciado distintas teorías, que tienen origen en la diversa fundamentación de la punibilidad de la tentativa.

1) Teoría formal objetiva. Establece que hay comienzo de ejecución cuando el autor ha llevado a cabo una parte de la acción de ejecución misma, como, por ejemplo, apretar el gatillo. Esta acción es suficiente para que desde ese momento el bien jurídico corra peligro.

2) Teoría material objetiva. Involucra cualquier acción que implique un peligro inmediato para el bien jurídico.

El sistema funciona de la siguiente manera: podemos partir de la acción típica y se cuestionarnos después de acuerdo al plan del autor (no desde el punto de vista de un espectador), cuando el autor penetra en el núcleo del tipo (cuándo comienza a matar, a apoderarse, etc.).

3) Teoría subjetiva: Existe comienzo de ejecución, cuando de la acción resulta innegable la meta del propósito delictuoso. Si se toma en cuenta la punibilidad de la tentativa inidónea, la base del sistema no puede ser el peligro que haya corrido el bien jurídico.

4) Teoría que fusiona elementos objetivos y subjetivos. Toma en cuenta el comienzo de ejecución cuando el autor ha iniciado a realizar una acción que según su plan, implica situarse directamente en la realización de la acción típica, si desde el punto de vista de la experiencia general, es una parte integrante de la acción típica.

2.10 CONCURSO DE DELITOS.

Se produce, según explica Manuel Osorio en su Diccionario De Ciencias Jurídicas, Políticas y Sociales, "cuando a una persona se la llama a responder de varias violaciones de la ley penal". Y añade que "no es suficiente que su conducta encuadre en más de una figura delictiva, sino que, además, es necesario que las respectivas figuras puedan funcionar al mismo tiempo de manera autónoma, sin que la aplicación de una esté excluida por la aplicación de la otra".[85]

En lo que respecta al concurso formal o ideal encontramos que admite necesariamente el conjunto de normas compatibles entre sí; de tal forma que se departe la unidad del delito en virtud de que la conducta o el hecho caen bajo una variedad de sanciones, obteniendo por ello, como lo opina Soler, "un encuadramiento múltiple".

El concurso ideal o formal surge cuando con una sola conducta se originan varios resultados típicos, en cuyos casos se dice que existe unidad de acción y pluralidad de resultados. Así tenemos que el Código Penal Federal en su artículo 18, primera parte, establece al concurso de delitos de la siguiente manera: "Existe concurso ideal, cuando con una sola conducta se cometen varios ilícitos."

Así encontramos que para sancionar esta forma de manifestación del delito hay que recurrir al primer párrafo del artículo 64 del propio código, que establece: "En caso de concurso ideal, se aplicará la pena correspondiente al delito que merezca la mayor, la cual se podrá aumentar hasta en una mitad más del máximo de su duración, sin que pueda exceder de las máximas señaladas en el Título Segundo del Libro Primero."

---

[85] Osorio, Manuel. *Diccionario de Ciencias Jurídicas, Políticas y Sociales.* 1ª Ed. Electrónica. Datscan S.A. Guatemala, 2009 Pág. 213

2.11 AUTORÍA Y PARTICIPACIÓN PENAL.

Podemos empezar por mencionar que en la mayoría de los casos, el delito es el resultado de la actividad de un individuo; sin embargo, en la práctica muchas veces dos o más sujetos colectivamente realizan un mismo delito; es entonces cuando se habla de la participación.

Expuesto lo anterior podemos definir a la participación como: "la intervención de dos o más personas en la realización de un delito".[86]

De esta manera podemos deducir que la participación consiste en la voluntaria cooperación de varios individuos en la realización de un delito, sin que el tipo requiera de manera indispensable esa pluralidad.

Así tenemos que el criterio más aceptado por la Doctrina divide tradicionalmente a la participación en tres formas:

a) Autores: Principal, material, intelectual, mediato, inmediato.

b) Coautores

c) Cómplices

a) AUTORES

Para exponer el concepto de "autores", el Diccionario Jurídico Mexicano, cita lo siguiente:

[86] Castellanos Tena, Fernando.- Lineamientos Elementales de Derecho Penal, Parte General, Editorial Porrúa, S.A. trigésima quinta edición, México 1994. Pág. 293.

" En materia de Derecho Penal, autor, y en concordancia con el Diccionario de la Lengua Española, que en este caso sigue lo establecido por el Código Penal Español, es: la persona que comete el delito, o fuerza o induce directamente a otras a ejecutarlo, o coopera a la ejecución por un acto sin el cual no se habría ejecutado. Cuando en la realización de un hecho delictivo hay una concurrencia de varias personas, cabe distinguir siempre entre las que son autores y otras que participan en el mismo pero no son autores. A esa concurrencia de personas en el delito se la llama "participación criminal", que abarca a quienes son autores y a quienes son cómplices e instigadores o inductores, que dan origen a las formas de: autoría, complicidad e instigación, respectivamente".[87]

Por su parte Raúl Carrancá y Trujillo define al "autor" como: "la persona que sola o conjuntamente con otra u otras lo ejecuta todo entero y de propia mano, o bien que determina a otro, imputable y culpable o no, para que aquella lo ejecute". [88]

Asimismo Fernando Castellanos Tena nos explica con relación a este tema lo siguiente: "Llamase autor al que pone una causa eficiente para la producción del delito; es decir, al ejecutor de una conducta física y psíquicamente relevante. La doctrina está de acuerdo, por supuesto, en considerar como autores no sólo a quienes material y psicológicamente son causa del hecho típico, sino que es suficiente, para adquirir tal carácter, la contribución con el elemento físico o con el anímico, de donde resultan los autores materiales y los autores intelectuales".[89]

---

[87]. Instituto de Investigaciones Jurídicas. *Diccionario Jurídico Mexicano,* Editorial Porrúa, S.A., Octava Edición, México 1995. Págs. 283-284.

[88] Carrancá y Trujillo, Raúl. Óp. Cit. Pág. 674.

[89]Castellanos Tena, Fernando. Óp. Cit. Pág. 296.

A su vez, Eugenio Cuello Calón menciona con respecto al autor: “Es autor del delito el que lo ejecuta realizando los elementos que integran su figura legal”.[90]

También encontramos que en lo que respecta a los autores de delitos, la doctrina divide a estos en subdivisiones refiriéndose a: autor principal ó directo, autores materiales, autores intelectuales, autores por cooperación y autores mediatos.

El autor directo ó principal.

Es aquel que tiene el poder de dirección sobre la configuración del hecho, y es el que concibe, prepara o ejecuta el acto delictuoso; éste puede ser material intelectual, mediato e inmediato;

El autor material.

Llámense así a aquellos que realizan el acto directamente constitutivo del delito. Es decir, aquel sujeto que realiza directamente la conducta delictiva.

El autor intelectual.

Se entiende por actor intelectual a aquellos sujetos quienes no realizan por sí el delito pero logran que otro lo ejecute. Instigan a otro determinando su voluntad, con el propósito de que se cometa el delito.

El autor por cooperación.

Son todos aquellos que no ejecutan el acto a que se refiere la descripción legal del delito, ni inducen a ello directamente, pero si prestan auxilio necesario para una u otra cosa, sin el cual no hubiera sido posible la consumación criminal.

[90] Cuello Calón, Eugenio. Óp. Cit. Pág. 645.

Por otra parte se han llamado “autores mediatos”, a todos aquellos que realizan un delito valiéndose de otra persona que actúa como mero instrumento, ya sea porque actúa sin dolo, atípicamente o injustificadamente, o incluso inculpablemente como es el caso de una persona excluida de responsabilidad que como ejemplo y por medio de la fuerza física obligan a ejecutar los movimientos que han de consumar el delito. El autor o autores mediatos se valen de un inimputable o de alguien que está en error para cometer el delito.

Y por último tenemos al autor inmediato, que es aquél que realiza con su propia mano la conducta prohibida.

b) COAUTORES

Francisco Pavón Vasconcelos define a los autores como: “al igual que el autor, es quien realiza la actividad conjuntamente con otro u otros, descrita en la ley”.[91]

Asimismo Luis Jiménez de Asúa nos dice al respecto: “El coautor no es más que un autor que coopera con otro u otros autores. Todos los coautores son, en verdad autores, en modo alguno se trata de un autor mediato; porque todos ellos responden como autor”.[92]

Por nuestra parte encontramos en el Diccionario Jurídico Mexicano una definición más amplia respecto al coautor que a la letra dice: “el coautor es también un autor que comparte o divide con otro una misma tarea. Para el derecho penal, coautor es aquel que conjuntamente con otro u otros lleva a cabo la realización de un delito, en forma tal que cada uno de ellos, aisladamente, ejecuta la conducta típica

[91] Pavón Vasconcelos, Francisco.- Manual de Derecho Penal Mexicano, Editorial Porrúa, S.A. sexta edición. México 1984. Pág. 508.
[92] Jiménez de Asúa, Luis.- La Ley y el Delito, Editorial Sudamericana, décimo segunda edición, Argentina 1981. Pág. 220.

en su totalidad y ambos reúnen los requisitos típicos necesarios para ser autores. Por lo tanto coautor es aquel que teniendo la calidad de autor, posee el codominio del hecho. Todo coautor es, por tanto, autor; en él deben concurrir, en primer lugar la característica general que es el "dominio del hecho" y, en segundo ciertas características especiales -que el tipo penal puede requerir para el autor-, que pueden ser objetivas (cierta calidad en él, por ejemplo, ser funcionario o empleado público) o subjetivas (ánimo, deseo, propósito, etc., por ejemplo, ánimo de lucro, deseo erótico). Los que no reúnan tales características, entonces, no serán coautores. Es aquí donde se encuentra el punto distintivo entre autor (coautor) y partícipe (cómplice e instigador). Conforme a esto para ser coautor debe tenerse la calidad de autor. En principio bastará una calidad o característica genérica, que es la que corresponde a todo sujeto según el criterio que se siga de los anteriormente mencionados; en la medida en que cada uno de los que realizan el hecho conjuntamente tiene tal característica, como sería. p.e. el dominio del hecho, será coautor. Habrá casos en que además de la característica genérica se requiera por el tipo en particular una característica específica, como puede ser una determinada calidad en el sujeto, como ser servidor público, p.e., o un elemento subjetivo que deba concurrir en él, como es el propósito de hacerse ilícitamente de una cosa o de obtener un lucro indebido en el caso del fraude mediante libramiento de cheque sin fondos. En ambos casos, para ser coautor se requerirá que concurra en los intervinientes la característica genérica y la específica; si falta esta última, aun cuando se dé la primera no podrá hablarse de coautoría.".[93]

La coautoría se basa fundamentalmente en el principio de la división del trabajo, ya que cada coautor complementa con su parte en el hecho la de los demás, en la totalidad del delito; por eso responde también por el todo.

[93] Diccionario Jurídico Mexicano. Óp. Cit. Págs.486-487.

c) CÓMPLICES

Como última forma de participación encontramos a la figura jurídica de los cómplices, mismos que Luis Jiménez de Asúa nos define como: “los que prestan al autor una cooperación secundaria a sabiendas de que favorecen la comisión del delito, pero sin que su auxilio sea necesario”.[94]

Para Raúl Carranca y Trujillo establece en su obra que la complicidad consiste en: “Cuando al delincuente principal lo ayudan o socorren otros mediante previo acuerdo, estos son cómplices”.[95]

A su vez Francisco Pavón Vasconcelos expone con respecto a la complicidad: “Consiste en el auxilio prestado a sabiendas, para la ejecución del delito, pudiendo consistir en un acto o un consejo”.[96]

Por su parte Ignacio Villalobos éstos menciona con respecto a los cómplices: “los que inducen a cometer un delito, los que lo ejecutan y aquellos que prestan un auxilio necesario para la realización del mismo, quedan como cómplices todas las demás personas que concurren indirectamente a la causación del evento”.[97]

Por último mencionare una definición muy completa y que aclara cualquier duda respecto a los cómplices, misma que proviene del Diccionario Jurídico Mexicano, y que a la letra dice:

“Cómplice, del latín “complex-icis”; participante o asociado en crimen imputable a dos o más personas. Cómplice, en un sentido más técnico, se refiere a aquel que

[94]Jiménez de Asúa, Luis. Óp. Cit. Pág. 315.
[95]Carrancá y Trujillo, Raúl. Óp. Cit. Pág. 675.
[96]Pavón Vasconcelos, Francisco. Óp. Cit. Pág. 508.
[97] Villalobos, Ignacio. Óp. cit. 489.

presta auxilio o coopera dolosamente en el injusto doloso de otro. El cómplice es un participe en sentido estricto y, en tal virtud no tiene el dominio del hecho al que ayuda o coopera; quien lo tiene es el autor. La conducta del partícipe (cómplice o instigador) es, por eso, accesoria del injusto cometido por otro u otros".[98]

El hecho principal en el que se participa, o del que es accesoria la complicidad, debe, además, encontrarse por lo menos en la etapa ejecutiva, para que la participación sea punible; por lo que una participación a nivel de la concepción o de los actos preparatorios no puede ser punible si el hecho principal no llega por lo menos a la etapa de la tentativa.

La complicidad se distingue de la autoría en virtud de que en aquélla el cómplice no tiene el dominio del hecho, es decir, no tiene la posibilidad de controlar la configuración del hecho como ocurre con el autor.

Como cómplice se puede auxiliar a la ejecución del delito, ya sea proporcionando medios materiales o bien puramente psicológicos, por lo que podemos mencionar que se llama cómplice a la persona que contribuye a la ejecución del delito de una manera consciente que coopera en su consumación teniendo precisamente la tendencia a ése fin.

Por otra parte encontramos que no será cómplice el que favorece o coopera para la ejecución del delito si ignora ésta circunstancia. Así tenemos que la complicidad puede ser psíquica, cuando el individuo apoya emocionalmente al autor material, puede ser material cuando se ofrecen medios materiales para la ejecución del delito, cuando se coopera de cualquier modo para que éste se efectué.

[98]Diccionario Jurídico Mexicano. Óp. Cit. Pág. 547.

CAPITULO III.- DELITOS INFORMÁTICOS.

3.1 Antecedentes históricos del delito informático.

3.2 Concepto de delito informático y principales características.

3.3 Principales diferencias entre la concepción de delito informático y delito cibernético.

3.4 El delito informático como delito de “cuello blanco”.

3.5 Clasificación de los delitos informáticos.

- **3.5.1 Elemento Subjetivo**
- **3.5.2 Elemento Objetivo**
- **3.5.3 Elemento Funcional**

3.6 Diferentes tipos de delitos informáticos.

3.7 Sujetos activo y pasivo del delito informático.

3.8 Avances legislativos en materia de delitos informáticos en Latinoamérica.

3.9 La policía cibernética y su labor en la persecución de los delitos informáticos.

CAPITULO III.- DELITOS INFORMÁTICOS.

3.1 ANTECEDENTES HISTÓRICOS DEL DELITO INFORMÁTICO.

En el año de 1975, fecha en que se creó la primera PC (Computadora Personal), así como las redes informáticas que se originaron a partir de 1963, difícilmente se podría apreciar la complejidad en el manejo de la información que se generaría debido principalmente a que en aquel entonces eran tecnologías conocidas para muy pocas personas, dado que su utilización se restringía al campo militar, tecnológico y universitario fundamentalmente; sin embargo, la masificación y disminución en los costos de las computadoras personales, así como la apertura de la red, que cambió su denominación a Internet, dio inicio a la formación de un mundo virtual, con ilimitadas posibilidades, lo por su parte trajo consigo grandes beneficios a la humanidad como un por ejemplo: la ventaja de la comunicación al instante entre dos países situados en los extremos del globo terráqueo, pero como ya hemos comentado con anterioridad, también se generaron serios problemas en relación con el uso y abuso de tal producto tecnológico, la incorporación del Internet al mundo real fue avasallador de tal manera que los sistemas jurídicos de las naciones no se encontraban preparadas con los mecanismos legales necesarios para afrontar dicha problemática.

Años después, en 1983 en París, la Organización para la Cooperación y el Desarrollo Económico (OCDE) designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en las legislaciones penales. El dictamen de esta organización, recomendó a los países miembros la modificación de su legislación penal, de forma que se integraran los nuevos delitos informáticos.

En 1989, el Consejo de Europa convocó a otro comité de expertos, que en la Recomendación emitida el 13 de septiembre de ese año, presentaron una lista

mínima de los delitos que debían agregarse a las legislaciones de cada país miembro, junto con una lista opcional.

Como ya hemos mencionado con anterioridad, este tema también ha sido tomado en cuenta en diversos eventos internacionales como el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado de Montreal en 1990, en el Octavo Congreso Criminal de las Naciones Unidas celebrado en el mismo año, y en la Conferencia de Wurzburgo, en Alemania, en 1992.

De forma más específica, se estableció en 1996, por el Comité Europeo para los Problemas de la Delincuencia, un nuevo comité de expertos para que emprendieran un estudio más profundo acerca del tema de los delitos informáticos.

Por su parte México no fue la excepción, lo que dio lugar a que se considerara participar en los diversos congresos internacionales que han surgido en la actualidad para intentar regular principalmente en qué casos debían considerarse ilícitas determinadas conductas ejecutadas a través del uso de los equipos informáticos y el Internet, así fue como poco a poco se generaron nuevas denominaciones de delito, entre otras, delito informático, ciberdelito, etc. Así tenemos que en nuestro país fue hasta el año de 1999 en que se incorporaron a la legislación vigente los delitos informáticos, aunque cabe destacar que diversos ordenamientos comprenden algunas figuras lesivas genéricas en las que bien se puede integrar conductas delictivas llevadas a cabo por el uso de Internet, el propósito de esta tesis es denotar los signos distintivos de los delitos informáticos en nuestro país, a fin de visualizar la complejidad que representa en algunos casos la ubicación de los sujetos activos del delito, así como también la complejidad que resulta para el Estado la persecución de muchos ilícitos informáticos con motivo del derecho constitucional a la no intervención de comunicaciones privadas.

3.2 CONCEPTO DE DELITO INFORMÁTICO Y PRINCIPALES CARACTERISTICAS.

Concepto de delito informático.

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

De esta manera, el autor mexicano Julio Téllez Valdés señala que los delitos informáticos son: "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)". [99] Es decir, que en base a este concepto podemos considerar a los delitos informáticos como cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin.

Organismos internacionales como la OCDE, lo define como "cualquier conducta, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos."[100]

[99] Téllez Valdés, Julio. Óp. Cit. Pág. 53
[100] López Betancourt, Eduardo. *Delitos en particular*. México, Porrúa, 2004, p. 270.

Para Gabriel Andrés Campoli, los delitos informáticos son “aquéllos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por medio de la utilización indebida de medios informáticos”, y asimismo agrega que “delitos electrónicos o informáticos electrónicos, son una especie del género delitos informáticos, en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios”.[101]

Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo". [102]

Principales características de los delitos informáticos.

Según Téllez Valdés, este tipo de acciones presentan las siguientes características principales: [103]

1) Son conductas criminales de “cuello blanco”, en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

2) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

3) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

---

[101] Campoli, Gabriel Andrés, *“Hacia una correcta hermenéutica penal delitos informáticos vs. delitos electrónicos”.* Revista de Derecho Informático núm. 048, Julio de 2002,pág. 45
[102] Fernández Delpech, Fernando. Óp. Cit. Pág. 64
[103] Téllez Valdés, Julio. Óp. Cit. Pág. 65

4) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

5) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

6) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

7) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

8) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

9) Pueden ser imprudenciales y no necesariamente cometerse con intención.

10) Ofrecen facilidades para su comisión a los menores de edad.

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

12) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

3.3 PRINCIPALES DIFERENCIAS ENTRE LA CONCEPCIÓN DE DELITO INFORMÁTICO Y DELITO CIBERNÉTICO.

Como ya hemos analizado con anterioridad, podemos admitir como delitos informáticos de una manera general a "cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin para su consecución"[104], pero también hemos mencionado que dentro de la amplitud de éste desarrollo de la informática existe un área que ha evolucionado de una forma particularmente exponencial, siendo ésta el Internet, para lo cual considero relevante hacer un estudio más específico de los principales delitos informáticos cometidos a través de esta tecnología, los cuales a su vez han sido denominados de forma particular como "delitos cibernéticos", dado que utilizan el llamado "espacio virtual" o "ciberespacio" que brinda el internet para su realización.

Así tenemos que según la opinión de Fernando Fernández Delpech "los delitos cibernéticos presentan una gravedad mayor toda vez que el objetivo central es atacar a la población más vulnerable", que de acuerdo con el Jefe del Departamento de Delitos Cibernéticos de la Secretaría de Seguridad Pública Federal, son niños mayores de 10 años y menores de 19, así como adultos mayores.

Asimismo de acuerdo con un estudio elaborado por la Asociación Mexicana de Internet (AMIPCI), el 43% de los internautas se conectan a Internet desde su domicilio particular, lo que nos hace suponer que cualquier miembro del hogar de manera indistinta puede ser víctima de algún tipo de delito cibernético si no se toman las precauciones de seguridad debidas.

---

[104] Ídem, pág. 65

De acuerdo con la AMIPCI, al 2006 del total de computadoras instaladas en México 59% están conectadas a la red, lo que representa 20.2 millones de cibernautas, de las cuales 45% son niños y jóvenes de entre 12 y 19 años.

La siguiente tabla muestra el porcentaje de las actividades más frecuentes en internet.[105]

Principales actividades en Internet.

ACTIVIDADES	PORCENTAJE
Correo electrónico	80.8%
Mensajes instantáneos	68.0%
Investigación	67.9%
Comunicación a través de sala de chat	65.3%
Ingreso a sitios de noticias y/o sitios de gobierno	60.9%
Uso de banca en línea y pagos electrónicos	47.4%
Ingreso a sitios de educación/aprendizaje	45.9%
Escuchar música en línea	45.1%
Videojuegos en línea	44.0%
Descarga de música en formato MP3	42.7%
Visitas a páginas de humor y entretenimiento	42.6%

[105] Fuente: *Anuario de Internet*. Asociación Mexicana de Internet (AMIPCI) 2006.

3.4 EL DELITO INFORMÁTICO COMO DELITO DE “CUELLO BLANCO”.

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "ingresa" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (Números. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

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

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", los estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo 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 de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros".

Asimismo, este criminólogo estadounidense dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no se determina a través del interés protegido, como sucede en los delitos convencionales sino de atiende principalmente a las cualidades del sujeto activo que los comete.

Entre las características en particular que poseen este tipo de delitos tenemos que: [106]

- 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.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. Sin embargo, la cifra es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico

[106] Pérez Luño, Antonio. Óp. Cit. Pág. 18

de quienes los 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 tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

3.5 CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

Actualmente en Latinoamérica, existen tres grandes corrientes teóricas dirigidas a definir o conceptualizar el alcance de la criminalidad informática. Estas tendencias doctrinarias del Derecho Informático suelen clasificar a los delitos informáticos según el análisis de su elemento subjetivo, objetivo y funcional.

3.5.1 ELEMENTO SUBJETIVO.

En los primeros estudios teóricos sobre la delincuencia informática se ha hecho hincapié en la personalidad singular de los sujetos activos de estas conductas delictivas. Así encontramos que mediante esta teoría se pretende analizar al delito informático dando énfasis en la peculiaridad de los delincuentes así como en los rasgos comunes que posean para tal efecto. Como un ejemplo de este enfoque tenemos principalmente la asociación de los delitos informáticos con las actividades de los llamados “Hackers”, es decir jóvenes intrusos capaces de acceder a los sistemas informáticos gracias a sus conocimientos de las nuevas tecnologías. Así encontramos como punto fundamental base de esta teoría, el hecho de que para estos individuos el acceso ilícito a las redes y equipos informáticos constituye un reto intelectual realizado en un primer lugar con un propósito lúdico, más que por un afán de carácter económico.

3.5.2 ELEMENTO OBJETIVO.

En los análisis actuales de los delitos informáticos ha sido también frecuente tomar como denominador común el elemento objetivo, consistente en los resultados materiales perpetrados sobre los equipos informáticos o sobre el patrimonio de las personas propietarias de los mismos. El delito informático se identifica así con las lesiones ilícitas del patrimonio conformado por ordenadores, ya sea en su equipo físico o directamente en la información que contienen lo que incluso puede traer como consecuencia como ya hemos analizado anteriormente un daño pecuniario a la víctima.

Entre los delitos informáticos que ocasionan un daño de contenido patrimonial podemos encontrar:

- Los fraudes cometidos a través de manipulaciones contra los sistemas de procesamiento de datos,
- El espionaje informático y la falsificación o piratería de software,
- El sabotaje informático a través de virus u otras herramientas que ocasionan un daño físico en los sistemas,
- El acceso no autorizado a sistemas y equipos de informática con el objetivo de modificar o destruir la información contenida en los mismo o simplemente con el propósito de violentar su seguridad,
- El robo de servicios como el acceso a internet o la interconexión entre llamadas de larga distancia, etc.

3.5.3 ELEMENTO FUNCIONAL.

Ante la insuficiencia de los planteamientos subjetivos y objetivos se ha atendido al estudio de otros factores como el elemento funcional para delimitar la criminalidad informática. Esta corriente a su vez tiende a acentuar la relevancia de la dimensión funcional, es decir de la operatividad y funciones que cumplen los sistemas informáticos. [107] Desde este punto de vista, las conductas delictivas informáticas serán aquellas que sirvan para o tengan por objeto el funcionamiento de los sistemas informáticos.

Un ejemplo de un delito informático analizado desde esta perspectiva lo encontramos en el sabotaje del que pudiera ser efecto la puesta en marcha de un sistema informatizado de control o diagnostico médico. Así encontramos que la informática puede tomarse en cuenta como un elemento funcional activo para la comisión de actos delictivos o bien pasivo, en cuanto a que puede constituir también un sistema objeto de ataques criminales.

[107] Ibídem, pág. 21

3.6 DIFERENTES TIPOS DE DELITOS INFORMÁTICOS.

Para poder hacer una clasificación general de los delitos informáticos, retomaremos aquella hecha por el maestro Téllez Valdés en su obra y de manera muy amplia la establece de acuerdo a dos criterios:

1.- COMO INSTRUMENTO O MEDIO.

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

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

2.- COMO FIN U OBJETIVO.

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

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

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

- *Acceso no autorizado*: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
- *Destrucción de datos*: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- *Infracción al copyright de bases de datos*: Uso no autorizado de información almacenada en una base de datos.
- *Interceptación de e-mail*: Lectura de un mensaje electrónico ajeno.
- *Estafas electrónicas*: A través de compras realizadas haciendo uso de la red.
- *Transferencias de fondos*: Engaños en la realización de este tipo de transacciones.

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

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

- *Terrorismo:* Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

- *Narcotráfico:* Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

- *Otros delitos:* Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o viceversa.

3.7 SUJETOS ACTIVO Y PASIVO DEL DELITO INFORMÁTICO.

Sujeto activo.

El sujeto activo de los delitos informáticos, es un individuo que por sus capacidades en el conocimiento de sistemas informáticos y en ocasiones por la oportunidad de laborar en determinado puesto que implica el manejo de información, comete el delito. Algunos de estos delincuentes son personas particularmente inteligentes y creativas.

En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, los conocimientos o habilidades del delincuente en ese campo.

Sujeto Pasivo.

Es la persona física o moral o la víctima que recibe la agresión o sobre quien recae el daño o peligro ocasionado por el sujeto activo. Existen dos clases de sujetos pasivos:

Sujeto pasivo de la conducta.- Es la persona que de manera directa recibe la agresión del sujeto activo, pero la afectación la recibe el titular del bien jurídico tutelado.

Sujeto pasivo del delito.- Es el titular del bien jurídico tutelado que resulta afectado, aunque directamente no recibe la agresión.

El sujeto pasivo, puede ser una persona individual o colectiva, usualmente es presa fácil de los delincuentes informáticos por su ignorancia en el manejo de las tecnologías.

El sujeto pasivo en el caso de los delitos informáticos puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

3.8 AVANCES LEGISLATIVOS EN MATERIA DE DELITOS INFORMÁTICOS EN LATINOAMÉRICA.

Argentina.

La Argentina sancionó el 4 de junio del 2008 la Ley 26.388 (promulgada el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

Venezuela.

Concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001.

En este país la ley tipifica cinco clases de delitos:

Contra los sistemas que utilizan tecnologías de información: acceso indebido (Art.6); sabotaje o daño a sistemas (Art.7); favorecimiento culposos del sabotaje o daño. (Art. 8); acceso indebido o sabotaje a sistemas protegidos (Art. 9); posesión de equipos o prestación de servicios de sabotaje (Art. 10); espionaje informático (Art. 11); falsificación de documentos (Art. 12).

Estados Unidos.

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

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país (tras un año largo de deliberaciones) establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos y/o mensajes electrónicos y contratos establecidos mediante Internet, entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

México.

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el titulo noveno capítulo I y II.

El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería está regulada en la Ley Federal del Derecho de Autor en el Título IV, capítulo IV.

También existen leyes locales en el código penal del Distrito Federal y el código penal del estado de Sinaloa.

3.9 LA POLICÍA CIBERNÉTICA Y SU LABOR EN LA PERSECUCIÓN DE LOS DELITOS INFORMÁTICOS.

Debido a la reciente aparición de los denominados delitos cibernéticos y a sus características especiales para desarrollarse sólo en Internet, en la actualidad se han generado diversos mecanismos informáticos de protección en el ámbito tecnológico, como lo son programas que codifican nuestra información, programas protectores y antivirus, vigilancia de la red, etc. Asimismo ante la insuficiencia de estas medidas para controlar aquellas conductas delictivas realizadas a través del Internet, el Gobierno Federal ha llevado a cabo la implementación en el año 2000, de un órgano denominado Policía Cibernética, para combatir estos ilícitos y disminuir sus riesgos.

La Policía Cibernética pertenece a la Dirección General de Tráficos y Contrabandos, de la Secretaría de Seguridad Pública Federal, que además de las acciones de investigación y persecución en materia de delitos cometidos en Internet usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, basándose en cuatro objetivos básicos:

1. Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración y distribución y promoción de pornografía infantil.
2. Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos.
3. Realización de operaciones de monitoreo anti-hacker, utilizando Internet como instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.

4. Análisis y desarrollo de investigaciones en el campo sobre las actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

Asimismo este departamento dedicado a la seguridad informática, señala que un delito cibernético puede adoptar muchas formas y producirse prácticamente en cualquier momento y en cualquier lugar por criminales que utilizan métodos muy variados en función de sus habilidades y objetivos.

De esta forma encontramos que la posibilidad de que un usuario sufra un daño o una pérdida en Internet se incrementa al reunir tres factores:

1. Algo que tiene valor, es decir, la información de nuestra computadora, archivos, información personal, contraseñas, etcétera;
2. Amenaza, como un evento generado por una persona maliciosa que puede causar un daño o robo, y,
3. Vulnerabilidad, como la falla o deficiencia de un sistema o programa informático.

Aunque si bien es cierto que aún no se ha desarrollado un mecanismo integral que brinde control sobre hackers, virus, códigos maliciosos, phishing, etcétera, también lo es que sí podemos evitar las vulnerabilidades de nuestra computadora e incrementar las medidas necesarias para minimizar cualquier amenaza.

De acuerdo con la información presentada en el 1er Congreso Navega Protegido realizado el 4 y 5 de Octubre del presente año por el Jefe del Departamento de

Delitos Cibernéticos de la Policía Cibernética, en nuestro país los principales delitos cometidos en Internet son:

Principales conductas ilícitas cometidas en Internet

Tipo I	• Robo de identidad y datos personales (Spyware) • Phreaking (mecanismos que vulneran la seguridad de los sistemas telefónicos). • Amenazas. • Fraudes en e-commerce (compra-venta en línea). • Clonación de tarjetas de crédito. • Robo de información. • Carding (utilización ilegal de tarjetas de crédito) • Traspasos ilegítimos. • Phishing (correos falsos para robar datos del usuario). • Extorsiones, secuestros o localización de objetivos.
Tipo II	• Pornografía infantil. • Explotación sexual comercial infantil.

- Lenocinio infantil en Internet.
- Abuso de menores.
- Turismo sexual en Internet.
- Robo y substracción de menores.

La Policía Cibernética, independientemente de las investigaciones que realiza, recibe gran parte de los casos por denuncias ciudadanas.

Por otro lado de acuerdo a un estudio realizado por el Sans Institute, dedicado a la capacitación sobre seguridad en equipo de cómputo y el Buró Federal de Investigaciones (FBI) ambas en los Estados Unidos de América, señalan que el 90% de los delitos informáticos pueden ser evitados si los usuarios siguen varias medidas de seguridad en sus equipos.[108]

[108] Cassou Ruiz, Jorge Esteban. "Delitos Informáticos en México". *Revista de Derecho Informático*, núm. 028, Consejo de la Judicatura Federal, México, Septiembre de 2006.

CAPITULO IV.- EL DELITO DE ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA PREVISTO EN EL CAPÍTULO SEGUNDO DEL TÍTULO NOVENO DE EL CÓDIGO PENAL FEDERAL.

4.1 Reforma del 17 de Mayo de 1999 mediante la cual se implementa en el Código Penal Federal el delito de acceso ilícito a sistemas y equipos de informática.

4.2 Sistemas y equipos de informática.

4.3 Diversos mecanismos de protección de datos electrónicos, sistemas y aplicaciones de seguridad.

4.4 El acceso ilícito a sistemas y equipos de cómputo pertenecientes al Estado y su relación con el delito de ejercicio indebido del servicio público.

4.5 Acceso ilícito a sistemas y equipos de cómputo integrantes del sistema financiero mexicano.

4.6 Implementación del tipo penal "delito informático" dentro de la legislación estatal en México y sus principales diferencias con el delito de acceso ilícito a sistemas y equipos de informática.

CAPITULO IV.- EL DELITO DE ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA PREVISTO EN EL CAPÍTULO SEGUNDO DE EL TÍTULO NOVENO DE EL CÓDIGO PENAL FEDERAL.

4.1 REFORMA DEL 17 DE MAYO DE 1999 MEDIANTE LA CUAL SE IMPLEMENTA EN EL CÓDIGO PENAL FEDERAL EL DELITO DE ACCESO ÍLICITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA.

El 17 de mayo de 1999 se publicó en el Diario Oficial de la Federación, la modificación al Título Noveno del Código Penal Federal con el nombre de "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática" en donde se adicionó un segundo capítulo con siete nuevos tipos penales, como un primer intento por parte de la LVII Legislatura de nuestro país por regular jurídicamente los llamados delitos informáticos.

Código Penal Federal

Reforma publicada el 17 de Mayo de 1999 en el Diario Oficial de la Federación

"EL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, D E C R E T A:

SE REFORMAN DIVERSAS DISPOSICIONES EN MATERIA PENAL

ARTICULO PRIMERO.- *Se reforman, adicionan y derogan los artículos 25; 40; 64, párrafos primero y segundo; 65, párrafo tercero; 70, párrafo último; 85; 86; 90, fracción I incisos b), c) y d); 167, párrafo primero y fracciones II y VI; 168 Bis; la denominación del Título Noveno del Libro Segundo; la denominación del Capítulo Único del Título Noveno del Libro*

Segundo; el Capítulo II del Título Noveno del Libro Segundo; 211 Bis 1; 211 Bis 2; 211 Bis 3; 211 Bis 4; 211 Bis 5; 211 Bis 6; 211 Bis 7; el Capítulo XI al Título Décimo del Libro Segundo; 222 Bis; 225, fracciones XXVII, XXVIII y los tres párrafos últimos; 253, fracción I inciso j); 254, fracción VII; 298; 307; 320; 366, fracciones I, II y párrafo último; 368, fracciones II y III; 368 Quáter; 376 Bis; 378; 381, primero y dos últimos párrafos; 381 Bis; 424, fracciones III y IV; 424 Bis, y 424 Ter, todos del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, para quedar como sigue:

TITULO NOVENO

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

CAPITULO I

Revelación de secretos

CAPITULO II

Acceso ilícito a sistemas y equipos de informática

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

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

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

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

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

Asimismo encontramos que el capítulo objeto del presente análisis fue adicionado mediante la inclusión de un tercer párrafo final en los artículos 211 bis 2 y 211 bis 3, mediante reforma con fecha del 24 de Junio de 2009, incluyendo el siguiente texto:

Reforma publicada el 24 de Junio de 2009 en el Diario Oficial de la Federación

"EL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, DECRETA:

SE ADICIONAN DIVERSAS DISPOSICIONES AL CÓDIGO PENAL FEDERAL.

Artículo Único. *Se adicionan un párrafo tercero al artículo 211 bis 2; un párrafo tercero al artículo 211 bis 3; un párrafo último al artículo 223; y los artículos 250 bis y 250 bis 1, todos del Código Penal Federal; para quedar como sigue:*

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

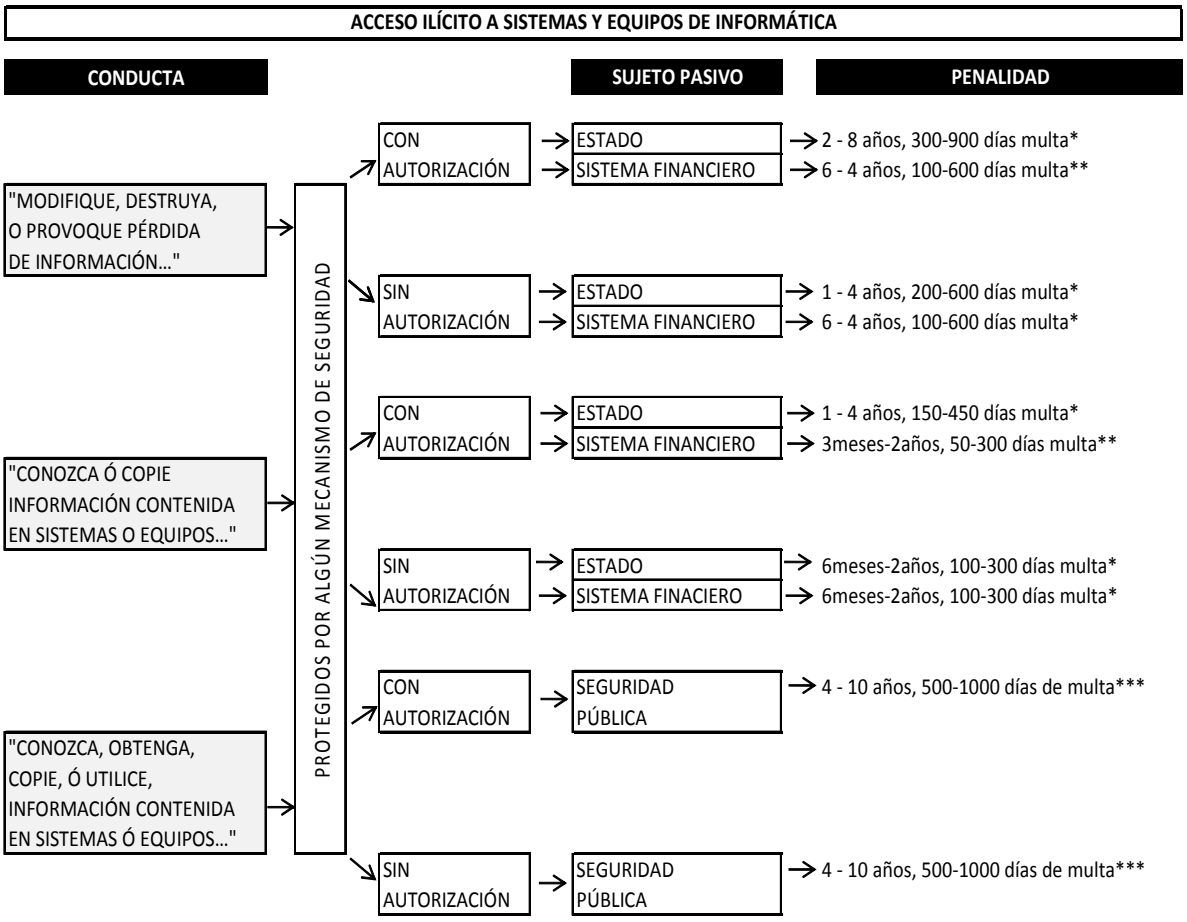
A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

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

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Para efecto de facilitar el análisis de los artículos anteriores, tenemos el siguiente esquema:



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

** Art. 211 Bis-5. "Las penas previstas se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero".

*** Art. 211 Bis-2. "Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública."

De esta forma podemos establecer que estas figuras delictivas incorporadas recientemente al código penal incluyen básicamente tres conductas:

a) Modificar, alterar, destruir o provocar pérdida de información,

b) conocer o copiar información, y

c) Conocer, obtener, copiar y utilizar información.

Estas dos conductas básicas sufren algunas variantes que influyen en la penalidad. Tales variantes son:

- Si el sujeto activo está autorizado o no para acceder a los equipos y a la información.
- Si se trata de sistemas protegidos por mecanismo de seguridad o no.
- Si pertenece al Estado, al Sistema Financiero o a cualquiera otra persona.

Existen asimismo algunas circunstancias que califican el delito aumentando la penalidad en un cincuenta por ciento. Tales calificativas son:

- Que la información se use en provecho de alguien.
- Ser empleado del sujeto pasivo.

No son delitos graves.- Cabe aclarar que ninguna de las figuras aquí comentadas ha alcanzado la definición de "delito grave" lo cual establece alguna dificultad en la persecución de estos delincuentes. En efecto, teniéndose el derecho a la libertad bajo fianza, es muy posible que estos delincuentes puedan obtenerla y evadir el proceso. No hay que olvidar que este tipo de delitos como ya hemos anotado con anterioridad usualmente es cometido por delincuentes que pueden operar en cualquier parte del mundo situación que compromete la jurisdicción y competencia. Debe considerarse seriamente el que algunos de estos delitos sean considerados graves, especialmente aquellos que tengan el potencial de causar daños cuantiosos o que sean el camino asociado a la comisión de otros delitos.

4.2 SISTEMAS Y EQUIPOS DE INFORMÁTICA.

Sin pretender elaborar un análisis más profundo acerca de la naturaleza de un sistema informático, para efectos de continuar con el estudio y la correcta interpretación del delito que nos ocupa, mencionaré una breve aproximación acerca de este tema.

Iniciaremos nuestra investigación definiendo en primer lugar, cual es el significado de "*sistema y equipo de informática*" al cual hace referencia el legislador en el multicitado capítulo en estudio.

Así tenemos que un sistema informático, como todo sistema, es "un conjunto de partes interrelacionadas, en este caso específico conformado por elementos de hardware, software y de recursos humanos".[109] Un sistema informático típico emplea una computadora que usa dispositivos programables para ingresar, almacenar y procesar datos. De esta forma encontramos entonces que una computadora personal o PC, junto con la persona que lo maneja y los periféricos que los envuelven, resultan un ejemplo de un sistema informático.

Se puede definir un sistema informático grosso modo como la unión de diversos elementos, especialmente el hardware, el software y un soporte humano que los controla o administra. [110] Por hardware podemos entender como todos aquellos componentes que físicamente componen al sistema y que pueden incluir una o varias Unidades Centrales de Procesamiento (CPU), módulos de memoria, sistemas de almacenamiento externo, como por ejemplo los discos duros, flexibles (disquetes) y compactos (CD). El software se refiere al conjunto de instrucciones lógicas que se han programado en el equipo para que éste funcione incluyendo dentro de éste ámbito al sistema operativo, firmware y demás aplicaciones, siendo

[109] "Sistema (informática)" Microsoft® Student 2009 [DVD]. Microsoft Corporation, 2008
[110] Téllez Valdés, Óp. Cit. Pág. 12

especialmente importante los sistemas de gestión de bases de datos. Por último el soporte humano incluye al personal técnico (administradores, analistas, programadores, operadores, etc.) que crean y/o mantienen el sistema y a los perfiles que los usuarios utilizan.

De esta forma podemos concluir que para efectos de la interpretación del precepto legal objeto de este estudio podemos definir a los sistemas o equipos informáticos como cualesquiera conjuntos o unidades de máquinas, aparatos, sistemas, equipos de informática o en general cualquier dispositivo, ya sea electrónico, óptico, magnético, o de cualquier otra tecnología, que realice funciones lógicas, aritméticas, transmisión, procesamiento o almacenamiento de datos de cualquier naturaleza, así como para el tratamiento sistemático de la información mediante el procesamiento automático de datos electrónicos o de cualquier otra tecnología.

4.3 DIVERSOS MECANISMOS DE PROTECCIÓN DE DATOS ELECTRÓNICOS, SISTEMAS Y APLICACIONES DE SEGURIDAD.

Como ya hemos visto con anterioridad, el texto del multicitado capítulo exige una condicionalidad adicional para la correcta configuración del tipo, siendo ésta, la existencia de “un mecanismo de seguridad” que brinde alguna protección a los sistemas y equipos de informática objeto de estas conductas, por lo que continuaremos con el estudio de éste concepto.

Seguridad Informática.

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo por supuesto, la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y normas concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

La información contenida se ha convertido en uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general. y como principal contribuyente al uso de programas realizados por programadores.[111]

En el caso del delito de *acceso ilícito a sistemas y equipos de informática*, el bien jurídicamente tutelado lo constituye la propiedad de la información, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena.

Asimismo el artículo que establece este delito señala la necesidad de que el sujeto activo "*sin autorización modifique, destruya, conozca o copie, y provoque perdida de información, contenida en sistemas o equipos de informática*", también señala que para la correcta configuración de éste delito estos deben de estar "*protegidos por algún mecanismo de seguridad*".

Mecanismos de seguridad Informática.

Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existen una gran variedad de técnicas y mecanismos para asegurar un sistema informático, dentro de los que destacan debido a su gran aceptación y uso los siguientes:

[111] Fernández Delpech, Fernando. Óp. Cit. Pág. 90

- *Codificación de la información*: Se lleva a cabo a través de técnicas especializadas como la Criptología, Criptografía y Criptociencia, las cuales generan contraseñas para los datos difíciles de averiguar a partir de datos personales del individuo.
- *Vigilancia de red interna* de la corporación por medio de un monitoreo de sus servidores en tiempo real.
- *Tecnologías repelentes o protectoras*: Diversas tecnologías desarrolladas en software como el firewall (cortafuegos), antispyware (sistema de detección de intrusos), antivirus, llaves para protección de software, etc. Además de complementarse con el mantenimiento de los sistemas de información con las actualizaciones que más impacten en la seguridad.
- *Sistema de Respaldo Remoto*. El cual se implementa con el objeto de realizar un respaldo o copia de seguridad de los datos de la corporación en unidades de almacenamiento físicas existentes en una instalación diversa a la original mediante un servicio remoto.

Esto puede esto permite brindar de seguridad a los sistemas cumpliendo los siguientes objetivos generales:[112]

1) Restringir el acceso a ciertos usuarios a todos los programas y archivos.
2) Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan.
3) Asegurar que se utilicen los datos, archivos y programas correctos en el procedimiento elegido.
4) Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
5) Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

[112] Pérez Luño, Antonio. Óp. cit. Pág. 69

6) Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
7) Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

Dado lo anterior podemos resumir que para efecto de nuestro análisis el término “mecanismo de seguridad” incluye cualquier dispositivo físico o electrónico, palabra clave, código de acceso, programa de cómputo o equipo informático que tenga por objetivo proteger una computadora, un programa de cómputo o la información contenida en un, sistema o equipo informático contra:

a) Accesos internos o externos no autorizados;

b) Borrado, alteración o daño de información;

c) Ataque informático de cualquier índole;

d) Rechazo del emisor, receptor o destinatario de la información.

e) Copiado, distribución, uso ilícito o no autorizado.

4.4 EL ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE CÓMPUTO PERTENECIENTES AL ESTADO Y SU RELACIÓN CON EL DELITO DE EJERCICIO INDEBIDO DEL SERVICIO PÚBLICO.

Como hemos revisado con anterioridad la conducta sancionada por él capitulo en objeto de éste análisis consiste en la modificación, destrucción, pérdida, copia o conocimiento indebido de la información contenida en sistemas o equipos de informática, protegidos por algún mecanismo de seguridad, y asimismo la redacción de los consiguientes artículos nos brindan distintas variantes que inciden en la penalidad, que radican fundamentalmente en la autorización con la que puede o no contar el sujeto activo para acceder a dichos sistemas, además de la diferencia entre distintos sujetos pasivos en los que recae el ilícito.

Así encontramos que los artículos 211 Bis-2 y 211Bis-3, aumentan la penalidad en caso de que la conducta delictiva sea cometida en contra de un "sistema o equipo de informática del Estado", además de que establece como una agravante el hecho de que el sujeto activo cuente con autorización para acceder a dicha información y indebidamente la modifique, destruya, copie, o provoque su pérdida; para lo cual comenzaremos por delimitar el alcance de ésta expresión.

El Estado Mexicano.

Para desglosar a que hace referencia el legislador al utilizar La frase "sistema o equipo de informática del Estado", debemos recordar en primer término los elementos fundamentales de éste: la población, el territorio y el gobierno.

El Gobierno Federal es "el poder público que emana del pueblo, por el cual ejerce su soberanía nacional y representa jurídicamente a la nación"[113]. A su vez el

[113] Castrejón García, Gabino Eduardo. *Derecho Administrativo Constitucional*. Cárdenas Velasco Editores S.A. de C.V. México 2006, pág. 305

gobierno está constituido por los Poderes de la Unión, para el ejercicio del poder público.

Poder Ejecutivo.

Representado por el Presidente Constitucional, apoyándose en la administración centralizada y paraestatal, quien administra los fondos y recursos públicos y ejecuta los programas y acciones de gobierno. La Administración Pública Centralizada está conformada por la Presidencia de la República, las Secretarías de Estado, la Consejería Jurídica del Ejecutivo y la Procuraduría General de la República. La Administración Pública Federal se encuentra sectorizada por actividades, lo cual consiste en agrupar diversas dependencias y entidades por ramas de la actividad pública, atendiendo a las características de sus funciones y atribuciones. La Administración Pública Paraestatal está conformada por los Organismo Descentralizados, las Empresas de Participación Estatal, los Fideicomisos Públicos y las Instituciones Nacionales de Crédito.[114]

Poder Legislativo.

Integrado por la Cámara de Diputados, la Cámara de Senadores y la Comisión Permanente del Congreso de la Unión. El art. 136 constitucional establece que las legislaturas de los estados también forman parte del Poder Legislativo Federal excluyendo de manera tajante a la Asamblea Legislativa del Distrito Federal.

Poder Judicial.

Integrado por la Suprema Corte de Justicia de la Nación, Tribunales Colegiados de Circuito, Tribunales Unitarios de Circuito y Juzgados de Distrito.

[114] *Ibídem,* pág. 309

Instituciones de Seguridad Pública.

Por otro lado como ya hemos mencionado los artículos 211 bis 2 y 211 bis 3, fueron adicionados mediante la inclusión de un tercer párrafo final, el cual sanciona el ilícito cometido en contra de "cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública," para lo cual mencionaremos brevemente cuales son las instituciones que conforman dicha área, que si bien forma parte del Estado y podría ya estar contemplada en el párrafo anterior, incide en la variación de la penalidad debido a la condición que reviste dicha información.

Para poder definir cuáles son las instituciones o dependencias que pertenecen al rubro de la seguridad pública en nuestro país, nos remitimos en primer término a la legislación vigente:

LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA

TÍTULO PRIMERO
DISPOSICIONES PRELIMINARES.

ARTÍCULO 5°. Para los efectos de esta Ley, se entenderá por:

Fr. IX. *Instituciones de Procuración de Justicia:* a las Instituciones de la Federación y entidades federativas que integran al Ministerio Público, los servicios periciales y demás auxiliares de aquél;

Fr. X. *Instituciones Policiales*: a los cuerpos de policía, de vigilancia y custodia de los establecimientos penitenciarios, de detención preventiva, o de centros de arraigos; y en general, todas las dependencias encargadas de la seguridad pública a nivel federal, local y municipal, que realicen funciones similares…

Por otro lado el Gobierno Federal a través de su portal oficial en internet menciona como Instituciones de Seguridad Pública y Defensa Nacional:[115]

- El Centro de Inteligencia y Seguridad Nacional (CISEN)

[115] http://www.gob.mx/inicio/cuidadanos/temas/seguridad/

- La Secretaria de la Defensa Nacional (SEDENA)
- La Secretaría de Marina (SEMAR)
- La Procuraduría General de la República (PGR)
- La Secretaría de Seguridad Pública (SSP)

Ejercicio indebido del Servicio Público.

Asimismo en el supuesto de que el sujeto activo hubiera estado autorizado por razón de su cargo empleo o comisión dentro de alguna de las dependencias que forman parte del Estado al momento de cometer el delito de acceso ilícito a sistemas, dado que con la misma acción comete a su vez el delito de ejercicio indebido del servicio público, podemos considerar la aplicación del concurso ideal, y de esta manera el primero subsuma al siguiente ya que sin la realización de esta conducta no hubiera sido posible la comisión del delito de acceso ilícito sistemas y equipos de informática.

El capítulo II del Título Décimo, denominado Delitos cometidos por servidores públicos, del Código Penal Federal, establece en su Artículo 214 Fracción IV, lo siguiente:

CÓDIGO PENAL FEDERAL

TÍTULO DÉCIMO

DELITOS COMETIDOS POR SERVIDORES PÚBLICOS

CAPITULO II

ARTÍCULO 214. Comete el delito de ejercicio indebido del servicio público, el servidor público que:

Fr. IV. Por si o por interpósita persona, *sustraiga, destruya, oculte, utilice, o inutilice ilícitamente información* o documentación que se encuentre bajo su custodia *o a la cual tenga acceso*, o de la que tenga *conocimiento* en virtud de su empleo, cargo o comisión.

Asimismo el artículo 212 nos define con exactitud quienes deben entenderse por servidores públicos:

ARTÍCULO 212. Para los efectos de este Título y el subsecuente es *servidor público* toda persona que desempeñe un empleo, cargo o comisión de cualquier naturaleza en la Administración Pública Federal centralizada o en la del Distrito Federal, organismos descentralizados, empresas de participación estatal mayoritaria, organizaciones y sociedades asimiladas a éstas, fideicomisos públicos, en el Congreso de la Unión, o en los poderes Judicial Federal y Judicial del Distrito Federal, o que manejen recursos económicos federales. Las disposiciones contenidas en el presente Título, son aplicables a los Gobernadores de los Estados, a los Diputados a las Legislaturas Locales y a los Magistrados de los Tribunales de Justicia Locales, por la comisión de los delitos previstos en este título, en materia federal.

Así encontramos la siguiente Jurisprudencia para efectos de dar más claridad a lo anteriormente expuesto:

EJERCICIO INDEBIDO DEL SERVICIO PÚBLICO. La fracción IV del Artículo 214 del Código Penal Federal contempla una hipótesis que, literalmente no alude al aprovechamiento o destrucción de la papelería en blanco parcial e indebidamente empleada en una dependencia oficial. El tipo que se describe por estar inmerso en el Título Décimo del Código Penal Federal, examinado de forma integral, lleva a concluir que *el bien jurídicamente protegido*, es el no ejercicio arbitrario del empleo, cargo o comisión del servidor público, así como la fidelidad que deben regir los actos del mismo en el desempeño de su cargo. Bajo ese supuesto, debe entenderse que el delito se comete cuando se "*sustraiga, destruya, oculte o inutilice ilícitamente información o documentación que se encuentre bajo su custodia o a la cual tenga acceso, o de la que tenga conocimiento en virtud de su empleo, cargo o comisión*". Es decir, que el servidor se aproveche de su empleo y que por tener ese carácter y acceso a la información o a los documentos esta impedido para sustraerlos, destruirlos, etcétera, porque sobre la información, esta debe ser del conocimiento oficial, o porque la documentación forma parte de un acervo, como instrumento, constancia, etcétera, entendiéndose, por documentación para los fines de la

precitada hipótesis, la documental anexa, que obre en poder de la institución pública y que sea considerada con ese carácter por los códigos procesales o administrativos correspondientes.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO. Amparo directo 628/89. Alejandro Ovilla González. 13 de Septiembre de 1989. Unanimidad de votos. Ponente Gonzalo Ballesteros Tena. Secretaria María del Pilar Vargas Codina.[116]

EJERCICIO INDEBIDO DEL SERVICIO PÚBLICO Y FRAUDE. CASO EN EL QUE EL PRIMERO SE SUBSUME EN EL SEGUNDO. El delito de ejercicio indebido del servicio público a que se refiere la fracción IV del Artículo 214 del Código Penal Federal, *quedo inmerso* en el de fraude, cuando quedó demostrado que el quejoso sustrajo un talonario de cheques que estaba a su cargo, con el deliberado propósito de obtener un lucro indebido, y que mediante el proceder de su coacusado de falsificar en esos documentos las firmas habituales correspondientes a diversos clientes que tenían registrados en la institución bancaria pasiva, obtuvo, engañando a ésta, dicho lucro, *pues sin aquella sustracción no hubiera sido posible* llevar a cabo el fraude cometido en perjuicio del banco. Luego, *no puede estimársele* también como responsable de aquel ilícito.

TRIBUNAL COLEGIADO EN MATERIA PENAL DEL SÉPTIMO CIRCUITO. Amparo directo 44/96. Román Morales Jiménez. 26 de Agosto de 1996. Unanimidad de votos. Ponente: José Pérez Troncoso. Secretario: Marco Antonio Ovando Santos. [117]

[116] *Semanario Judicial de la Federación*. Séptima Época, Volúmenes 217-228,Sexta Parte, pág.267
[117] *Semanario Judicial de la Federación y su gaceta.* Tribunales Colegiados de Circuito. Novena Época, Tomo IV Noviembre de 1996, Tesis VII. P.45.P. pág. 433

4.5 ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE CÓMPUTO INTEGRANTES DEL SISTEMA FINANCIERO MEXICANO.

Para continuar con nuestro estudio de los diversos tipos penales contenidos en el Capítulo II del Título Noveno de nuestro Código Penal Federal, analizaremos más a fondo las conductas descritas en el Artículo 211 bis 4. Y Artículo 211 bis 5, las cuales reciben una condición agravante en caso de que el sujeto pasivo pertenezca a las "*instituciones que integran el sistema financiero".*

Sistema Financiero Mexicano.

El sistema financiero mexicano es coordinado por la Secretaría de Hacienda y Crédito Público, a través de tres Comisiones y del Banco de México, que controlan y regulan las actividades de las instituciones.

El Banco de México.

También llamado Banca Central tiene como actividad principal la regulación y el control de la política monetaria crediticia y cambiaria del país. Asimismo, es el representante del país en las negociaciones de deuda externa y frente al Fondo Monetario Internacional.

La Comisión Nacional Bancaria y de Valores.

Es la encargada de coordinar y regular la operación de las instituciones de Crédito de Banca Comercial o Múltiple y de Banca de Desarrollo, el Patronato del Ahorro Nacional y los fideicomisos del gobierno federal y las organizaciones auxiliares de crédito. Tiene a su cargo la vigilancia y auditoría de las operaciones bancarias y está autorizada a sancionar, en el caso que alguna institución viole la Ley General de Títulos y Operaciones de Crédito o la Ley General de Sociedades Mercantiles.

Además es la que tiene a su cargo principalmente regular y vigilar el mercado de valores, las operaciones bursátiles y las actividades de los agentes de bolsa, así como el estudio de las empresas que quieren participar en la bolsa, a través de la bolsa Mexicana de Valores, el Instituto para Depósito de Valores, las casas de bolsa, los agentes de bolsa, las sociedades de inversión y las sociedades operadoras de sociedades de inversión.

Comisión Nacional de Seguros y fianzas.

Es la encargada de coordinar y regular las operaciones de instituciones de seguros, las sociedades mutualistas y las instituciones de fianzas.

El sistema financiero mexicano, también llamado sistema bancario mexicano, está integrado por:

- El Banco de México.

- Las instituciones de crédito de Banca Múltiple y de Banca de Desarrollo.
- El Patronato del Ahorro Nacional.
- Fideicomisos del Gobierno Federal.
- Instituciones de seguros.
- Las sociedades mutualistas.
- Las instituciones de fianzas.
- La Bolsa Mexicana de Valores.
- Instituto para depósito de Valores.
- Las casas de bolsa.
- Los agentes de bolsa.
- Las sociedades de inversión.
- Las sociedades operadoras de sociedades de inversión.
- Banca Múltiple y la Banca de Desarrollo.

- Administradoras de fondos de ahorro para el retiro.
- Cualquier otro intermediario financiero o cambiario.

A su vez las instituciones de crédito están formadas por dos grandes grupos:

- La Banca de Desarrollo.
- La Banca Múltiple o comercial.

La Banca de Desarrollo está integrada por las instituciones encargadas de realizar la intermediación financiera con fines de fomento.

La Banca Múltiple o Comercial es aquella que está integrada por todas las instituciones encargadas de realizar la intermediación financiera con fines de rentabilidad, ésta última constituye el centro de la actividad financiera. Capta los recursos del público, sobre los que se constituye su capacidad de financiamiento y haciendo uso de ésta, principalmente en operaciones activas “créditos”, realiza su función de promover la creación y desarrollo de las empresas como complemento en la inversión de las sociedades industriales, comerciales y de servicios.

Las operaciones que pueden efectuar entre otras, son las siguientes:

- Recibir depósitos bancarios de dinero.
- Emitir bonos bancarios.
- Emitir obligaciones subordinadas.
- Constituir depósitos en instituciones de crédito y entidades financieras del exterior.
- Efectuar descuentos y otorgar préstamos o créditos.
- Expedir tarjetas de crédito.
- Practicar las operaciones de fideicomisos.

4.6 IMPLEMENTACIÓN DEL TIPO PENAL “DELITO INFORMÁTICO” DENTRO DE LA LEGISLACIÓN ESTATAL EN MÉXICO Y SUS PRINCIPALES DIFERENCIAS CON EL DELITO DE ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA.

Si bien el objetivo principal del presente trabajo es el análisis de la normatividad Federal, consideramos relevante hacer una mención del avance legislativo por parte de los las Entidades Federativas, con el objeto de complementar el análisis jurídico de los delitos informáticos objeto del presente trabajo.

Así encontramos que de manera muy particular podemos tomar como referencia de un intento innovador por parte de las legislaturas locales por regular éstas conductas al *Código Penal para el Estado de Sinaloa,* el cual incluye desde Junio de 2006 un capítulo exclusivo para este tema, ubicado dentro del Título Décimo denominado “delitos contra el patrimonio” de la parte especial, lo cual denota que la perspectiva del legislador que elaboró esta norma coincide con lo expuesto en esta tesis, referente a considerar que en el caso del acceso ilícito a sistemas de informática el bien jurídicamente tutelado es constituido principalmente por el derecho de propiedad que se tiene sobre la información contenida en estos equipos.

De esta forma tenemos que el Artículo 217 del Código Penal vigente para el Estado de Sinaloa señala lo siguiente:

CÓDIGO PENAL PARA EL ESTADO DE SINALOA

LIBRO SEGUNDO

PARTE ESPECIAL

TITULO DÉCIMO

DELITOS CONTRA EL PATRIMONIO

CAPÍTULO V

DELITO INFORMÁTICO

ARTÍCULO 217. *Comete delito informático, la persona que dolosamente y sin derecho:*

I. Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o

II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

De manera especialmente relevante, encontramos la intención del legislador de incluir de forma inédita el concepto de “delito Informático” por primera vez en una ley penal en nuestro país, además de brindar una definición diferente de éste delito incluyendo una variedad más amplia de conductas que integran el tipo, como lo son el *usar, o entrar a una base de datos o sistema de computadoras,* y además establece la limitante de que éste uso o entrada se dé con el propósito de *diseñar, ejecutar, o alterar* lo que consideramos mal nombrado “esquema o artificio”, y condicionando además estas conductas a que sean llevadas a cabo con la finalidad de defraudar, *obtener dinero, bienes o información.*

Así tenemos que la fracción primera de éste artículo es congruente con la ley Federal vigente en el sentido de proteger el acceso a la información contenida en los soportes informáticos de posibles intrusos, que por medio de diversos “artificios”, o mejor dicho, “técnicas informáticas”, puedan llegar a en un momento dado a vulnerar los mecanismos de seguridad implementados para tal efecto, además de requerir para su integración el “dolo” como elemento subjetivo del tipo, y “sin derecho”, con lo cual parece un intento del legislador local por establecer la “falta de autorización” para accesar a dicho sistema por parte del activo.

Por otra parte mientras que la primera fracción del artículo en comento sanciona únicamente la acción de *usar o acceder* a un sistema informático o a la información contenida en el mismo, tenemos que la segunda fracción de éste artículo abarca una variedad más amplia de conductas como lo son el *interceptar, interferir, recibir, usar, alterar, dañar o destruir,* lo que se denomina "*soporte lógico" ó "programa de computadora",* con lo que considero de manera personal aporta un elemento innovador al tipo al incluir en un primer término expresiones propias de la informática, la cuales brindan mayor exactitud y precisión respecto del objeto material del ilícito, ya que al nombrar "*soporte lógico*" se hace alusión no solo a un equipo informático determinado, sino a toda una amplia gama de dispositivos electrónicos que incorporen a su estructura la tecnología del procesamiento automatizado de datos, incluidos en este supuesto por mencionar algunos ejemplos: equipos diversos como tabletas digitales (Tablet Pc´s) y teléfonos inteligentes (Smart Phones), hasta equipos más básicos como las Terminales de punto de venta lectoras de códigos de barras, utilizadas en los centros comerciales, etc.

Además el uso del término "*programa de computadora*", como ya hemos mencionado con anterioridad, hace referencia al conjunto de instrucciones programadas en la memoria de los equipos informáticos (software), que tienen por objeto permitir la funcionalidad de dichos equipos, por lo cual la protección jurídica que pretende brindar este precepto alcanza incluso a éste elemento fundamental para el funcionamiento de cualquier sistema.

Para finalizar podemos mencionar también con respecto a la parte final de la segunda fracción de este artículo, que a diferencia de lo establecido en la ley Federal, no se limita solo a aquellos actos perpetrados en contra de "sistemas o equipos de informática", si no que incluye para tal efecto a la plataforma o base que sirve de sustento al sistema, al sistema en sí mismo, e incluso a la red de la que pueda forma parte dicho sistema.

CONCLUSIONES.

1.- Como primera conclusión con relación a nuestro trabajo encontramos una gran necesidad de regulación de los aspectos relacionados con las Tecnologías de la Información por parte del Derecho toda vez que como se expuso a lo largo del presente, existen en la actualidad una gran variedad de carencias y lagunas legales respecto a este tema.

2.- También podemos concluir que como consecuencia del desarrollo de estos avances tecnológicos, se han revolucionado en gran medida las formas de interacción de las personas físicas y morales, dando como resultado un universo nuevo de conductas y actos jurídicos mediante los cuales se producen una amplia gama de consecuencias jurídicas.

3.- Con respecto al Derecho Informático podemos concluir que si bien es una rama del derecho que actualmente presenta un importante crecimiento y desarrollo todavía presenta en su naturaleza diversas carencias que lo limitan y hacen cuestionable el hecho de que pueda considerarse como una rama autónoma del Derecho.

4.- De la teoría del delito podemos concluir que nos sirve de fundamento doctrinal para poder identificar aquellos delitos relacionados con equipos o sistemas de informática, de tal modo que nos aporta los elementos necesarios para poder analizar más a fondo estas conductas ilícitas.

5.- Con base en lo anterior podemos mencionar que con respecto a los llamados “delitos informáticos”, el Derecho poco a poco ha ido creando a través de diversos cuerpos legislativos alrededor del mundo una variedad de tipos penales adecuados a esta gama de conductas, dentro de los cuales podemos encontrar como bienes jurídicamente tutelados principalmente el patrimonio, la privacidad e intimidad de las personas, los derechos de propiedad intelectual, la identidad de los individuos, el funcionamiento de los sistemas informáticos y la propiedad de la información, entre muchos otros.

6.- Asimismo se concluye que estos delitos informáticos y en especial el delito de acceso ilícito a sistemas y equipos de informática, pueden ser clasificados como delitos de cuello blanco debido a las cualidades particulares y conocimientos específicos que posee el sujeto activo.

7.- También podemos concluir de nuestro estudio que el acceso ilícito a sistemas y equipos de informática, la interferencia o interrupción de comunicaciones, la piratería y otras violaciones en materia de derechos de autor, y el fraude por medios electrónicos, constituyen los ilícitos de mayor relevancia en nuestro país en materia de delitos informáticos debido a los graves daños que pueden ocasionar en el patrimonio y la intimidad de las personas.

8.- Atendiendo a este aspecto el Estado mexicano otorga mediante las Reformas de fecha 17 de mayo del 2000 publicadas en el Diario Oficial de la Federación, la creación de los artículos 211 bis 1 al 211 bis 7 en el Código Penal Federal, que en lo medular, tipifican comportamientos de los llamados *hackers* ó *crackers,* que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano o de las corporaciones de seguridad pública. Así encontramos que a grandes rasgos en este cuerpo normativo federal se sancionan el que un sujeto tenga acceso ilegal a dichos sistemas y los altere, dañe, modifique o provoque pérdida de la información que contienen.

9.- Sin embargo, en mi opinión, la complejidad y costo económico que representará el acreditar ante un juez penal un comportamiento ilícito que se ejecuta en el escenario virtual como el Internet por ejemplo, rebasa en mucho, los buenos deseos del legislador mexicano, reflejados en la reforma penal citada. Por otro lado hoy en día existe una acelerada creatividad legislativa de fondo y forma que se está impulsando a nivel mundial, principalmente en los países desarrollados, para hacer frente a tal fenómeno de la tecnología y a los comportamientos ilícitos que desafortunadamente traen aparejados dichos avances tecnológicos, por lo que considero que nuestros representantes deberán hacer lo propio en un momento dado y así crear y proponer nuevos tipos penales así como impulsar la creación de normas procesales enfocadas a la acreditación

de los delitos informáticos, para poder fundamentar y motivar la labor de los cuerpos especializados de investigación criminal como Unidad de Policía Cibernética, y brindar de esta manera un marco legal oportuno para la persecución de estos ilícitos.

10.- De igual manera, de forma muy particular considero necesario el establecimiento de programas de capacitación para los Agentes del Ministerio Público y Jueces especializados en el tema, así como impulsar la creación de plazas para los peritos en informática como auxiliares de las Procuradurías de Justicia Federal o Estatales, además de crear un sistema de autorizaciones y certificaciones especiales para los Ingenieros en Informática o Sistemas para que como peritos autorizados, auxilien a los abogados postulantes independientes y Jueces, así como procurar la celebración de tratados internacionales mediante los cuales, entre países, se convenga el auxilio mutuo para combatir y sancionar los comportamientos ilícitos por el ilegal aprovechamiento de las tecnologías informáticas, el Internet, y sus herramientas virtuales.

B I B L I O G R A F Í A.

1.- Aboso, Gustavo, Zapata, María. *Cibercriminalidad y Derecho Penal.* Ed. B de F Ltda. Buenos Aires, 2006.

2.- Castellanos Tena, Fernando. *Lineamientos Elementales de Derecho Penal*, *Parte General.* Editorial. Porrúa, Trigésima quinta Edición, México, 1994.

3.- Carrancá y Trujillo, Raúl. *Derecho Penal Mexicano, Parte General*. Ed. Porrúa. Tercera Edición, México, 1996.

4.- Cuello Calón, Eugenio. *Derecho Penal*, Editorial Nacional. Novena Edición, México, 1961.

5.-Fernandez Delpech, Horacio. *Internet: su problemática jurídica.* Ed. Abeledo Perrot. Argentina 2001.

6.- Giraldo, Jaime. *Informática Jurídica Documental*. Editorial Trillas, México 1990.

7.- González de la Vega, Francisco*. Derecho Penal Mexicano.* Editorial Porrúa, Décima Edición, México, 1970.

8.- Instituto de Investigaciones Jurídicas. *Diccionario Jurídico Mexicano*. Editorial Porrúa, S.A., Octava Edición, México 1995

9.- Jiménez Huerta, Mariano. *Derecho Penal Mexicano*. Editorial Porrúa, Tercera Edición, México, 1980.

10.-López Betancourt, Eduardo. *Teoría del Delito.* Editorial Porrúa, Décima Edición, México, 2002.

11.- López Betancourt, Eduardo. *Delitos en particular*. Ed. Porrúa, México, 2004.

12.-Nicoltello, Nelson*. Diccionario del Latín Jurídico.* Julio César Faira, Editor. Argentina, 2004.

13.-Núñez Ponce, Julio. *Nociones básicas del derecho de la Informática.* Ed. Tecnos, Madrid 1996.

14.-Oronoz Santana, Carlos. *Manual de Derecho Procesal Penal*, Noriega Editores, México, 2003.

15.-Palomar de Miguel, Juan. *Diccionario para Juristas*. Editorial Porrúa, México, 2000.

16.-Pavón Vasconcelos, Francisco. *Manual de Derecho Penal Mexicano*, Editorial Porrúa, Sexta Edición, México 1984.

17.-Pérez Luño, Antonio. *Ensayos de Informática Jurídica*. Distribuciones Fontamara, Segunda Reimpresión México, 2009.

18.- Porte Petit, Celestino, *Apuntamientos de la parte general de Derecho Penal.* Editorial Porrúa, México 1984.

19.-Soler, Sebastián, *Derecho Penal.* Editorial Tea. Buenos Aires, 1999.

20.-Téllez Valdés, Julio, *Derecho informático*. Ed. McGraw-Hill Interamericana, México, 2004.

21.-Villalobos, Ignacio. *Derecho Penal Mexicano*, Editorial Porrúa, Cuarta Edición, México 1983.