UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

SEMINARIO DE DERECHO ROMANO Y DE HISTORIA DEL DERECHO

“DELITOS INFORMÁTICOS EN DERECHO COMPARADO”

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN DERECHO

P R E S E N T A:

ZULEIKA MAREL HERNÁNDEZ GALLEGOS.

DIRECTOR DEL SEMIRARIO: DRA. SARA BIALOSTOSKY BARSHAVSKY

ASESOR: DR. ERIC TARDIF CHALIFOUR.

CIUDAD UNIVERSITARIA **2009.**

AGRADECIMIENTOS.

A la Universidad Nacional Autónoma de México.

Con orgullo y mi más profundo agradecimiento a mi alma mater por darme la oportunidad de aprender y crecer como persona, sin más requisito que el deseo de superación.

A la Facultad de Derecho.

Por brindarme grandes y valiosas oportunidades de aprender y desarrollarme en la vida.

A mis padres (Lucila Gallegos y Severo Hernández)

Con gran respeto y admiración como el resultado de todos sus esfuerzos, por ser las personas a quienes debo todo lo que soy, por su gran apoyo para lograr esta meta.

A mis hermanos (Ana y Carlos)

Gracias por todo el apoyo que he recibido durante este tiempo cada día crece más mi cariño, admiración y respeto.

Al Doctor Eric Tardif Chalifour.

Por el apoyo brindado durante este trabajo, por enseñarme a trabajar con un orden y por su amistad.

A mis mejores amigas (Ana e Ivonne)

A mis mejores y más grandes amigas por su amistad y cariño incondicional, cuya compañía y disponibilidad constituyeron una ayuda para mi superación, gracias por su motivación, pero sobre todo por lo que son.

A mis grandes amigos de toda la vida (Elizabeth, Paula, Dolores, Carolina, Brenda, Fernando, Raúl, Jesús)

Gracias por todo su apoyo y paciencia pero sobre todo por su amistad.

A cada persona que conocí aun cuando haya sido por poco tiempo, que me ha enseñado algo.

DELITOS INFORMÁTICOS EN DERECHO COMPARADO.

CAPÍTULO III. REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN MÉXICO Y OTROS PAÍSES.

CAPÍTULO IV. DELITOS INFORMÁTICOS: NECESIDAD DE UNA REFORMA A NIVEL NACIONAL E INTERNACIONAL.

INTRODUCCIÓN.

En la actualidad tanto en México como en todo el mundo se ha dado un gran desarrollo en la tecnología de la información y en la forma de llevar a cabo las actividades, ya que esta cambia debido a las diversas innovaciones que se crean en una diversidad de campos como lo son la ciencia, la tecnología, la informática, entre otras.

Por supuesto que en el campo del derecho hay cambios, pero estos son más pausados y más rigurosos de acuerdo a las variantes en la realidad que se van presentando.

Por lo anterior, es oportuno el desarrollo del presente trabajo debido al auge que está teniendo la tecnología y la información en todo el mundo, la cual se ha vuelto accesible a todas las personas para realizar un gran número de actividades.

Si bien es cierto que México no es un país de primer mundo con alta tecnología si tenemos acceso a una parte de esta, por tanto, estamos ante la imperiosa necesidad de establecer regulación jurídica sobre los conocidos “delitos informáticos”.

El presente trabajo se abordará en cuatro capítulos con la finalidad de tener un mayor entendimiento de lo que son los delitos informáticos, así como su desarrollo tanto en México como en otros países.

En el capítulo uno se tocará los conceptos fundamentales para entender al delito informático y estar en posibilidad de formar una definición sobre el mismo. Asimismo se denotará la importancia del derecho comparado en el tema que nos ocupa.

Por tanto es necesario hacer un análisis de cada uno de los doctrinarios que hablen sobre delitos informáticos, es decir, la forma en que los definen, los clasifican ¿Cómo y por qué surgieron? y las hipótesis que se pueden presentar.

En el capítulo dos se analizará lo referente a la teoría de delito, es decir, la forma de conceptualizar un delito, lo cual es de suma importancia porque en base a la teoría del delito se puede configurar el mismo.

No sólo basta con conceptualizar el delito, también se debe dar una regulación expresa para que los sujetos activos de los delitos informáticos no queden sin castigo y los delitos no queden impunes, y no sólo eso sino que se puedan clasificar exista un orden, un control, una forma de agruparlos y definirlos no solo para castigarlos sino para combatirlos y prevenirlos dentro de lo posible.

La necesidad de establecer un tipo específico para los delitos informáticos es importante para salvaguardar principios fundamentales establecidos en nuestra carta Magna.

Los artículos 14 y 16 de la Constitución Política de los Estados Unidos Mexicanos, son de suma importancia en un primer término el artículo 14 ya que a través de este se puede tener seguridad jurídica que es un rasgo imprescindible para las personas; específicamente en su párrafo tercero en donde se establece que “En los juicios del orden criminal queda prohibido imponer, por simple analogía y aún por mayoría de razón, pena alguna que no este decretada por una ley exactamente aplicable al delito de que se trata”.

Por lo anterior, se ve en la imperiosa necesidad de establecer un concepto base de delitos informáticos que si bien la tecnología va cambiando con rapidez puede establecer un tipo lo más exacto posible hasta el momento e irlo modificando de acuerdo a las necesidades.

Puesto que el capítulo “Acceso ilícito a Sistemas y equipos de Informática” por el momento a rebasado la realidad ya que deja fuera una diversidad de supuestos como la estafa electrónica, el fraude, los virus, etc., por tanto debe regularse.

El ya mencionado artículo 14 Constitucional no sólo contempla la seguridad jurídica sino también la legalidad, punto importante que hay que retomar en nuestra sociedad.

Otro de los preceptos constitucionales de relevancia es el artículo 16 Constitucional ya que abarca la legalidad y el hecho de que dicho artículo salvaguarda las garantías que otorga la Constitución.

Además abarca el hecho de que las comunicaciones son inviolables y la ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas.

Si bien en la Constitución Política de los Estados Unidos Mexicanos básicamente es una regulación que se dirige primordialmente al correo y a las líneas telefónicas el Internet no es algo que este regulado como tal, si se debe hacer hincapié en que el Internet si puede ser utilizado como medio de comunicación y no sólo como eso sino como medio para celebrar cualquier tipo de contrato.

Por lo cual debe regularse para que haya una seguridad en cuanto a la privacidad de los actos que se celebren utilizando cualquier medio de comunicación.

Se tiene que abordar los delitos informáticos tanto a nivel nacional como internacional por el rápido flujo que puede existir en la información y por la dificultad de encontrar al sujeto activo del delito, por lo que este tema será estudiado en el capítulo tres.

En algunos Estados de la República Mexicana se ha dado ya una regulación de delitos informáticos pero esto es insuficiente ya que sería necesario se diera una regulación en cada uno de los Estados o mejor aún sería más complementario que se diera una regulación a nivel Federal.

Asimismo, resulta trascendente tomar en cuenta lo relativo ha dicho tema tratado por organismos tanto nacionales como internacionales o países que se han referido a dichos delitos por lo que será motivo de estudio en el capítulo cuatro de la presente tesis.

No sólo es trascendental crear un tipo penal referente a los delitos informáticos, sino además es necesario que se de una capacitación a las personas encargadas de impartir justicia, la creación de un organismo especializado en la investigación de estos delitos.

O bien si no se crea un organismo se cree un área específica en alguno de los Organismos establecidos, para que los investiguen. Así como una red o alianza en el campo internacional para una mayor seguridad jurídica.

En conclusión resulta imperante que se establezca en el Código Penal Federal y en los Códigos Penales a nivel Estatal un tipo concreto de “delitos informáticos”, se establezcan las hipótesis que se pueden suscitar en dicho tipo, así como las penas a que se harán acreedores las personas que realicen dicho acto comisivo.

Para lo cual es necesaria la utilización del derecho comparado y de esa forma poder observar los lineamientos y figuras que son utilizadas en otros países las cuales podrían ser aplicadas en México, asimismo descartar o darnos cuenta de que es lo que no funciona y por tanto no implementarlo y tomar otras medidas.

Por último, crear un organismo especializado para la investigación y persecución de estos delitos, así como establecer una cultura no sólo para proteger la seguridad de las personas contra este tipo de delitos sino para prevenirlos.

DELITOS INFORMÁTICOS.

CAPÍTULO I. CONCEPTOS FUNDAMENTALES.

En el presente capítulo se abordará de manera clara y breve los conceptos fundamentales necesarios para comprender y establecer qué son los delitos informáticos.

Por otro lado, se señalarán los antecedentes que se dieron en los diversos países que los contemplan, así como la forma en que se ha desarrollado el presente tema en nuestra legislación y la forma en que fueron contemplados desde su origen hasta la actualidad.

1. Antecedentes de los delitos informáticos.

La concepción de delitos informáticos es reciente. No existe fecha precisa del primer ilícito informático.

Al conectarse con servicios de comunicaciones y de información, a través del uso de redes los usuarios, es decir, las personas que accedan a estas, crean una especie de espacio común que es conocido como "ciberespacio", que es utilizado con fines legítimos pero que también puede ser objeto de un mal uso.

Este tipo de medios es utilizado para fines ilícitos ya sea que se cometan contra la integridad, la disponibilidad y la confidencialidad de los sistemas informáticos y las redes de telecomunicaciones o bien consisten en el uso de dichas redes o sus servicios para cometer delitos tradicionales, vg. robo, fraude, etc.

Se necesita un esfuerzo tanto en nuestras normas nacionales como una cooperación internacional para tratar el mal uso de las redes de información, esto es, debido a la naturaleza transfronteriza de este tipo de delitos, se entraría al estudio de un problema jurisdiccional y por consiguiente se tendría que regular cual es el país que debe aplicar su legislación y como hacerlo si se ven implicados varios países, la dificultad de esto radica en el hecho de que hay países más avanzados que otros en el ámbito tecnológico.

1.1 Historia internacional de los delitos informáticos.

Los delitos informáticos son de creación reciente y se tienen pocos datos acerca de como surgieron, es decir, se contemplan de manera muy somera y solo por algunos tratadistas.

"La primera propuesta para legislar sobre delitos informáticos se presentó en 1977 por el Senador Robicoff en el Congreso Federal de los Estados Unidos de América".[1] En 1983 en París, la Organización de Cooperación y Desarrollo Económico (OCDE) designó un comité de expertos para discutir los crímenes relacionados con las computadoras y la necesidad de cambios en los Códigos Penales; se recomendó alguna modificación en los códigos penales en donde pudieran incluir los delitos informáticos o algunos delitos en esta área que fueran comunes entre sí.

La OCDE inició un estudio sobre la posibilidad de armonizar leyes sobre éstos delitos en el ámbito internacional por lo que en 1986 publicó un informe, llamado "Delitos de informática: análisis de la normativa jurídica", con recomendaciones las cuales versaban sobre los usos indebidos en estos delitos así como lo que podrían prohibir y sancionar a través de sus leyes penales los diversos países.

[1] López Betancourt Eduardo, "Delitos en Particular, Tomo IV", Editoral Porrúa, México, 2004 p.274.

El 13 de septiembre de 1989, el Consejo de Europa presentó una lista mínima de los delitos que debían necesariamente agregarse a las legislaciones de cada país miembro, junto con una lista opcional.

El tema fue abordado y estudiado en 1990 tanto en el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado de Montreal como en el Octavo Congreso Criminal de las Naciones Unidas y en la Conferencia de Wurzburgo, en Alemania, en 1992.

En el año de 1995 el Consejo de Europa adopta una recomendación sobre problemas de derecho procesal conectados con la información tecnológica. En 1996, se creó un nuevo comité de expertos para que abordaran el tema de delitos informáticos.

El comité inició su labor en abril de 1997 y efectuó negociaciones con respecto al borrador de un convenio internacional en materia de delitos informáticos. El Comité de Ministros estableció el nuevo comité denominado: "Comité especial de expertos sobre delitos relacionados con el empleo de computadoras (PC-CY)" por decisión nº CM/Del/Dec(97)583, tomada en la 583ª reunión de los representantes de los Ministros la cual fue celebrada el 4 de febrero de 1997.

Con el fin de combatir los delitos informáticos se elaboró un borrador del instrumento legal obligatorio al recién formado “Comité Especial de Expertos sobre delitos relacionados con el empleo de las computadoras”. Esto debido a que una recomendación no es suficiente ya que no tendría poder coercitivo por lo que se decidió elaborar un convenio.

Los puntos de consulta fueron acerca de los siguientes temas:

- ✓ Los delitos informáticos, en particular aquellos cometidos mediante el uso de las redes de telecomunicaciones.

- ✓ Cuestiones de derecho penal sustantivo, donde puede ser necesario un enfoque común a fin de lograr una cooperación internacional en cuanto a definiciones, sanciones y la responsabilidad de los actores en el ciberespacio, incluyendo a los proveedores de estos servicios.
- ✓ La posibilidad del uso transfronterizo y la aplicabilidad de los poderes coercitivos en un entorno tecnológico, la prohibición de acceder a material ilegal y el requerimiento de que los proveedores de servicios cumplan con obligaciones especiales, teniendo en cuenta los problemas causados por ciertas medidas de seguridad de la información, como puede ser la encripción.
- ✓ El problema de la jurisdicción en relación con los delitos relacionados con la tecnología de la información, para poder determinar el lugar donde se cometió un delito y por consiguiente cuál es el derecho que corresponde aplicar, incluyendo el problema de múltiples jurisdicciones.
- ✓ El problema de la cooperación internacional en la investigación de los delitos informáticos, en estrecha cooperación con el comité de expertos sobre el funcionamiento de los convenios europeos en el campo penal (PC-OC).

En 2001, el texto del borrador del convenio fue sometido a consideración del Comité de Ministros para su aprobación y quedó abierto para su firma.

Entre los principales objetivos del convenio se encuentran:

1. Armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones relacionadas en materia de delitos informáticos.
2. Establecer conforme al derecho procesal penal de cada país, las facultades necesarias para la investigación y el procesamiento de dichos delitos así como otros delitos cometidos mediante el uso de un sistema informático o las pruebas relacionadas que se encuentren en formato electrónico.

3. Establecer un régimen rápido y eficaz de cooperación internacional.[2]

El documento comienza con un preámbulo dirigido a los estados miembros del mencionado consejo y demás países signatarios del convenio, en el cual se establece la necesidad de alcanzar como una cuestión prioritaria una política criminal común dirigida a la protección de la sociedad contra los delitos informáticos, aprobando entre otras cosas una legislación que sea apropiada a tal fin y fomentando la cooperación internacional entre los Estados. Por otro lado en sus capítulos aborda el tema de la manera siguiente:

El Capítulo I se refiere a las definiciones de los términos que se utilizaran en el resto del convenio.

El Capítulo II (cuestiones de derecho sustantivo) abarca disposiciones sobre delitos y otras relacionadas referentes al área de los delitos informáticos o los delitos relacionados con el empleo de computadoras: primero define 9 delitos agrupados en 4 diferentes categorías, luego versa sobre la responsabilidad secundaria y las sanciones.

La sección II del Capítulo II se refiere a cuestiones de Derecho procesal, cuyo alcance va más allá de los delitos definidos ya que se aplica a cualquier delito cometido a través de un sistema informático o cuya evidencia se encuentre en formato electrónico, determina en primer lugar las condiciones y salvaguardas comunes aplicables a todas las facultades procesales contenidas en este capítulo finaliza con las disposiciones referentes a la jurisdicción.

El Capítulo III contiene las disposiciones concernientes a la asistencia mutua en relación con los delitos tradicionales y con los delitos relacionados con el uso de computadoras, así como también las referentes a la extradición.

[2] http://www.delitosinformaticos.com.mx/legislacion.htm, 20/01/2008.

Finalmente, el Capítulo IV contiene las disposiciones finales, las cuáles (con ciertas excepciones) repiten las disposiciones convencionales de los tratados del Consejo de Europa.

1.2 Historia nacional de los delitos Informáticos.

La Legislación en México incluyó los delitos informáticos con las reformas publicadas en el Diario Oficial de la Federación el 17 de mayo de 1999.

Los tipos se encuentran regulados en el Título Noveno Capítulo II, con el Título "Revelación de secretos y acceso ilícito a sistemas y equipos de informática". Se encuentra regulado del artículo 211 BIS 1 al 211 BIS 7 del Código Penal Federal.

La exposición de motivos de esta Reforma, en términos generales señala lo siguiente:[3]

El avance logrado en los últimos años en el sector tecnológico ha permitido que un número creciente de personas tengan acceso a él y por tanto la utilicen cotidianamente para realizar actividades de muy diversas índoles, como las educativas, culturales, comerciales, industriales, financieras o de comunicación, entre otras.

Debido a este avance tecnológico surgen nuevas formas de conducta antisocial que ha hecho de los equipos y sistemas informáticos, instrumentos o medios para delinquir.

Dentro de las conductas ilícitas más comunes que constituyen los "delitos informáticos", se encuentran: el acceso no autorizado a computadoras o sistemas

[3] López Betancourt Eduardo, *op. cit.*, p. 275-276.

electrónicos, la destrucción o alteración de información, el sabotaje por computadora, la intercepción de correo electrónico, el fraude electrónico y la transferencia ilícita de fondos.

La exposición de motivos también manifiesta el punto de vista en un contexto internacional, en el cual la Organización de las Naciones Unidas ha reconocido que los delitos por computadora constituyen un grave problema, ya que las leyes, los sistemas de impartición de justicia y la cooperación internacional no se han adecuado a los cambios tecnológicos, por lo que se necesita crear medios para combatir este tipo de conductas. Además se da como ejemplo el hecho de que países pertenecientes a la Unión Europea tienen una regulación en el campo cibernético.

Algunos países optaron por establecer estos delitos como una ley específica mientras que otros han preferido que se encuentren incluidos en sus códigos penales.

El país está obligado a proteger los bienes jurídicos de los sectores que utilizan la informática como instrumento de desarrollo; y es el caso de Sinaloa que ha incorporado en sus ordenamientos penales normas tendientes a la protección de la información.

La inexistencia a nivel federal de tipos penales aplicables, ha dado lugar a que sus autores queden impunes, por lo que se debe hacer algo.

La iniciativa propone adicionar un capítulo al Código Penal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar o provocar la pérdida de información que contenga.

El bien jurídico que se pretende tutelar es la privacidad y la integridad de la información, además imposición de penas mayores cuando sea realizado en agravio del Estado o de entidades financieras

2. Delitos informáticos.

Para emprender el estudio de los llamados delitos informáticos es necesario tener una idea clara de los conceptos que se relacionan con esta materia, en virtud de que para la comprensión y mejor tratamiento de los mismos se requiere de un vocabulario específico.

2.1 Conceptos clave para el desenvolvimiento de los delitos informáticos.

Acceso no autorizado a servicios y sistemas informáticos.

Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la simple curiosidad, el sabotaje o el espionaje informático.

El convenio del comité de expertos sobre el funcionamiento de los convenios europeos en el campo penal lo maneja como acceso ilegal y lo define de la siguiente manera: cuando se efectúe de manera intencional, el acceso a un sistema informático o a una parte del mismo sin permiso. Se deja opción a las partes signatarias para que requieran que el delito sea cometido infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención dolosa o en relación con un sistema informático que esté conectado con otro sistema informático.

Se entenderá como interceptación ilegal: interceptación intencional sin permiso de trasmisiones de datos informáticos de carácter no público efectuada desde o dentro de un sistema informático, incluyendo las emisiones electromagnéticas desde un sistema informático que transporta dichos datos informáticos.

Cibernética.

"Tiene su origen en la voz griega kybernetes, "piloto" y kibernes, concepto referido al acto de gobernar. Es la ciencia de la comunicación y control".[4]

"La cibernética estudia, por tanto, lo que tienen en común los diferentes mecanismos de control."[5]

Ciberpiratas.

"Son aquellos que roban propiedades de terceros en la red para después extorsionar a los legítimos titulares o venderlos al mejor postor".[6]

Los ataques preferidos de los piratas informáticos son de tres tipos:

1. Violación a la privacidad de los mensajes de correo electrónico.
2. Acceso a ordenadores remotos para utilizar la información que contiene.
3. Bloqueo de ordenadores mediante programas especializados, evitando que sus usuarios los puedan utilizar.[7]

Computación.

"En informática, conjunto de disciplinas y técnicas desarrolladas para el tratamiento automático de la información mediante máquinas computadoras (hardware) que funcionan con distintos programas (software)".[8]

Computadora.

"Es un dispositivo electrónico que interpreta y ejecuta comandos programados para operaciones de entrada y salida de datos, de cómputo y lógicos. Máquina

[4] Tellez Valdes Julio, "Derecho informático", tercera edición, Editorial Mc Graw Hill, México, 2004, p.3.
[5] LIMA VIANNA Tulio, *"*La era del control. Introducción crítica al derecho penal cibernético*"*, *Ciencias Penales*, Año 16, Número 22, Costa Rica, Septiembre, 2004, p.43.
[6] Molina Salgado Jesús Antonio, "Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial", Porrúa, México, 2003, p.17.
[7] Carballar Falcón José A, "Internet libro del navegante", España, Editorial Ra-Ma, 3ª edición, p. 357.
[8] Campoli Gabriel Andrés, "Derecho penal informático en México", Instituto Nacional de Ciencias Penales", México, 2004, p.10.

compuesta de elementos físicos, en su mayoría electrónicos, capaz de realizar de acuerdo con las instrucciones que se le den, una serie de trabajos a gran velocidad y con gran precisión".[9]

La computadora tuvo una evolución importante. Se dio a través de lo que se llama generaciones de computadoras.

- Primera generación. Utilizaron bulbos de alto vacío como componentes básicos de sus circuitos internos.
- Segunda generación. Se introdujeron las memorias de ferrita que permitieron reducir el tamaño.
- Tercera generación. Usó circuitos integrados monolíticos que aumentaron la velocidad de operación.
- Cuarta generación. Contaban con microcircuitos integrados en plaquetas de silicio.

La computadora cuenta con los siguientes elementos:

- Elementos de entrada. Como pantalla, discos, etc.
- Procesador central. Es la unidad central de proceso. En esta se da el procesamiento lógico.
- Dispositivo de almacenamiento. Almacena la información.
- Elementos de salida. Reciben resultados del proceso.
- Hardware. Es constituida por las partes mecánicas, electromecánicas y electrónicas, es la estructura física de las computadoras.
- Software. La parte lógica de la computadora que le permite ejecutar actividades.

Cracker.

"Proviene de "crack" que significa romper algo o descifrar un código y sirve para identificar a quienes entran simplemente en sistemas informáticos de terceros

[9] López Betancour Eduardo, *op.cit.*, p.269.

constantemente".[10] Persona que sin derecho penetra un sistema informático con el fin de robar o destruir información valiosa, realizar transacciones ilícitas, o impedir el buen funcionamiento de redes informáticas o computadoras. Alguien que viola la seguridad en un sistema.

Delito.

El Código Penal Federal lo define como el acto u omisión que sancionan las leyes penales.

"Es el acto u omisión del ser humano, descrito en la ley penal, realizado con pleno control y sin justificación legal, con el cual se atenta, altera o destruye un bien jurídico penal".[11]

"El delito es: la infracción de un deber exigible, en daño de la sociedad o de los individuos (Rossi); en un ente jurídico constituido por una relación de contradicción entre un hecho y la ley; es la infracción de la ley del Estado promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso (Carrara), es la violación de un derecho (Frank); es la violación de un derecho o de un deber (Tarde); de un ángulo histórico es toda acción que la conciencia ética de un pueblo considera merecedora de pena, en determinado momento histórico; y desde el ángulo valorativo , todo acto que ofende gravemente el orden ético y que exige una expiación consistente en pena José Maggiore)"[12]

Electrónica.

"Ciencia que estudia dispositivos basados en el movimiento de los electrones libres en el vacío, gases o semiconductores, cuando dichos electrones están

[10] Molina Salgado Jesús Antonio, *op. cit.*, p.17
[11] Hernández Islas Juan Andrés, "Mitos y realidades de la teoría del delito", Editorial Jahia, México, 2006, p.35.
[12] Carranca y Trujillo Raúl y Carrancá y Rivas Raúl, "Derecho penal mexicano. Parte general", Vigésimo primera edición, Editorial Porrúa, México, 2001, pp.220 y 221.

sometidos a la acción de campos electromagnéticos. (Diccionario Nuevo Mundo de la Lengua Española, ediciones Nuevo Mundo, España, 1999)".[13]

Hacker.

"Es un término empleado para identificar indistintamente a un "programador habilidoso", o bien a un "allanador de sistemas informáticos que altera programas".[14] Individuo que sin derecho penetra un sistema informático sólo por gusto o para probar sus habilidades.

Además los hackers tienen una serie de características como son:

1. Son personas con capacidades en el campo de la tecnología.
2. Personas inteligentes en una diversidad de materias.
3. Tienen conocimientos en materia de programación. (Cuando menos UNIX).
4. Suelen tener una identidad secreta a través de la red por medio de un nombre en la red mejor conocido como "nick".

Otra cosa que los caracteriza es que "acostumbran a tener una actitud antisistémica y ansían obtener conocimientos prohibidos, impulsados por una curiosidad insaciable"[15].

Informática.

"Tratamiento automático de la información".[16] Es decir, conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información para una adecuada toma de decisiones.

[13] Campoli Gabriel Andrés, *op.cit.* p.10.
[14] Molina Salgado Jesús Antonio, *op.cit*. p.17
[15] R. Nielsen Daniel, *"*Los casos más usuales de criminalidad informática y cibernética*"*, *Revista Catalana de Seguretat Pública. Los nuevos retos en la investigación de delitos*, Editorial Escola de Policia de Catalunya, Número 3, Diciembre, 1998, 23.
[16] López Betancourt Eduardo, *op. cit.*, p.269.

Internet.

Sobre este punto nos detendremos un poco, debido a que es de suma importancia entender como surgió y como se desarrolla ya que es una de las formas más comunes, sino es que la más usada de los delincuentes informáticos para auxiliarse de la misma y cometer sus crímenes.

La palabra Internet es una contracción de Internetwork system (sistema de intercomunicación de redes) y es un conjunto de redes locales conectadas entre sí a través de una computadora especial por cada red, conocida como gateway. Es una red que se diseñó para una serie descentralizada y autónoma de uniones de redes de cómputo, con la capacidad de transmitir comunicaciones rápidamente sin control de persona o empresa comercial alguna y con la habilidad automática de enrutar datos, si una o más uniones individuales se dañan o están por alguna razón inaccesibles.

En los años sesenta, los investigadores comenzaron a experimentar con la posibilidad de crear redes de computadoras que fueran veloces y confiables, por lo que nació la idea de las redes de conmutación de paquetes; la información que viaja a través de la red se divide en cierto número de fragmentos, llamados paquetes.

Estos paquetes no sólo incluyen la información entres sí, también contienen datos del domicilio del destino final y del orden que tienen en la transmisión. Los paquetes se transmiten a través de la red y con el tiempo llegan al destino deseado, después se reensamblan y una computadora que se encuentra al otro extremo de la red recibe el mensaje.

En 1969, el departamento de defensa estadounidense, a través de la Agencia para Proyectos de Investigación Avanzada (ARPA, Advanced Research Projects Agency), creó una red experimental de conmutación de paquetes utilizando las líneas telefónicas.

Del conjunto inicial de redes nació una red denominada Arpanet la cual es, es uno de los primeros antecedentes de Internet. ARPANET permitió a científicos, investigadores y personal militar ubicados en diversos puntos, comunicarse entre sí utilizando éstas redes; por lo que otros centros de cómputo no conectados a ARPANET se percataron de las ventajas de la comunicación electrónica. Se encontraron una diversidad de formas de conectar redes privadas.

En los ochenta, más usuarios se unieron a Internet, por lo que el papel de ARPANET fue disminuyendo, y se fueron creando otras redes.

La Internet no tiene personal de mantenimiento, no hay compañía o agencia que establezca reglas y que por tanto logre que se utilice adecuadamente, sin embargo, existe una organización de usuarios llamada Sociedad Internet (también conocida por las siglas ISOC, Internet Society) integrada por voluntarios cuya única meta es promover el intercambio global de la información a través de la tecnología que es utilizada en Internet.

Los líderes de ISOC integran el "Consejo de Arquitectura de Internet, en ellos recae la tarea de administrar y dirigir técnicamente a Internet".[17]

Las redes son un medio para transportar información, algunas computadoras necesitan utilizar programas especiales, un ejemplo de estos programas es el denominado Unix el cual es pertenece a una familia de sistemas operativos de las más usadas para poder tener cierto control sobre una computadora.

La Internet proporciona un sin número de servicios, existen algunos más comunes que otros, entre ellos se encuentran los siguientes:

1. Servicio de correo electrónico mediante el cual existe una comunicación ya que se transmite y recibe mensajes.

[17] Este extracto se obtuvo de Wyatt Allen L., "La magia del Internet", Mc Graw – Hill, México, 1995.

2. Servicio de Telnet, permite establecer una sesión de trabajo con una computadora remota (es decir, para conectar con una computadora que tenga terminal en otro lado, diferente ubicación, vg. de un país a otro.
3. Se llama FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos). Esta permite transferir archivos de una computadora a otra.
4. Programa cliente, este puede conectar con otra computadora y solicitar ayuda de un programa servidor.[18]

SEGURIDAD EN INTERNET.

La seguridad física de los equipos.

Se refiere a la protección de los equipos contra vandalismo, incendio, sobretensiones, etc. Cualquiera de estas causas puede hacer que los equipos no puedan seguir realizando su función.

Esta seguridad se garantiza mediante sistemas de vigilancia, control de accesos, detención y prevención de accidentes, protectores contra sobretensiones, etc.

La seguridad funcional de los equipos.

Se refiere a garantizar el funcionamiento de los equipos frente a riesgos de fallos, pérdida de información, presencia de virus, etc. Esta función se garantiza con medidas preventivas a nivel sistema.

La seguridad de los contenidos.

Se refiere a garantizar que los contenidos no sean alterados, borrados o utilizados fraudulentamente por personas propias o ajenas.

[18] Harley Hahn y Rick Stout, "Internet. Manual de referencia", Mc Graw – Hill – Interamericana, España-México, 1999, p.16

Ante estos riesgos aparecen dos grupos de protecciones:

1. Protección de los entornos.
2. Protección de las comunicaciones.

Las estrategias de seguridad informática tienen que cumplir cinco funciones principales:

1. Deben disuadir a la gente de intentar cometer acciones no autorizadas.
2. Las medidas de seguridad deben prevenir la exitosa ejecución de los delitos informáticos.
3. Las estrategias de seguridad deben detectar los delitos informáticos con el fin de evitar la ejecución de acciones completas, de prevenir la realización de intentos, permitir la corrección y recuperación y en general disuadir a los delincuentes potenciales.
4. Las estrategias de seguridad deben minimizar los efectos y daños de los delitos informáticos que no hayan podido preveerse y simplificar la recuperación y corrección.
5. Cumplir las exigencias legales.

Legislación Informática.

"Es un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso de la informática".[19]

Phreaker.

"Se utiliza para denominar a cualquiera que use sus conocimientos para hacer daño, por gamberrismo, terrorismo, venganza u otras múltiples razones..."[20]

[19] Téllez Valdés Julio, *op. cit.*, p23.
[20] Marcelo Rodao Jesús de, "Piratas cibernéticos", 2ª edición, Editorial Ra-Ma, p.151

Penetrar ilícitamente sistemas telefónicos o de telecomunicaciones con el fin de obtener beneficios o causar perjuicios a terceros.

Piratería (Hacking).

"La piratería es el acceso no autorizado a un sistema de procesos de datos a través de un proceso de datos a distancia, no cometido con finalidades manipulatorias, fraudulentas, de espionaje ni de sabotaje sino sencillamente como placer no autorizado (joyriding) por el ordenador de otra empresa (hackito ergo sum) puede ser catalogado como una forma especial de hurto de servicios".[21]

Programa.

"Conjunto de órdenes que se dan a una computadora para realizar un proceso determinado".[22] "Se caracterizan por ser un medio necesario para ofrecer un conjunto de instrucciones comprensibles por una computadora, a efecto de resolver determinado problema".[23]

Otra definición es de la Organización Mundial de la Propiedad Intelectual, que considera a los programas como un conjunto de instrucciones expresadas en un lenguaje ya sea natural o formal, las cuales una vez colocadas en un soporte descifrable por una máquina de tratamiento de datos puede efectuar operaciones lógicas para obtener un resultado en particular.

Red.

"Serie de ordenadores conectados entre sí por medio de canales de comunicación. Es decir, conjunto de ordenadores, dispositivos de procesos de datos, periféricos y aplicaciones que se encuentran conectados entre sí. La conexión se realiza a través de enlaces conectados por un conjunto de protocolos lógicos que regulan los procesos de comunicación. Las razones para unir a las computadoras son variadas pero entre las principales se encuentran permitir la

[21] Mir Puig Santiago, Compilador, "Delincuencia informática", Editorial PPU, Barcelona, 1ª ed., 1992, p.77.
[22] López Betancourt Eduardo, *op. cit.*, p.269.
[23] Téllez Valdés Julio, *op. cit.*, p.92.

comunicación entre personas y compartir recursos (en este punto pueden ser programas o archivos, así como funciones)"[24]

Existe una división de redes de computadoras, esta se clasifica de acuerdo a donde se encuentran ubicadas las terminales y servidores de red.

> "Las redes que se encuentran en un área geográficamente limitada, se conocen como redes de área local (Local Area Network, LAN); las que se encuentran ubicadas en grandes extensiones territoriales, en todo un país o en varios, conectadas mediante diferentes dispositivos, se denominan redes de área amplia (Wide Area Network, Wan) y el tercer tipo de red se circunscriben a un área metropolitana (Metropolitan Area Network, MAN), estan se utilizan para enlazar servicios urbanos (vg. semáforos)".[25]

Virus.

"Son elementos de software diseñados y creados para perjudicar una computadora mediante alteraciones de la forma en que trabaja con su información. Son pequeños programas diseñados para alterar la forma en que funcionan las computadoras, sin la autorización o sin el conocimiento del usuario".[26]

Otra definición consiste en establecer que "son pequeños programas que introducidos subrepticiamente en una computadora, poseen la capacidad de autorreproducirse sobre cualquier soporte apropiado que tenga acceso al ordenador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar".[27]

Por el tipo de daño que causa un virus, puede clasificarse como:

---

[24] Harley Hahn y Rick Stout, *op. cit.*, p.7.
[25] Ferreyr Gonzalo, "Internet. Paso a paso hacia la autopista de la información", Alfaomega Grupo editor, México, 1996, pp.32 y 33.
[26] Santamaría Raga José Mario y Santamaría Raga Sergio, "Introducción a la computación", México, p. 119.
[27] Fornagueira Andrea Isabel y Etienne Patricia Marcela, "Los virus informáticos y la protección penal de la información", *Anuario 1993*, Universidad Nacional de Córdoba, Facultad de Derecho y Ciencias Sociales Córdoba, Argentina, 1993, p.139.

1. Inocuo o no destructivo. Estos virus causan molestias porque aparecen en la forma de un programa que se ejecuta repentinamente. Entorpecen el trabajo normal del usuario, no destruyen ninguna información.
2. Hostiles o destructivos. Existen virus que alteran archivos de datos. Por lo tanto, estos virus son difíciles de detectar. De este tipo hay virus que destruyen selectivamente, es decir, archivos o grupos de archivos específicos. Otros más destruyen parcialmente, es decir, destruyen una porción del disco. Y finalmente están los que destruyen masivamente.

Los virus también pueden clasificarse por el tipo de sistema al que infecten:

1. Los objetivos son IBM PC y compatibles.
2. Las Apple Macintosh.
3. El sistema operativo Unix.

La *Computer Virus Industry Association* ha definido tres clases de virus:[28]

1. Los que infectan programas de propósito general. Los virus que tienen a estos programas como su objetivo de ataque son los que se multiplican realmente rápido. Uno de estos virus puede infectar en cuestión de minutos a todos los programas que estén en una computadora, incluso los programas utilizados para diagnosticar y remover virus (vacunas). Obtienen el control cuando una aplicación infectada es ejecutada y busca anfitriones adicionales en el disco duro o en los diskettes. Una vez que el virus ha buscado e infectado, normalmente regresa al programa de aplicación.
2. Los que infectan archivos de sistema operativo (System Foles). El virus puede adherirse a uno o varios de los archivos del sistema operativo y obtener el control de casi cualquier parte de la operación de la computadora, tal como acceso a disco, etc. Afectan el intérprete de

[28] Rodríguez Luis Ángel, “Seguridad de la información en sistemas de cómputo”, México, 1995, pp. 132-133.

comandos, rutinas de entrada o de salida, drivers especiales para cualquier tipo de hardware. Son más difíciles de detectar por que han infectado al sistema operativo.

3. Los que atacan al sector de inicialización. Este virus afecta el mecanismo de arranque de la computadora. Estos virus monitorean toda la actividad del sistema “atrapando” las interrupciones y “viendo” cuando el usuario inserta nuevos diskettes en las unidades de disco.

Un virus tiene tres etapas de vida:[29]

a) Penetración. Un virus de computadora normalmente entra en un sistema de cuatro formas.

1. A través de intercambio de discos infectados.
2. Bajando un programa infectado.
3. A través del intercambio de archivos infectados en una red.
4. A través de actos específicos de sabotaje.

Una vez dentro del sistema anfitrión, el virus localiza un “hogar adecuado”, entonces se adherirá al programa anfitrión o bien lo reemplazará enteramente.

b) Reproducción. Se multiplica (copiándose a sí mismo) en otros programas dentro del mismo sistema o en archivos de nodos en la red.

c) Activación. Se activa para realizar la tarea para la que fue diseñado.

Algunos de los virus más usados se dan a través de las siguientes técnicas:

1. Bomba lógica. El método consiste en que el virus se activa cuando se cumple con una condición lógica.

[29] *Ibid* pp. 133-134.

2. Bomba de tiempo. La orden de activación y ataque la indica la fecha y hora. “Es un programa contenido dentro de otro con instrucciones precisas de destruir al legítimo”.[30]
3. Variante. También se le llama “Truco de lamer”, cuando el diseñador no es muy hábil para fabricar un virus nuevo, se limita a usar uno ya conocido con pequeñas variantes, suponiendo que la vacuna no va a detectarlo.
4. Killers. También conocidos como retrovirus. Entre sus instrucciones llevan órdenes de borrado contra uno o más antivirus.

Otros tipos de programas malignos son los gusanos, troyanos y droppers.

2.2 Diversas acepciones de delito informático.

Delito informático, suele aludirse a conductas que atentan de forma grave a determinados bienes del individuo –pero también personas jurídicas- que presentan una configuración específica y exclusiva de la actividad informática y telemática y han sido sometidos a una tipología técnico criminológica: acceso, alteración, o destrucción no autorizados de los datos almacenados en un sistema informático; reproducción completa o parcial de datos contenidos en un sistema informático, creación de un fichero clandestino; sustracción del tiempo de sistemas informáticos o telemáticos, etc. En estos casos el ordenador, sus elementos o los sistemas de telecomunicación al servicio de estos son el objeto del delito. En otros supuestos, todos ellos son un mero instrumento. [31]

Para Julio Téllez Valdés los delitos informáticos: “Son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o

[30] Téllez Valdés Julio, *“*Los delitos informáticos: Situación en México*”*, *La Barra*, Revista de la Barra Mexicana, Colegio de Abogados, Número 14, México-Junio, 1997, p. 24.
[31] Luzón Peña Diego Manuel, “Enciclopedia Penal Básica”, Granada, 2002, p.518.

fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)".[32]

Carlos Sarzana en su obra Criminalista y Tecnología, especifica que los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminogena, como mero símbolo".[33]

Rafael Fernández Calvo define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto del delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos".[34]

María de la Luz Lima define delito electrónico estableciendo lo siguiente: "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que en un sentido estricto, el delito informático, es cualquier acto ilícito penal en que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, o fin.[35]

CONCEPTOS AFINES A LOS DELITOS INFORMATICOS:

DELITOS INFORMÁTICOS.

- *"Son todos aquellos en los cuales el sujeto activo lesiona un bien jurídico que puede estar o no protegido por la legislación vigente y que puede ser de diverso tipo por la utilización indebida de los medios informáticos"*.[36]

[32] Téllez Valdés Julio, *op. cit.*, p.163.
[33] Aequitas, segunda época, numero 32, 1998.
[34] *Idem.*
[35] *Idem.*
[36] Campoli Gabriel Andrés, *op.cit.* p.14.

- "Son aquellos realizados por el autor con el auxilio o utilizando la capacidad de los sistemas informáticos para garantizar su anonimato o impunidad territorial, pero que pueden tener tipos penales específicos en algunas legislaciones, definidos con anterioridad a la aparición de los nuevos sistemas de información y telecomunicaciones".[37]

DELITOS ELECTRÓNICOS.

- "Son una especie del género de delitos informáticos en los cuales el autor produce un daño o intromisión no autorizada en aparatos 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 física y lógica de los equipos electrónicos y la intimidad de sus propietarios".[38]

- "Son aquellos que surgen de las nuevas tecnologías aplicadas y tienen como objeto material del delito expresamente las mismas, por regla general no poseen definiciones de tipo posible de ser aplicadas por estar referidos a bienes y conceptos inexistentes a la sanción de leyes penales".[39]

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a París en mayo de 1983 el término delitos relacionados con los ordenadores (computer-related crime) se define como cualquier comportamiento antijurídico no ético o no autorizado relacionado con el procesado automático de datos y/o transmisores de datos.

2.3 Concepto vigente del delito informático y su clasificación.

De la diversidad de acepciones que existen se llega a una conclusión de lo que podría considerarse como delito informático.

[37] *Ibid*, p.17.
[38] *Ibid*, p.14.
[39] *Ibid*, p.17.

Son las conductas ilícitas que comete un sujeto utilizando como medio o instrumento los equipos de cómputo, las redes de Internet y la informática para obtener, modificar, destruir una serie de datos o información confidenciales o restringidos tanto de personas públicas como privadas, o crear una serie de programas u órdenes para causar un daño o cometer un ilícito. Además se vale de una serie de conocimientos en la materia.

Cabe señalar que puede existir una diversidad de hipótesis que pudiesen constituir delitos informáticos. Además pueden adecuarse varios de los delitos ya existentes con la diferencia de que se hace uso de la tecnología y los sistemas para realizarlo.

CARACTERÍSTICAS:

1. Son conductas que sólo determinado número de personas con ciertos conocimientos, pueden llegar a cometerlas.
2. Provocan pérdidas económicas para los afectados y algunos beneficios para aquellos que los realizan.
3. Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin la necesaria presencia física pueden llegar a cometerse.
4. Son muchos los casos y pocas las denuncias, todo ello a la falta misma de regulación jurídica a nivel internacional.
5. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
6. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales y en ocasiones van más allá de la intención (preterintencionales).

Los sujetos que participan en los delitos informáticos son:

SUJETO ACTIVO.

El sujeto activo es la persona que realiza un comportamiento que se encuentra descrito en el tipo penal, el cual causa una lesión a un bien jurídico protegido.

Es decir viola o transgrede una ley. Realiza la acción punible y dicha acción se le es atribuible. Es quien comete un delito o participa en su ejecución.

Las personas que cometen los delitos informáticos son aquellos que poseen ciertas características que no presentan el común denominador de los delincuentes, tienen que tener conocimientos previos en la materia.

Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y en ocasiones se encuentran laborando en lugares en donde se maneja una diversidad de información, aún cuando no es una regla.

"Entre los sujetos activos se encuentran: Operadores, programadores, analistas de sistemas, analistas de comunicaciones, supervisores de servicios, funcionarios, auditores de operaciones, personal de limpieza, mantenimiento, así como usuarios en general."[40]

SUJETO PASIVO.

Es el titular del bien jurídico tutelado, ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, pueden ser individuos, instituciones, gobiernos, entre otros.

Es la persona que sufre directamente la acción; sobre la que recaen los actos materiales mediante los que se realiza un delito.

[40] Pérez Martínez Alfonso, *"*Necesidad de tipificar el delito computacional en el Código de Defensa Social de Puebla*"*, *IUS Revista del Centro y Documentación Jurídica del Instituto de Ciencias Jurídicas de Puebla*, Año V, Número 98, México, Abril-Noviembre, 2001, p41.

Además un punto que es importante destacar es la seguridad en Internet, para resaltar un medio por el cual pueden llevarse a cabo los delitos a los que nos referimos, o bien, podrían establecerse como tipos.

OBJETO DEL DELITO.

El objeto del delito es la persona o cosa, o el bien o el interés jurídico, penalmente protegidos.[41]

Se encuentra dividido en material y jurídico. El primero es la entidad corpórea, persona o cosa, sobre la que recae el delito y el segundo es el bien jurídico lesionado o puesto en peligro.

En el delito informático los objetos del delito son los sistemas, así como los equipos de cómputo y programas que son vulnerados, o el uso de estos equipos y medios electrónicos que se encuentran protegidos.

Es decir, "El bien jurídico tutelado es la información… y aquellos en que el bien jurídico que requiere de protección resulta amparado por otras normas penales…"[42]

Clasificación.

El delito informático puede clasificarse como:

1. Como instrumento o medio.
2. Como fin u objetivo.[43]

[41] Carranca y Trujillo Raúl y Carrancá y Rivas Raúl, *op.cit.*, p.270.
[42] Lara Berrios Bernardo y Morales Godoy Misael, "Los delitos informáticos. ¿Nuevos tipos penales o nuevas formas comitivas de los delitos tradicionales?", *La Revista de Derecho*, Universidad Central de Chile, Facultad de Ciencias Jurídicas y Sociales, Año X, Número 6, Santiago, Chile, Enero-Junio 2004, p.187.
[43] Téllez Valdés Julio, *op.cit.*, pp. 165-166.

1. Como instrumento o fin. En esta se encuentran las conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- ✓ Falsificación de documentos vía computarizada.
- ✓ Variación de activos y pasivos en la situación contable de las empresas.
- ✓ Planeación o simulación de delitos convencionales como son: robo, fraude, etc.
- ✓ Robo de tiempo de computadoras.
- ✓ Lectura, sustracción o copiado de información confidencial.
- ✓ Aprovechamiento indebido o violación de un código para penetrar a un sistema.
- ✓ Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- ✓ Uso no autorizado de programas de cómputo.
- ✓ Insertar instrucciones que provocan interrupciones en la lógica interna de los programas, a fin de obtener beneficios.
- ✓ Alteración en el funcionamiento de los sistemas.

2. Como fin u objetivo. En esta se encuentran las conductas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

Algunos ejemplos son:

- ✓ Programación de instrucciones que producen un bloqueo total del sistema.
- ✓ Destrucción de programas por cualquier método.
- ✓ Daño a la memoria.
- ✓ Atentado físico contra la máquina y sus accesorios.
- ✓ Secuestro de soportes magnéticos.

La Comisión de las Comunidades Europeas señala como clasificación de delitos informáticos los siguientes:

1. Acceso no autorizado a sistemas de información.
2. La perturbación de los sistemas de información.
3. Ejecución de programas informáticos perjudiciales que modifican o destruyen datos.
4. Intervención de las comunicaciones.
5. Declaraciones falsas.

Podrían considerarse las siguientes consultas como tipos de delitos informáticos:[44]

- Delitos contra la propiedad intelectual.
- Difusión y exhibición de material pornográfico a menores.
- Pornografía infantil.
- Difusión de mensajes injuriosos o calumniosos.
- Publicidad engañosa.
- Revelación de secreto.
- Uso de terminales de comunicación sin autorización.
- Infracción de los derechos de autor.
- Delitos transfonterizos.
- Interceptación de telecomunicaciones.
- Interceptación de correo electrónico.
- Cesión de datos reservados de carácter personal.
- Fraude electrónico.
- Daño informático.
- Falsedad documental.

También podrían catalogarse y encuadrarse las siguientes conductas:

[44] Molina Salgado Jesús Antonio, *op. cit.*, p. 23

- Espionaje.
- Terrorismo.
- Fraudes.
- Spamming.

Tipos de delitos informáticos reconocidos por Naciones Unidas.[45]

1. Manipulación de los datos de entrada. Puede ser realizado por cualquiera que tenga acceso a los datos de entrada de los sistemas computacionales.
2. Manipulación de programas. Consiste en modificar programas dando o creando nuevas instrucciones entre los cuales pueden figurar los virus.
3. Manipulación de datos de salida. Por ejemplo fraude a cajeros informáticos.
4. Fraude efectuado por manipulación informática.
5. Daños ocasionados por virus, gusanos, bombas lógicas.
6. Piratas informáticos o hackers.
7. Reproducción no autorizada de programas informáticos.

3. Derecho comparado.

El Derecho comparado, es una rama general del derecho que tiene por objeto el examen sistematizado del derecho positivo vigente en los diversos países, ya sea con carácter general o en algunas de sus instituciones para establecer analogías y diferencias.[46]

"El derecho comparado es una comparación entre los diferentes sistemas legales existentes".[47] Su fin es el conocimiento de los mismos.

El derecho comparado surgió en 1900 en la Exposición Mundial ya que en los congresos que se llevaron a cabo los estudiosos Edouard Lambert y Raymond

[45] Téllez Valdés Julio, *op.cit.*, p.172
[46] Sirvent Gutiérrez Consuelo y Villanueva Colín Margarita, "Sistemas Jurídicos Contemporáneos", Harla, México, 2004, p.17.
[47] Zweigert Honrad y Kotz Hein, "Introducción al derecho comparado", Editorial Oxford, 2002, p.3.

Saleilles fundaron el Congreso Internacional de Derecho Comparado cuya finalidad era crear un derecho común en el mundo.

Lo anterior básicamente con el fin de reducir divergencias en materia legal, crear y aportar nuevas ideas para crear un derecho más completo. Esto se puede lograr creando comparaciones en diferentes aspectos como ordenamientos legales, métodos para dirimir controversias, nuevas formas de resolver conflictos atendiendo también a la eficacia de los mismos.

Por ello, el derecho comparado sirve como instrumento del legislador para poder crear normas más rigurosas y completas, sirviendo la mayor parte de las veces el siguiente método:

1.- Analizar cada uno de los aspectos de los diferentes sistemas legales, después realizar una crítica.
2.- Observar cada uno de los enfoques y
3.- Finalmente las conclusiones de que es lo mejor a aplicar en cada caso concreto.

El derecho comparado nos sirve para entender mejor las propias leyes, crear otras más completas y buscar una mejor aplicación de las mismas, ya que de este estudio de ordenamientos se puede aprender la influencia de otras culturas y la interacción que puede haber con determinadas materias creando así una unificación del Derecho.

Otra contribución del Derecho comparado es que se puede establecer en los programas universitarios para un mejor estudio de cada una de las propias leyes y con ello encontrar una solución a las lagunas jurídicas tomando en cuenta los usos y costumbres de cada sociedad.

Otra función del Derecho comparado es la elaboración de proyectos para unificar internacionalmente el Derecho, esto es, con la finalidad de crear seguridad.

El siguiente paso del proceso comparativo es la construcción del sistema, para lo cual se requiere crear un vocabulario especial el cual debe ser amplio y con flexibilidad para que pueda ser adaptado a varios países.

Por lo cual es importante resaltar el concepto de sistema jurídico el cual “es el conjunto de normas e instituciones que integran un Derecho positivo y que rigen una determinada colectividad. Los elementos que integran un sistema jurídico son la legislación que rige una colectividad y una autonomía legislativa”.[48]

[48] Sirvent Gutiérrez Consuelo y Villanueva Colín Margarita, *op.cit.*, p.5.

CAPÍTULO II. LA TEORÍA DEL DELITO Y EL TRATAMIENTO EN MÉXICO DE LOS DELITOS INFORMÁTICOS ACTUALMENTE.

En este capítulo se abarcara lo referente a la teoría del delito, a los aspectos positivos y negativos que integran el delito y la explicación e importancia que tienen para algunos tratadistas del Derecho, los cuales han tratado de establecer aspectos y complementar lo que constituye la teoría del delito. La constitución del delito, a través de lo que es conocido como elementos del delito.

Se explicara cada uno de estos elementos del delito en su aspecto positivo y negativo.

1. Teoría del delito.

Se ha desarrollado a través del tiempo en el Derecho penal una serie de ideas y tesis sobre cómo abordar al delito y la forma en que se encuentra conformado, por lo que ha sido necesario que varios tratadistas y expertos en la materia den su opinión y sugieran la forma en que debe ser estudiado.

Lo anterior con el objetivo de tener una mejor comprensión para una adecuación de conductas al Derecho positivo de cada país.

1.1 Concepto de teoría del delito.

La teoría del delito es el estudio de los elementos que conforman al delito.

Mientras más avanzaba el estudio del delito a través del tiempo se desarrollaron diversidad teorías en donde se fueron agregando elementos que conformaran al delito, hasta que se llegó a la idea que considera que son siete los elementos de la teoría del delito y que son imprescindibles para poder establecer el mismo.

Tales elementos en sus aspectos positivos y negativos son los siguientes:

Aspectos positivos:

a) Conducta.
b) Tipicidad.
c) Antijuricidad.
d) Imputabilidad.
e) Culpabilidad.
f) Condiciones objetivas de punibilidad.
g) Punibilidad.

Las anteriores cuentan cada una con su aspecto negativo y son:

a) Falta de acción.
b) Ausencia de tipo.
c) Causas de justificación.
d) Causas de Inimputabilidad.
e) Causas de inculpabilidad.
f) Falta de condiciones objetivas de punibilidad.
g) Excusas absolutorias.

La teoría del delito sistematiza los presupuestos generales y los elementos de la acción para que una vez integrado el delito se aplique la consecuencia jurídica que es la pena o la medida de seguridad en su caso.

El fundamento de la teoría del delito es la ley positiva, sirve para unir el mundo fáctico con el mundo normativo, el primero es la concreción de un hecho material y el segundo es la descripción legal.

Tiene como naturaleza, el estudio de las características comunes, que debe tener cualquier ilícito, para ser considerado como delito.

1.2 Teorías referentes al estudio del delito.

Existen otros estudios de la teoría del delito como son la teoría unitaria o totalizadora y la teoría analítica o atomizadota. La primera de ellas establece que el delito no se puede dividir para que se pueda estudiar sino que debe ser visto como un todo. La segunda, también era conocida como pluralista o estratificada, se refiere a que el delito para que pueda ser estudiado debe ser fraccionado por partes para un mejor análisis.

Existen varias visiones referentes a la teoría del delito y son:[49]

a) El sistema causal psicológista también conocido como sistema clásico.
b) El sistema causal normativista o sistema neo-clásico
c) El sistema finalista.
d) El sistema funcionalista.

a) Sistema causal psicológico. Sus principales exponentes fueron Liszt y Beling. Se basó en que lo injusto y culpabilidad forman la parte externa e interna del delito. Por lo que, lo que es conocido como dolo y culpa son formas psicológicas de la culpabilidad.

En este sistema también encuentra una base en la conformación del delito según el número de elementos que lo componen.

En esta clase de sistema encontramos entre otros a los siguientes autores. Francisco Carrara quien establece que en el delito actúan dos fuerzas, la fuerza

[49] Berchelmann Arizpe Antonio, “Derecho penal mexicano” “Parte General”, Editorial Porrúa, México, 2004, p.362.

subjetiva y la física. Giussepe Magiores que establece que se encontraban tres elementos el hecho, la antijuridicidad y la culpabilidad y Franz Von Liszt agrega la punibilidad.

La teoría del delito utiliza como fundamento la distinción entre el aspecto externo (objetivo) y el aspecto interno (subjetivo) del delito.

Lo objetivo está constituido por la acción, tipicidad y antijuridicidad y la parte subjetiva corresponde a la culpabilidad con sus especies o elementos dolo y culpa.

Entendiendo a sus elementos de la siguiente manera:[50]

1. Acción. Aparece como lo sustantivo, como una causa que altera el mundo exterior por una conducta corporal voluntaria. Se compone de movimiento corporal (conducta) que produce una modificación del mundo externo (resultado), no contiene elementos de valoración.
2. Tipicidad. Entendida como la descripción externa de la acción sin contenido normativo, se fijó como indicio.
3. Antijuridicidad. Es un juicio de valor que recae sobre la acción, como aspecto objetivo.
4. Culpabilidad. Es el aspecto subjetivo del delito. Su presupuesto es la imputabilidad y sus especies el dolo y la culpa.

b) Sistema causal normativo. Esta teoría es de Mezger. Este estudio del delito se basa en que lo injusto no es explicable en todos los casos por elementos materiales y normativos y que la culpabilidad no se basa en elementos subjetivos.

En el causalismo implica que haya una conducta y un resultado que se encuentran unidos por un nexo causal.

[50] Daza Gómez Carlos, *"*Teoría del delito*", Responsa*, Centro Universitario México, División de Estudios Superiores A.C., Año 3, Número 16, México, Agosto-Septiembre 1998, p.5.

Comprende a sus elementos de la siguiente manera:[51]

1. Acción. El acto interno de la voluntad y la manifestación externa de este acto.
2. Tipicidad. Se le considera como *ratio essendi*, de la antijuridicidad. Es la descripción exenta de valoración.
3. Antijuridicidad. Es una lesión objetiva de las normas de valoración.
4. Culpabilidad. La concepción normativa, es un juicio de reproche al actor por haber realizado un hecho típico y antijurídico, pudiendo haber actuado conforme a lo que ordena el derecho. Además de tener un contenido determinado de carácter psicológico (dolo y culpa), es un juicio de desvalor, la culpabilidad es reproche.

c) Sistema finalista. En esta teoría la persona que realiza un acto antisocial tiene una idea de lo que va a ocurrir si comete determinada conducta. En este caso el dolo se entiende como una forma de culpabilidad, por que el sujeto ya va encauzado a cometer una conducta que dará en un resultado específico. Es la voluntad dirigida a lograr determinados resultados con base a objetivos marcados.

Para la teoría final, la voluntad de realización del autor integran ya los factores que determinan el ilícito de la conducta, en este caso al dolo lo consideran como presupuesto de la tipicidad.

Sus elementos son los siguientes:[52]

1. Acción. En esta teoría el dolo pertenece a la acción, siendo natural y final, apartándolo de la culpabilidad.
2. Tipicidad. Hay una parte objetiva y una subjetiva del tipo. La primera es la objetivización de la voluntad integrante del dolo, comprende las características externas del autor, la parte subjetiva esta formada por el

[51] *Idem.*
[52] *Ibid.*, p.6

dolo y los elementos subjetivos. El dolo se agota en la finalidad dirigida al tipo objetivo.

3. Antijuridicidad. Es un juicio de valor el cual expresa que la acción puede ser contraria a la norma y lo será cuando no exista causa de justificación. Toma en cuenta la conducta externa del autor.
4. Culpabilidad. Es el juicio de reproche que se formula al autor por no haber adecuado su conducta al derecho, a pesar de que estaba en situación de hacerlo.

   Sus componentes son:
   - Imputabilidad.
   - Conocimiento de la antijuridicidad.
   - Exigibilidad.

d) Sistema funcionalista. Parten de la hipótesis de que la formación del sistema jurídico penal no se puede vincular a realidades ontológicas previas como son la acción y la causalidad; sino que deben guiarse por los fines del Derecho Penal.

Algunos criterios importantes sobre esta teoría son los siguientes:

- Criterio de Claus Roxin: Explica que al sistema de la teoría del delito se le debe estructurar con base a los fines de la pena, siempre y cuando se conciban los fines del estado de derecho.

- Criterio de Gunter Jakobs: Dice que el sistema se basa en que la norma prevalezca, derivado de los sistemas de control social.

- Sistema funcional: En esta tesis que sostiene Zaffaroni explica que el delito debe satisfacer una serie de condiciones como servir para su función inmediata o práctica para facilitar la decisión jurídica; ser valorativa de acuerdo a cierto orden

y lógica; debe constituirse teleológicamente tomando en consideración el poder punitivo.

2. Elementos positivos y negativos del delito en general y en los delitos informáticos.

Para poder establecer lo que son los elementos positivos y negativos del delito, primero se tienen que establecer que es un elemento.

Elemento, es aquello que concurre para la formación de algo complejo. Por lo cual estos elementos son necesarios para la conformación de un todo que en este caso es el delito.

Ahora bien, después de saber lo que es un elemento, en su aspecto general, estudiaremos cada uno de ellos en su aspecto positivo y negativo, como integrantes del delito.

2.1 La conducta.

Puede ser entendida como el acto u omisión de llevar a cabo algo. Es aquella en donde interviene la voluntad. Es un elemento positivo del delito.

La conducta consiste en el comportamiento humano, manifestado mediante una acción, hecho, acto o actividad de carácter voluntario, activo o negativo que produce un resultado.

En la acción se pueden encontrar algunos elementos como son la voluntad de querer, la actividad y el abstenerse, además la realización de estas acciones implica un cambio en el exterior. La mayoría de las veces lleva consigo una finalidad.

Elementos de la Acción:

1.- Voluntad. Es el querer por parte del sujeto activo de cometer el delito, es la intención.

2.- Actividad. Consiste en “hacer” o actuar. Es el movimiento corporal humano encaminado a producir el ilícito.

3.- Resultado.- Consecuencia de la conducta. El fin deseado por el agente.

4.- Nexo de causalidad.- Ligamiento que une la conducta con el resultado, el cual debe ser material. De tal manera que el resultado no puede atribuirse a otra causa.[53]

El *nexo causal debe ser material*, ya que si es moral, psicológico o espiritual será irrelevante para el Derecho Penal. Debe ser el idóneo para producir el resultado típico.

Existen los delitos de comisión por omisión mediante el cual se omite una acción esperada produciéndose un resultado; y la omisión simple es el abstenerse de realizar algo y hay un deber jurídico de obrar.

Elementos de la omisión:

1.- Voluntad. Consiste en querer no realizar la acción esperada y exigida. Esto es querer la inactividad voluntaria o culposamente.

2.- Omisión. Consiste en “no hacer” o dejar de actuar.

3.- Resultado.- Consecuencia de la conducta.

4.- Nexo de causalidad.- Ligamiento que une la conducta con el resultado, el cual debe ser material. De tal manera que el resultado no puede atribuirse a otra causa.[54]

[53]Camargo Pacheco, María de Jesús, http://cursweb.educadis.uson.mx/mcamargo/documentos/NOTAS%20PARA%20EDICION%20DERECHO%20PENAL%20I.doc, 3 de marzo 2008.

El tiempo en que se realiza la conducta es relevante primero, en relación a la vigencia temporal de la ley penal, para observar la inimputabilidad de los menores infractores y para computar el término de prescripción de la acción penal.

En los delitos informáticos la conducta se da cuando hay una acción, se realiza un hecho, acto o actividad activa o negativa que produce una consecuencia, utilizando equipos de cómputo o redes informáticas.

2.2 La ausencia de conducta.

Es un elemento negativo del delito. En esta encontramos una serie de presupuestos como son:

a) El caso fortuito. Este es un suceso o acontecimiento inesperado, es ajeno a nosotros y puede provenir de la fuerza de la naturaleza o la humana; si proviene de la naturaleza se conoce como *vis mayor* y si proviene del hombre es *vis absoluta*.

En la *vis absoluta* supera la voluntad del sujeto de tal modo de que es incapaz de autodeterminarse.

b) Hipnotismo. Ya sea que se dé de manera voluntaria o con fines médicos, en este caso se tendrá que estudiar si estaba conciente o no de que iba a ser utilizado para cometer algún tipo de ilícito al ser hipnotizado.

c) Sonambulismo. Ya que aquí se encuentra una ausencia de voluntad y más si el sujeto activo del delito no sabía que sufría de este padecimiento.

---

[54] *Idem.*

d) Movimientos reflejos. Es una reacción del ser humano de forma involuntaria a un estímulo que le es proporcionado, no debe ser confundido con un acto impulsivo, debido a que en ese caso la acción no puede ser negada.

2.3 La tipicidad.

La tipicidad es la adecuación al tipo. Para lo cual se debe advertir que el tipo es una descripción detallada de una conducta o un acontecimiento que se considera delito. Es un elemento positivo del delito.

"El tipo es la creación legislativa, la descripción que el Estado hace de una conducta en los preceptos penales y la tipicidad es la adecuación de una conducta concreta con la descripción legal formulada en abstracto".[55]

En tiempos pasados el tipo en Alemania era considerado como el conjunto de caracteres integrantes del delito, tanto los objetivos como subjetivos e incluían el dolo y la culpa.

Para Ernesto Mayer, en su Tratado de Derecho Penal asegura que la tipicidad no es meramente descriptiva, sino indiciaria de la antijuridicidad, en toda conducta típica hay un principio, una probabilidad de antijuridicidad.

Para Edmundo Mezger, el tipo no es una simple descripción de una conducta antijurídica, sino la *ratio essendi* de la antijuridicidad, es decir, la razón de ella su real fundamento. En sentido estricto consiste en la descripción de la conducta contraria o la prohibición del mandato.

Las siguientes tesis muestran de manera clara lo que es el tipo:

Registro No. *263576*

[55] Castellanos Tena Fernando, "Lineamientos elementales de derecho Penal", Trigésima Segunda Edición, Editorial Porrúa, México, 1993, p.167.

Localización:
Sexta Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación
Segunda Parte, XVI
Página: 257
Tesis Aislada
Materia(s): Penal

TIPO PENAL.

El tipo delictivo está constituído por el conjunto de los presupuestos a cuya existencia se liga una consecuencia jurídica; o en otros términos, el tipo penal significa más bien el injusto descrito concretamente por la ley en sus diversos artículos y a cuya realización va ligada la sanción penal.

Amparo directo 4533/57. Antonio Sánchez Gavito. 23 de octubre de 1958. Cinco votos. Ponente: Luis Chico Goerne.

En la tesis anterior se puede observar que se maneja al tipo como los presupuestos que se encuentran contemplados en la ley y existe una sanción para los mismos.

Registro No. *292719*
Localización:
Quinta Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación
CXXXI
Página: 121
Tesis Aislada
Materia(s): Penal

TIPO PENAL.

Conforme a la teoría general del derecho, el tipo penal está constituido por el injusto descrito concretamente por un precepto de la ley, a cuya existencia se liga una consecuencia jurídica de punibilidad.

Amparo directo 1424/55. Por acuerdo de la Primera Sala, de fecha 8 de junio de 1953, no se menciona el nombre del promovente. 17 de enero de 1957. Unanimidad de cinco votos. Ponente: Luis Chico Goerne

En está tesis como en la que antecede se puede observar el hecho de ligar una conducta descrita como delito con una sanción.

El tipo cuenta con un elemento objetivo y subjetivo, el primero atiende a objetos corpóreos o materiales y el segundo, a la intensión que tiene el sujeto activo, la cual puede ser dolosa o culposa.

Para entender lo anterior es necesario establecer qué es el dolo y la culpa. El primero implica la intención que tiene el sujeto activo de dañar o perjudicar a alguien cuando comete la conducta, mientras que el segundo es realizado por un sujeto sin la intención de causar un daño y es causado por una negligencia o un descuido.

Tiene que coincidir con el supuesto legal de un hecho para poder ser considerado delito.

La tipicidad se encuentra apoyada por diversos principios que constituyen la garantía de legalidad. Establecido en el artículo 14 de la Constitución Política de los Estados Unidos Mexicanos. *Nullum crimen sine lege, nullum crimen sine tipo, nulla poena sine tipo*.

El tipo tiene un empleo de un verbo principal, es decir, es una acción específica, contienen modalidades y referencias a realizar una acción.

Existen diferentes clases de tipos legales:[56]

- Tipo fundamental.
- Tipo especial.
- Tipo independiente.
- Tipo subordinado.
- Tipo objetivo.
- Tipo subjetivo.

Doctrinalmente las clasificaciones del tipo, son las siguientes:

1. Por su composición se puede dividir en normales y anormales. El primero sólo contiene conceptos objetivos y el segundo describe situaciones valoradas y subjetivas.

2. Por su ordenación metodológica se puede dividir en fundamentales o básicos, especiales y complementados.

- Tipo fundamental. Este es considerado también como fundamental. La acción que se da en concreto y no necesita de nada. Por ejemplo el homicidio.

- Tipo especial. La figura del delito aparece completa, no es necesario acudir a otro para darle un sentido. Son los formados por el tipo fundamental y otros requisitos, cuya nueva existencia, excluye la aplicación del básico y obliga a subsumir los hechos bajo el tipo especial. Por ejemplo el infanticidio.

Existen de índole privilegiada y de naturaleza calificada o agravada. En los primeros hay menos daño o peligro de parte del sujeto activo, en los segundos el daño es más grande o mayor la temibilidad.

[56] Jiménez de Asúa Luis, “Teoría del delito”, IURE editores, México, 2003, 171-172.

- Tipo complementado. Estos tipos se integran con el fundamental y una circunstancia o peculiaridad distinta, se diferencian entre sí los tipos especiales y complementados, en que los primeros excluyen la aplicación del tipo básico y los complementados presuponen su presencia, a la cual se agrega, como aditamento, la norma en donde se contiene la suplementaria circunstancia o peculiaridad.

3. En función de su autonomía o independencia se divide en:

- Tipo independiente. Son independientes ya que tienen una completa descripción. Tienen vida propia sin depender de otro.

- Tipo subordinado. Necesitan una relación con los fundamentales, ya que cuentan con un complemento de los básicos. Dependen de otro tipo, adquieren vida en razón del básico, no lo complementan simplemente lo subordinan.

Ahora bien, de los tipos analizados con anterioridad se desprende que se pueden dividir en básicos, especiales y complementados según Paul Merkel[57]. Los primeros son fundamentales y tienen independencia de otros; el tipo especial supone el mantenimiento de los caracteres del tipo básico, añadiéndole una peculiaridad, cuya nueva existencia excluye de la aplicación del tipo básico y obliga a asumir nuevos hechos bajo el tipo especial; por lo que el básico y el especial se eliminan mutuamente. El tipo complementado presupone la aplicación del tipo básico que se ha de incorporar al especial.

4. Se divide por su formulación en casuísticos y amplios. Los primeros son aquellos en los cuales el legislador no describe una modalidad única, sino varias

[57] *Ibid.*, 175.

formas de ejecutar el ilícito, prevén varias hipótesis. Estas se clasifican en alternativamente formados en esta se prevén dos o más hipótesis comitivas, además el tipo se colma con cualquiera de ellas, puede ser sólo una y acumulativamente formados se requiere el concurso de todas las hipótesis.

5. Por el daño que causan se dividen en los que son de daño y los de peligro. Se considera de daño si el tipo tutela los bienes frente a su destrucción o disminución y de peligro cuando la tutela penal protege el bien contra la posibilidad de ser dañado.

6. Pueden ser tipo objetivo o subjetivo.

- Tipo objetivo. En los tipos existen referencias jurídicas y estas conservan su función descriptiva, ya que solo sirven para delimitar cierta conducta.

- Tipo subjetivo. Son aquellas descripciones que abarcan especiales intenciones o tendencias del agente o sujeto pasivo.

Integran el tipo todos los presupuestos materiales de punibilidad.

El hecho de que cierta conducta se encuentre establecida en el tipo es una garantía de legalidad.

El principio de la tipicidad en materia penal en el Distrito Federal se encuentra establecido en el artículo 2 del Código Penal para el Distrito Federal en donde se expone que se debe acreditar la existencia legal del delito.

Artículo 2 del Código Penal para el Distrito Federal. *"No podrá imponerse pena o medida de seguridad, sino se acredita la existencia de los elementos de la descripción legal del delito de que se trate…"*

De lo anterior, se advierte que es necesario que se cubran con ciertos requisitos establecidos en la conducta para que se encuadre lo que se conoce como tipo, así como el hecho de que estas conductas llevan implícitas una sanción; tal como nos ilustra la siguiente tesis aislada:

Registro No. *178461*
Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXI, Mayo de 2005
Página: 1459
Tesis: II.2o.P.159 P
Tesis Aislada
Materia(s): Penal

ELEMENTOS DE NATURALEZA SUBJETIVA EXIGIDOS POR LA DESCRIPCIÓN TÍPICA DEL DELITO QUE LOS CONTEMPLE COMO COMPONENTES. SU ACREDITAMIENTO.

Bajo un punto de vista legal y correcto es perfectamente válido afirmar que los elementos del tipo, aun los de naturaleza subjetiva pueden evidenciarse con base en la prueba indiciaria que la ley mexicana reconoce, al margen del sistema dogmático a la luz del que sistemáticamente pretenda hacerse el estudio respectivo.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL SEGUNDO CIRCUITO.

Amparo directo 470/2004. 21 de enero de 2005. Unanimidad de votos. Ponente: José Nieves Luna Castro. Secretario: Jorge Hernández Ortega.
Véase: Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo IX, junio de 1999, página 914, tesis XXIII.1o. J/13, de rubro: "SALUD, DELITO CONTRA LA. PRUEBA DE LOS ELEMENTOS CONSTITUTIVOS DEL DELITO PREVISTO POR EL ARTÍCULO 195 DEL CÓDIGO PENAL FEDERAL."

Por lo anterior, se puede establecer que es necesario que el tipo cuente con determinados elementos aún cuando estos sean subjetivos.

En los delitos informáticos el tipo se da cuando la conducta se adecua a lo preceptuado por la ley penal, aunque es necesario recalcar, que deben establecerse nuevos presupuestos en el Código Penal, ya que muchas veces estos ilícitos no se encuentran establecidos en nuestra legislación debido a los avances tecnológicos.

2.4 La atipicidad.

Es la ausencia de adecuación de la conducta al tipo, es decir, cuando no se integran todos los elementos descritos en el tipo penal se presenta el aspecto negativo del delito conocido como atipicidad.

Debe distinguirse entre ausencia de tipo y atipicidad; la primera se presenta cuando el legislador, deliberada o inadvertidamente, no describe una conducta que, según el sentir general, debería ser incluida en el catalogo de delitos y la ausencia de tipicidad surge cuando existe el tipo, pero no se amolda a el la conducta dada. En el fondo en toda atipicidad hay falta de tipo.[58]

Existen dos formas de atipicidad:

a) Atipicidad absoluta. No existe encuadramiento con ningún elemento del tipo.[59]

b) Atipicidad relativa. Falta o ausencia de algún elemento del tipo.[60]

Las causas de atipicidad son:[61]

[58] CastellanosTena Fernando, *op cit.* p.174.
[59] Hernández Islas Juan Andrés, *op. cit.* P.97.
[60] *Idem*.
[61] Castellanos Tena Fernando, *op.cit.*, p. 175.

- Ausencia de calidad o del número exigido por la ley en cuanto a los sujetos activo y pasivo.
- Si faltan el objeto material o el objeto jurídico.
- Cuando no se dan las referencias temporales o espaciales requeridas por el tipo.
- Al no realizarse el hecho por los medios comisivos específicamente señalados por la ley.
- Si faltan los elementos subjetivos del injusto legalmente exigidos, son referencias típicas a la voluntad del agente o al fin que se persigue.

2.5 La antijuridicidad.

Como elemento positivo del delito es aquello que es contrario a derecho. Actúa antijurídicamente quien contradice un mandato de poder, además presupone un juicio, una estimación de la oposición existente entre el hecho realizado y una norma jurídico penal.

Por lo tanto hay una necesidad de adecuación del hecho a la figura que lo describe y de oposición al principio que lo valora. La antijuridicidad radica en la violación del valor o bien protegido a que se contrae el tipo penal respectivo.

No se vulnera la ley, pero sí se quebranta algo esencial para la convivencia y el ordenamiento jurídico ya que la norma valoriza y la ley solo describe.

Existen dos tipos de antijuridicidad: la formal y la material. La antijuridicidad formal se refiere a la contradicción entre el hecho y la norma, cuando contradiga una norma positiva y la material se refiere a la trasgresión de la ley, cuando afecta a los intereses de la sociedad, es decir, de una colectividad.

Existe en la antijuridicidad un doble aspecto la rebeldía contra la norma jurídica que es la antijuridicidad formal y el daño o perjuicio social causado por esa

rebeldía que era antijuridicidad material. Para el tratadista Villalobos la infracción de las leyes significa una antijuridicidad formal y el quebrantamiento de las normas que las leyes interpretan constituye la antijuridicidad material.

Max Ernesto Mayer. Describe la antijuridicidad como la contradicción a las normas de cultura reconocidas por el Estado, da un contenido más ético la norma cultural comprende costumbres, valoraciones medias, etc.

La siguiente tesis muestra que no sólo debe acreditarse el tipo penal, sino que es necesario que ésta sea reprochable, así como contraria a derecho y a las normas.

Registro No. *178714*
Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXI, Abril de 2005
Página: 1420
Tesis: II.2o.P.163 P
Tesis Aislada
Materia(s): Penal

INJUSTO PENAL. SU ACREDITAMIENTO ES UN PRESUPUESTO DE APLICACIÓN DEL DERECHO PUNITIVO Y REQUIERE LA JUSTIFICACIÓN NO SÓLO DEL ENCUADRAMIENTO TÍPICO FORMAL, SINO TAMBIÉN DEL ANÁLISIS DE ANTIJURIDICIDAD EN UN CONTEXTO NORMATIVO INTEGRAL.

Para lograr la debida motivación respecto del acreditamiento de un delito, no basta con articular dogmáticamente una serie de razonamientos referentes a los componentes del delito en abstracto, entendidos como conducta, antijuridicidad, tipicidad y culpabilidad, sino que dependiendo de cada supuesto ese contenido de motivación, particularmente por lo que se refiere al encuadramiento típico y a la presencia de la antijuridicidad de la conducta, amerita un estudio completo, en su caso, de la normatividad existente aun de manera complementaria en el ámbito integral de la legislación del Estado de que se trate, es decir, que cuando la figura

delictiva se vincule con un comportamiento previsto u objeto de regulación en otros ámbitos de las ramas del derecho, además de la penal, ello hace indispensable para lograr el acreditamiento auténtico de la tipicidad conglobante, esto es, con la constatación de lo antijurídico, el que ese conjunto normativo se analice e interprete de manera sistemática, a fin de establecer, de ser el caso, cuál es la hipótesis conductual que realmente, por su nivel de afectación al bien jurídico, amerite ser digna del exclusivo universo de comportamientos penalmente relevantes. En otras palabras, la tipicidad y antijuridicidad penal presuponen, en casos como el que se menciona, que no cualquier comportamiento sea potencialmente encuadrable, sino únicamente aquel que descartado de los diversos ámbitos normativos, justifiquen la existencia del reproche penal. Lo anterior muestra mayor relevancia cuando la propia descripción típica de que se trate, ya sea de manera expresa o implícita, hace referencia, por ejemplo, a la "ilegalidad", forma "indebida", "ilicitud" o "incorrección" respecto del particular modo de ejecución del hecho, pues en tal supuesto se hará necesario confrontar el total de la normatividad a fin de establecer ese carácter que sin duda se traduce en un elemento normativo del propio delito en cuestión.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL SEGUNDO CIRCUITO.Amparo en revisión 141/2004. 10 de septiembre de 2004. Unanimidad de votos. Ponente: José Nieves Luna Castro. Secretaria: Alma Jeanina Córdoba Díaz.

Es claro como se observó de la tesis anterior que no basta con encuadrar una conducta a un tipo específico, es decir que se encuentre descrita dicha conducta como un ilícito, sino que además el tipo debe ser una conducta contraria al derecho.

Hay antijuridicidad en los delitos informáticos desde el momento en que se vulnera un bien que es jurídicamente protegido.

2.6 Las causas de justificación.

Este es un elemento negativo del delito, y no excluyen al delito sino a la responsabilidad.

Se puede fundar en la ausencia de interés y en el interés preponderante. En el primero el delito es la lesión de un bien jurídico, tutelado por razón del interés público y por ende indisponible.

En esta se puede encontrar un interés preponderante, que se da cuando existen dos intereses incompatibles; el derecho ante la imposibilidad de que ambos subsistan, opta por la salvación del de mayor valía y permite el sacrificio del menor, como único recurso para la conservación del preponderante. Esta es la razón por la cual se justifica la defensa legítima, el estado de necesidad, el cumplimiento de un deber y el ejercicio de un derecho, una obediencia jerárquica y el impedimento legítimo.

Por lo que se explican a continuación cada una de estas hipótesis:

a) Legitima defensa. Se da cuando se repele una agresión, real, actual o inminente, y sin derecho, en protección de bienes jurídicos propios o ajenos, siempre que exista la necesidad de defenderse y que sea proporcional al actuar.

Es decir, deben existir cinco requisitos para que se dé:

- Agresión.
- Real.
- Actual
- Inminente
- Sin derecho

En esta se trata de la protección individual y de que prevalezca algún derecho.

Las teorías para la explicar la naturaleza jurídica de la legítima defensa son las siguientes:

- Las que la señalan como una excusa, como causa de impunidad o motivo de inimputabilidad.
- Teoría intermedia de la mera colisión de intereses.

b) Estado de necesidad. Se da al salvaguardar un bien jurídico propio o ajeno, de un peligro real, actual o inminente que lesiona otro bien de igual o menor valor que el que salvaguarda, cuando no pueda ser evitado de otra forma más que de esa.

En esta se encuentran dos bienes jurídicos y es necesario tomar una decisión sobre cuál es el más importante, de esa forma se salvará uno y se perderá otro.

c) Cumplimiento de un deber. Que se realice un deber jurídico y no tenga como fin perjudicar. Esta se da cuando se encuentra ordenada por una norma. Además el que la comete es porque se encuentra subordinado a un superior y no tiene elección porque tiene que obedecer órdenes, se da en razón del oficio o profesión que desempeña.

Existen dos clases de deberes:[62]
1. Deberes emanados del cumplimiento de una función pública.
2. Deberes impuestos a los gobernados, directamente por la ley o indirectamente a través de un mandato legítimo de autoridad que los gobernados tengan que acatar. Se condiciona a la competencia de la autoridad para imponerlo y a que se imponga con las formalidades legales.

d) Ejercicio de un derecho. Que se realice un derecho y no tenga como fin perjudicar. Es una facultad que le es concebida a un sujeto.

Los requisitos que debe cumplir el ejercicio de un derecho son:[63]

[62] Arilla Bas Fernando, “Derecho penal. Parte general”, Editorial Porrúa, México, 2001, 265 y 266.
[63] *Ibid.*, 269.

1. Que el sujeto sea efectivamente el titular de ese derecho o que en caso de ser delegable dicho derecho, le haya sido delegado expresamente su ejercicio por el titular.
2. Que el derecho sea ejercitado de manera legal.

e) Obediencia jerárquica. Era el deber de una persona de obedecer a su superior pero ya quedo extinta.

2.7 La imputabilidad.

Es un elemento positivo del delito. La imputabilidad es imputar un hecho a un individuo y atribuírselo para hacerle sufrir las consecuencias.[64]

La responsabilidad resulta de la imputabilidad, puesto que es responsable el que tiene la capacidad de sufrir las consecuencias del delito.

La imputabilidad se basa en el libre albedrío y en la responsabilidad moral, además es considerado como la capacidad de entender y querer. Representa la capacidad de culpabilidad. Este tipo de juicio lo puede hacer quien es mayor de dieciocho años y se encuentre en pleno goce de sus facultades mentales, a partir de ese momento es considerado como imputable.

La imputabilidad afirma la existencia de una relación de causalidad psíquica entre el delito y la persona; la responsabilidad resulta de la inimputabilidad, puesto que es responsable el que tiene capacidad para sufrir las consecuencias del delito.

2.8 La inimputabilidad.

La inimputabilidad es un elemento negativo del delito.

[64] Jiménez de Asúa Luis, *op.cit.*, p. 302.

Las causas de inimputabilidad son todas aquellas capaces de anular o neutralizar, ya sea el desarrollo o la salud de la mente, en cuyo caso el sujeto carece de la aptitud psicológica para la delictuosidad. Un sujeto es inimputable cuando su aptitud psíquica o su capacidad para comprender la ilicitud de su actuar es inexistente por encontrarse gravemente alterada o inmadura. El inimputable es penalmente irresponsable.[65]

Principales causas de inimputabilidad:

a).- Minoría de edad

b).- Enfermedades mentales

c).- Estado mental transitorio

d).- Sordomudez

e).- Imbecilidad

a).- Minoría de Edad. Los menores de 18 años son inimputables y, por lo mismo, cuando realizan comportamientos típicos no se configuran los delitos respectivos.

b).- Enfermedades mentales. Las enfermedades mentales son procesos psicopatológicos agudos, crónicos o permanentes, que producen alteraciones modificatorias de la personalidad psíquica del enfermo, anulando su capacidad de entender y querer.

Los locos o los que sufran cualquier otra debilidad, enfermedad o anomalía mentales, y que hayan ejecutado hechos o incurrido en omisiones definidos como delitos serán recluidos en manicomios o en departamentos especiales por todo el tiempo necesario para su curación.

[65]Camargo pacheco, María de Jesús, *op cit.*, 3 de marzo 2008.

Existe en algunos casos la ausencia absoluta de imputabilidad y por lo tanto no se le aplica una pena sino una medida de seguridad.

Además las enfermedades mentales pueden ser permanentes o transitorias. Asimismo los trastornos mentales pueden tener diferentes grados, por lo que un perito valuador es el que debe considerar si tienen su capacidad disminuida por completo o no, y si por tanto excluye su imputabilidad o sólo esta atenuada.

c).- Estado mental transitorio.- Es toda perturbación psíquica de temporalidad pasajera que suprime las facultades volitivas e intelectivas del sujeto, sólo afecta la imputabilidad, cuando la alteración mental se traduce en un estado pleno de inconciencia. Hallarse el acusado, al cometer la infracción, en un estado de inconsciencia de sus actos, determinado por el empleo accidental o involuntario de sustancias tóxicas, embriagantes o estupefacientes.

Causas del estado mental transitorio:

1. Patológicas: empleo de sustancias embriagantes, tóxicas o enervantes.
2. Fisiológicas: hipnotismo y sonambulismo
3. Psíquicas: Emociones y arrebatos pasionales

- Sustancias tóxicas, embriagantes o estupefacientes.- Cuando por el empleo de una *sustancia tóxica* (yodoformo, ácido salicílico…), se produce una intoxicación que provoca un estado de inconsciencia patológica, las acciones que en tal estado se ejecutan, no son propiamente del sujeto sino ajenas. Ahora bien, si la intoxicación ha sido procurada por el sujeto mismo, voluntaria y deliberadamente se estará en el caso de una acción *liberae in causa*.

- Respecto de la *embriaguez,* solo habrá ininmputabilidad, cuando sea plena y accidental, involuntaria. Por el contrario la embriaguez voluntaria debe de ser considerada como índice de mayor temibilidad.

- Toxinfecciones. Por el padecimiento de algunas enfermedades de tipo infeccioso o microbiano, a veces sobreviven trastornos mentales, como el tifo, la tifoidea, la rabia o la poliomielitis. En estos casos el enfermo puede llegar a la inconsciencia. Para determinar los efectos de dichos padecimientos el juzgador debe tomar en cuenta a dictámenes médicos y psiquiátricos.

- Sonambulismo- El estado de inconsciencia natural no provocado excluye el delito. Puede dar lugar a delitos culposos cuando quien, sabedor de su anomalía no toma las medidas de prevención.

- Sordomudez. A los sordomudos que contravengan los preceptos de una ley penal, se les recluirá en una escuela o establecimiento especial para sordomudos por el tiempo que fuere adecuado para su educación e instrucción.

- Imbecilidad. Son perturbaciones del desarrollo psíquico en el area del intelecto , ya que no hay un desarrollo espiritual, la mayoría de las bases estan relacionados con comportamientos psicopáticos de la personalidad.

En este punto es de importancia tratar lo referente a las acciones libres en su causa.

Acciones libres en su causa son aquellas en que el autor establece la causa decisiva en una situación de imputabilidad y se desenvuelve luego en una decisión de inimputabilidad.[66]

Se decidió en un estado de imputabilidad y se produjo en estado de inimputabilidad.

[66] Mezger Edmund, “Derecho penal, Tomo I, parte general”, Valleta ediciones, Buenos Aires, 2004, p.152.

Cuando con anterioridad a dicho comportamiento se ha colocado dolosa o culposamente en un estado de inimputabilidad, conserva la imputabilidad del sujeto por el nexo causal entre la propia acción y el resultado.

2.9 La culpabilidad.

Como elemento positivo del delito; es el poder de hacer responsable al autor. Se refiere a la probable responsabilidad que tiene el inculpado.

"Consiste en un juicio sobre el autor mediante el cual se determina si se le puede reprochar el haberse comportado contrariamente a lo establecido en el orden jurídico".[67]

Abarca todos los presupuestos bajo los cuales una conducta puede resultar digna de pena. Se determina como contraria al deber y reprochable.

> "Existen tres requisitos que integran la culpabilidad. En el momento del hecho, el autor tiene que haber sido capaz, primero de percatarse de la antijuridicidad de su conducta y de orientarse según las normas jurídicas. Además tiene que haber conocido el ilícito efectivamente o, si no, haber tenido la posibilidad de conocerlo. Y finalmente, no debe haber cometido el hecho en una situación de apremio tan extraordinario que lo haga exculpable".[68]

Edmundo Mezger en su libro derecho penal menciona cuatro características legales de la culpabilidad.

1. La imputabilidad. Es decir el sujeto activo debe tener una condición mental normal.

[67] Diaz Aranda Enrique, "Derecho Penal, Parte General", Editorial Porrúa, México, 2004, p.359.
[68] Stratenwerth Gûnter, "Derecho penal. Parte general I", Editorial Hammurabi, Buenos Aires, Argentina, 2005, p.136.

2. Una forma de culpabilidad. Dolo o culpa.
3. La ausencia de causas de exclusión o de culpabilidad.
4. El concepto unitario de culpabilidad que se encuentra en la reprochabilidad.

Dos teorías explican la culpabilidad:

Teoría Psicológica de la culpabilidad.- Es el lazo de causalidad psíquica que une al sujeto con el hecho que realiza. Concibe a la culpabilidad como la relación subjetiva que media entre el autor y el hecho. En consecuencia, supone el análisis de la situación interna del sujeto, la culpabilidad reside en él, es la fuerza moral, subjetiva del delito.

Teoría Normativa. Concibe a la culpabilidad como un juicio de reproche. Es el juicio en el cual determinada conducta a causa de cierta situación dada, es reprochable. Es una valoración fundada en la exigibilidad de la conducta ordenada por la ley.[69]

La siguiente tesis da un enfoque más claro de lo que es la culpabilidad:

Registro No. *921582*
Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Apéndice (actualización 2002)
Tomo II, Penal, P.R. TCC
Página: 190
Tesis: 93
Tesis Aislada
Materia(s): Penal

CULPABILIDAD Y PELIGROSIDAD. SU DIFERENCIA.-

[69]Camargo pacheco, María de Jesús, http://cursweb.educadis.uson.mx/mcamargo/documentos/NOTAS%20PARA%20EDICION%20DERECHO%20PENAL%20I.doc, 3 de marzo 2008.

Por culpabilidad se entiende el conjunto de presupuestos o caracteres que debe tener una conducta para que le sea reprochada jurídicamente a su autor, ésta se entiende como el elemento subjetivo del delito que comprende el juicio de reproche por la ejecución de un hecho contrario a lo mandado por la ley; en tanto que la peligrosidad es una circunstancia personal del delincuente que lo hace socialmente temible por su malignidad, esto es, la perversidad constante y activa que se debe esperar de parte del mismo autor del delito, entendida también como la saña y maldad manifestada por el sujeto activo del ilícito penal en la realización de los actos criminales. Es por ello que se reformó el artículo 52 del Código Penal y que a partir del primero de febrero de 1994 establece: "El Juez fijará las penas y medidas de seguridad que estime justas y procedentes dentro de los límites señalados para cada delito, con base en la gravedad del ilícito y el grado de culpabilidad del agente ...", con lo cual se logra la finalidad de la individualización de la pena a imponer.

SEXTO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO.

Amparo directo 4586/2001.-31 de enero de 2002.-Unanimidad de votos.-Ponente: Guillermo Velasco Félix.-Secretaria: Gloria Rangel del Valle.

Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XV, mayo de 2002, página 1205, Tribunales Colegiados de Circuito, tesis I.6o.P.36 P.

La culpabilidad es un elemento característico de la infracción y de carácter normativo, puesto que no se puede hacer sufrir a un individuo las consecuencias del acto que le es imputable más que a condición de declararle culpable de él. Por lo que debe haber llevado a cabo la conducta para que pueda se ser considerado culpable.

Los motivos gradúan la culpabilidad. De ordinario, una vez afirmada la culpabilidad, concurren circunstancias que la agravan o atenúan, según los móviles del agente.

Las cuatro funciones del móvil son:[70]

1. El móvil debe servir para la investigación acerca de la calidad del motivo psicológico del delito.
2. La calidad moral y social del motivo conduce a un criterio fundamental para determinar la temibilidad y la condición peligrosa del delincuente.
3. La calidad de motivos actúa con eficacia permanente en cuanto a la elección del medio defensivo que debe adoptarse respecto a los distintos delincuentes.
4. Cuando el motivo sea de tal naturaleza que haga desaparecer el acto que se ejecutó toda huella de temibilidad, puede, excepcionalmente, cuando no se opongan otros factores, decidir que no procede la aplicación de ninguna medida defensiva, porque sería superflua.

El móvil se valora como decisivo en la elección de la pena.

La edad es un punto importante cuando se analiza la culpabilidad, tal como se observa en la siguiente tesis:

Registro No. *174502*
Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXIV, Agosto de 2006
Página: 2167
Tesis: VIII.4o.7 P
Tesis Aislada
Materia(s): Penal

CULPABILIDAD. LA EDAD E INSTRUCCIÓN DEL ACTIVO SIRVEN PARA SUSTENTARLA (LEGISLACIÓN DEL ESTADO DE COAHUILA).

[70] Jiménez de Asúa Luis, op. cit., p329.

La edad e instrucción del sujeto activo son datos pertinentes para considerar que conocía, o por lo menos que estuvo en condiciones razonables de conocer la ilicitud de la conducta que realizó al conducirse dolosamente, o bien, de conocer el deber jurídico que transgredió al obrar con culpa; por lo que, además de la exigibilidad de la conducta conforme al derecho, aquéllos sirven al juzgador para sustentar la culpabilidad del sentenciado como elemento del delito en lo sustantivo, y en lo procesal su responsabilidad penal, de conformidad con los artículos 449 y 487 del Código de Procedimientos Penales, en relación con los numerales 48 y 49 del Código Penal, ambos del Estado de Coahuila.

CUARTO TRIBUNAL COLEGIADO DEL OCTAVO CIRCUITO.

Amparo directo 261/2005. 20 de abril de 2006. Unanimidad de votos. Ponente: Ramón Raúl Arias Martínez. Secretario: Héctor Guillermo Maldonado Maldonado.

Formas de culpabilidad.

La culpabilidad reviste dos formas: dolo y culpa. Según el agente dirija su voluntad consciente a la ejecución del hecho tipificado en la ley como delito, o cause igual resultado por medio de su negligencia o imprudencia. También existe la preterintencionalidad que es una mezcla del dolo y la culpa.

El dolo.

"Los elementos que conforman el dolo son tres: intelectual (representación del resultado) ético (conciencia de la injusticia del resultado) y volitivo (propósito de producirlo). Los elementos intelectual y ético del dolo requieren el conocimiento del sujeto del orden jurídico pleno del Estado".[71]

En la tesis siguiente se muestra como se estudia el dolo como un elemento de la culpabilidad.

[71] Arilla Bas Fernando, *op. cit.*, p.250.

Registro No. 183551

Localización:

Novena Época

Instancia: Tribunales Colegiados de Circuito

Fuente: Semanario Judicial de la Federación y su Gaceta

XVIII, Agosto de 2003

Página: 1545

Tesis: I.10o.P. J/1

Jurisprudencia

Materia(s): Penal

DOLO GENÉRICO. SU ANÁLISIS DEBE HACERSE AL EXAMINARSE LA CULPABILIDAD (LEGISLACIÓN DEL DISTRITO FEDERAL).

No es legalmente aceptable que la Sala responsable analice el dolo genérico tanto en el injusto como en la responsabilidad penal, pues con independencia de que este tribunal de amparo considera respetable su posición ideológica welzeniana, o su simpatía con la llamada doble posición del dolo (doppelstellung), sea en el tipo o en la culpabilidad, sostenida por Jescheck, el legislador mexicano, desde el tres de mayo de mil novecientos noventa y nueve, consideró que el dolo debe estudiarse en la culpabilidad y así lo estableció en las reformas al artículo 122 del Código de Procedimientos Penales para el Distrito Federal; por lo que debe estarse a lo que disponga la ley y no a lo que digan respetables doctrinarios.

DÉCIMO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO.

Amparo directo 3840/2002. 31 de enero de 2003. Unanimidad de votos. Ponente: Jorge Ojeda Velázquez. Secretario: Jerónimo Nicolás Arellanes Ortiz.

Amparo directo 3940/2002. 31 de enero de 2003. Unanimidad de votos. Ponente: Jorge Ojeda Velázquez. Secretario: Jerónimo Nicolás Arellanes Ortiz.

Amparo directo 4000/2002. 31 de enero de 2003. Unanimidad de votos. Ponente: Jorge Ojeda Velázquez. Secretario: Jerónimo Nicolás Arellanes Ortiz.

Amparo directo 440/2003. 31 de marzo de 2003. Mayoría de votos; unanimidad en relación con el tema contenido de esta tesis. Ponente: Carlos Enrique Rueda Dávila. Secretario: Víctor Manuel Cruz Cruz.

Amparo directo 860/2003. 19 de mayo de 2003. Unanimidad de votos. Ponente: Jorge Ojeda Velázquez. Secretaria: Martha García Gutiérrez.

Ejecutoria:
1.- Registro No. 17684
Asunto: AMPARO DIRECTO 860/2003.
Promovente:
Localización: 9a. Época; T.C.C.; S.J.F. y su Gaceta; XVIII, Agosto de 2003; Pág. 1546;

Por lo que el dolo debe estudiarse en la culpabilidad para que pueda ser valorada de una forma adecuada de acuerdo a la forma de actuar del sujeto activo.

La Culpa.

La culpa simple consiste en la voluntaria omisión de diligencia en calcular las consecuencias posibles y previsibles del propio hecho. La culpa se da por negligencia, impericia, previsión, imprudencia, falta de aptitud o de cuidado.

Preterintencionalidad.

Esta se da cuando existe un exceso en el fin, es decir cuando el sujeto activo quiere causar un resultado y causa uno más grave.

Para poder establecer la culpabilidad es necesario estudiar el caso en concreto para ver si se configuro el dolo, la culpa o la preterintencionalidad.

2.10 La inculpabilidad.

Es un elemento negativo del delito y son las especiales situaciones que concurren en la ejecución del hecho realizado por quien siendo imputable, no se le puede reprochar su conducta. Como en la violencia moral o miedo grave y el error.

a).- Violencia moral o miedo grave.- Consiste en obrar en virtud de miedo grave o temor fundado o irresistible de un mal inminente y grave en bienes jurídicos propios o ajenos, siempre que no exista otro medio practicable y menos perjudicial al alcance del agente.

Para determinar lo fundado e irresistible se valorarán tomando en cuenta el carácter intimidante de la amenaza y la naturaleza débil del amenazado. Así como que el mal que amenaza sea mayor o igual que el causado para evitarlo; que el agente obre de buena fe creyendo la mayor gravedad del mal que amenaza; que exista amenaza a la vida a los bienes propios o ajenos.

En cuanto al miedo encontramos la siguiente tesis aislada:

Localización:
Sexta Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación
Segunda Parte, CXXVI
Página: 42
Tesis Aislada
Materia(s): Penal

MIEDO GRAVE O TEMOR FUNDADO, EXCLUYENTES DE.

La excluyente de miedo grave o temor fundado, plantea una situación disyuntiva, ya que independiza al miedo del temor, de tal suerte que ambos conceptos no son idénticos. El miedo, de acuerdo con la definición que establece Rivot en su tratado de psicología de los sentimientos, viene a ser la reacción emocional viva y

persistente de un mal futuro. El miedo, desde el punto de vista ideológico, puede provenir tanto del interior del sujeto, como del exterior del mismo, de percepciones y de ilusiones. Sin embargo, su prueba, por ser una situación eminentemente psicológica, solamente podrá ser apreciada por técnicas psicológicas que, previo estudio de la personalidad del sujeto, especiales de sus modalidades de reacción, pudieran determinar si el delito ejecutado por aquél era el resultado de una reacción emotiva de las que se hace mérito. En lo que respecta al temor, éste viene a constituir la prevención por parte del sujeto, de un mal del cual solamente puede liberarse mediante la ejecución; el temor coincide en otras palabras, con la antiguamente denominada vis compulsiva, en la cual la voluntad del sujeto, aunque coaccionada, no pierde su calidad de libre determinación.

Amparo directo 6855/64. Rafael Vicente Solís. 11 de febrero de 1965. Cinco votos. Ponente: Agustín Mercado Alarcón.

Por lo que el temor hace que la persona cometa ciertas conductas que no realizaría en otras circunstancias sino que una conducta o persona externa hace que reaccione de determinada manera.

Otra tesis que lo establece de manera clara es la siguiente:

Registro No. *258894*
Localización:
Sexta Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación
Segunda Parte, CXIX
Página: 29
Tesis Aislada
Materia(s): Penal

MIEDO GRAVE Y TEMOR FUNDADO, NO PUEDEN COEXISTIR LAS EXCLUYENTES DE.

El miedo grave y el temor fundado son excluyentes diversas, ya que el primero es causa e inimputabilidad en cuanto anula la causación psicológica normal y el

segundo es causa de inculpabilidad, por no exigibilidad de otra conducta. El miedo grave requiere que el sujeto activo, como resultado en un estímulo exterior, real o putativo, ejecute su conducta típica y antijurídica, bajo un estado psicológico que nulifique su capacidad de entender y querer, tanto de la conducta señalada como del resultado. Es decir, el fundamento de la inincriminación reside en que el agente haya perdido el dominio de su freno inhibitorio y actúe en forma automática y al impulso del instinto de conservación. El temor fundado, requiere de la existencia de un elemento objetivo, constituido por un mal inminente y grave en la persona del sujeto activo o de la persona ligada con él por afecto o gratitud suficientes; y requiere también de un elemento subjetivo, constituido por la imposibilidad de resistir el temor fundado que produce el mal referido. El temor fundado no opera en conductas de repulsa, como sucede en la legítima defensa, sino a la inversa, la conducta del sujeto activo es de aceptación y obedece a vis compulsiva ante el mal inminente y grave que le impone la comisión del acto típico, antijurídico, imputable pero no culpable, porque al sujeto en tales condiciones no se le puede exigir jurídica y racionalmente otra conducta. El temor fundado es acatamiento del actuar típico de quien lo sufre por la imposición de quien lo provoca.

Amparo directo 6152/66. J. Jesús Ochoa Vivas. 3 de mayo de 1967. Unanimidad de cuatro votos. Ponente: José Luis Gutiérrez Gutiérrez.

Sexta Epoca, Segunda Parte:

Volumen CXVIII, página 28. Amparo directo 8662/66. Cosme Regalado García. 12 de abril de 1967. Cinco votos. Ponente: Abel Huitrón y Aguado.

Volumen LIII, página 43. Amparo directo 4845/61. Aurelio Hernández González. 23 de noviembre de 1961. Cinco votos. Ponente: Alberto R. Vela.

Volumen VI, página 187. Amparo directo 52/55. Anselmo Peña Mosqueda. 18 de octubre de 1957. Cinco votos. Ponente: Luis Chico Goerne.

Volumen II, página 97. Amparo directo 998/56. Rodolfo Ordóñez H. 13 de agosto de 1957. Cinco votos. Ponente: Genaro Ruiz de Chávez.

Nota:

En el Volumen LIII, página 43, esta tesis aparece bajo el rubro "MIEDO GRAVE,

TEMOR FUNDADO, EXCLUYENTES.".

En el Volumen VI, página 187, esta tesis aparece bajo el rubro "MIEDO GRAVE Y TEMOR FUNDADO, COMO EXCLUYENTES (LEGISLACION DE GUANAJUATO).".

En el Volumen II, página 97, esta tesis aparece bajo el rubro "MIEDO GRAVE, TEMOR FUNDADO Y ESTADO DE NECESIDAD (EXCLUYENTES CONTRADICTORIAS)"

En la tesis anterior se puede observar que no es lo mismo miedo grave y temor fundado, aún cuando ambas son excluyentes de culpabilidad, son situaciones diversas las que regula y no pueden estar ambas en una conducta, ya que tienen diversos supuestos y los factores externos son diferentes.

Otra tesis que abarca el punto anterior es la siguiente.

Registro No. 258914
Localización:
Sexta Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación
Segunda Parte, CXVIII
Página: 28
Tesis Aislada
Materia(s): Penal

MIEDO GRAVE Y TEMOR FUNDADO, NO PUEDE COEXISTIR LAS EXCLUYENTES DE.

No puede coexistir las excluyentes de miedo grave y de temor fundado, por tener cada una un contenido distinto.

Amparo directo 8662/66. Cosme Regalado García. 12 de abril de 1967. Cinco votos. Ponente: Abel Huitrón y Aguado.

Sexta Epoca, Segunda Parte:

Volumen LIII, página 43. Amparo directo 4845/61. Aurelio Hernández González. 23 de noviembre de 1961. Cinco votos. Ponente: Alberto R. Vela.

Volumen VI, página 187. Amparo directo 52/55. Anselmo Peña Mosqueda. 18 de octubre de 1957. Cinco votos. Ponente: Luis Chico Goerne.

Volumen II, página 97. Amparo directo 998/56. Rodolfo Ordóñez H. 13 de agosto de 1957. Cinco votos. Ponente: Genaro Ruiz de Chávez.

Nota:

En el Volumen LIII, página 43, esta tesis aparece bajo el rubro "MIEDO GRAVE, TEMOR FUNDADO, EXCLUYENTES.".

En el Volumen VI, página 187, esta tesis aparece bajo el rubro "MIEDO GRAVE Y TEMOR FUNDADO, COMO EXCLUYENTES (LEGISLACION DE GUANAJUATO).".

En el Volumen II, página 97, esta tesis aparece bajo el rubro "MIEDO GRAVE, TEMOR FUNDADO Y ESTADO DE NECESIDAD (EXCLUYENTES CONTRADICTORIAS).".

En la tesis anterior se puede observar de manera clara el no poder coexistir ambos supuestos el miedo grave y el temor fundado.

Registro No. 259441
Localización:
Sexta Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación
Segunda Parte, LXXXIX
Página: 12
Tesis Aislada
Materia(s): Penal

MIEDO GRAVE O TEMOR FUNDADO.

No existe excluyente de responsabilidad de miedo grave o temor fundado, si en autos no se encuentra probado que la víctima realizara algún acto positivo en contra del acusado que creara en éste un estado psicológico que lo colocara en una situación de incapacidad para entender y querer tanto la acción como su resultado.

Amparo directo 4738/64. José Reynoso Padilla. 19 de noviembre de 1964. Unanimidad de cuatro votos. Ponente: Mario G. Rebolledo Fernández.

Por lo cual, para que haya una excluyente de responsabilidad es necesario que se genere una conducta por parte del sujeto que alega dicha excluyente, es decir tiene que actuar o reaccionar debido a la circunstancia que le esta infundiendo ese miedo grave o temor fundado.

b).- Error. Es la falsa concepción de la realidad, no es ausencia de conocimiento sino conocimiento distorsionado, deformado e incorrecto.

Cabe distinguir el error esencial del error accidental. Solo el error esencial excluye en delito cuando es invencible y dado las circunstancias del caso concreto, el sujeto no estaba en posibilidad de superarlo.

Se trata de error accidental cuando el error recae sobre circunstancias accidentales o secundarias. La persona equivoca el objeto o la persona sobre la cual dirigió su actuación:

Clases de error:

Error de tipo (o error de hecho).- El agente obra bajo el error sobre alguno de los elementos del tipo penal. Impide que el agente comprenda la naturaleza

criminosa de su acto. Ejemplo quien yace con madre o hermana ignorando el parentesco, quien se apodera de cosa ajena creyéndola propia.

Error de prohibición (error de derecho).- El agente cree erróneamente que su actuación está amparada en una causa de justificación, cree que su conducta es lícita. El error puede recaer también respecto de la ilicitud de la conducta, ya sea que el sujeto desconozca la ley o el alcance de la misma. Sin embargo el conocimiento de la ley constituye una presunción absoluta. La ignorancia de la ley a nadie beneficia. Ejemplo. Quien comete aborto en un país en donde sí es penado.

Hay ocasiones en que sin encontrarse en un peligro real e inminente, el sujeto tiene derecho a ejercer una repulsa sobre lo que cree que existe una agresión en su contra que es precisamente lo que se conoce como *eximentes putativas*.

Puede ser vencible cuando con un mínimo de cuidado el sujeto habría podido conocer sobre la licitud de la conducta es invencible cuando no es posible exigirle ese conocimiento.

2.11 Las condiciones objetivas de punibilidad.

Como aspecto positivo del delito. *"Son aquellas circunstancias objetivas y subjetivas establecidas en la ley, que sin pertenecer al tipo, tienen una relación directa e inmediata con éste y son necesarias para la existencia o modificación de la pena"*.[72]

Existen condiciones objetivas y subjetivas de punibilidad que aumentan las penas y condiciones objetivas y subjetivas de punibilidad que disminuyen las penas.

[72] Hernández Islas Juan Andrés, *op.cit*., p.137.

1. Las condiciones objetivas de punibilidad. Son circunstancias materiales o humanas fuera del tipo, es el acto procesal necesario para que la punibilidad se vea concretizada

2. Las condiciones subjetivas de punibilidad Son circunstancias anímicas extras todas estas influyen para que aumente la pena es una situación o previsión jurídica que debe rodear al agente para poder aplicar la pena o evitar que la punibilidad desaparezca.

Por otro lado las condiciones objetivas y subjetivas de punibilidad que disminuyen las penas son circunstancias materiales o humanas fuera del tipo y las subjetivas circunstancias anímicas extras las cuales influyen para que disminuya la pena.

Este elemento se refiere a la condición objetiva de procedibilidad, a la calidad indispensable que exige el poder judicial para que haya movimiento. En el caso de la querella, es una condición ineludible para proceder en determinados delitos, lo cual significa, que es necesaria la manifestación de la voluntad del que resulte agraviado para que el Estado pueda proceder a perseguir el delito en que la propia ley exige querellarse; la ley exige que solo la persona que resulte afectada directamente pueda presentarse ante el órgano investigador mediante querella, que deba presentar el propio agraviado, o en su defecto, el legítimo representante.

Conforme a lo que dispone el artículo 16, de la Constitución Política de los Estados Unidos Mexicanos, en su párrafo segundo, que es necesario para girar una orden de aprehensión, que preceda denuncia, acusación o querella, por lo cual, la falta de este requisito, constituirá una falta de condición objetiva.

Su característica consiste no sólo en ser objetivas, sino principalmente extrínsecas al tipo legal, que nada añaden a él y que por tanto, no tienen que ser abarcadas por la culpabilidad del autor.

Además en los delitos informáticos deben estudiarse las características de los sujetos que cometen ilícitos informáticos así como el trabajo o puesto que desempeñan para poder establecer una pena más justa para los sujetos activos.

2.12 La ausencia de condiciones objetivas de punibilidad.

Cuando no se den condiciones objetivas de punibilidad que disminuyen o aumenten las penas, se aplicará la pena establecida en el tipo básico.

2.13 La punibilidad.

Depende de condiciones, que derivan, de la exigencia del Estado de Derecho de la legalidad del hecho de imponer la pena. *"Es una situación jurídica en que se encuentra aquel que por haber cometido una infracción penal, se hace merecedor de un castigo"*.[73]

La pena se justifica desde un punto de vista político-criminal. Es decir, representa la amenaza de la pena que se impondrá al autor que comete una conducta delictiva.

La pena es, pues, la ejecución de la punición, y se da en la instancia o fase ejecutiva.

En la punibilidad es necesario que se tomen en cuenta varios aspectos, la cual va a ser determinada por el juzgador. La tesis que a continuación se menciona lo refiere de forma clara.

Registro No. 173753
Localización:
Novena Época

[73] Vergara Tejada José Moisés, "Manual de Derecho Penal", Ángel Editor, México, 2002, p.363.

Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXIV, Diciembre de 2006
Página: 1138
Tesis: I.7o.P. J/5
Jurisprudencia
Materia(s): Penal

INDIVIDUALIZACIÓN DE LA PENA. PARA ESTABLECERLA BASTA QUE LA EXPRESIÓN EMPLEADA POR EL JUZGADOR PERMITA DETERMINAR CON CONGRUENCIA, MOTIVACIÓN Y EXHAUSTIVIDAD EN CADA CASO CONCRETO Y TOMANDO EN CUENTA EL MÍNIMO Y MÁXIMO DE LA PUNIBILIDAD DEL DELITO DE QUE SE TRATE, LA CORRESPONDENCIA ENTRE LA SANCIÓN IMPUESTA Y EL GRADO DE CULPABILIDAD DEL SENTENCIADO.

Del análisis de los artículos 51 y 52 del Código Penal para el Distrito Federal (artículos 70 y 72 del Código Penal del Distrito Federal vigente) se advierte que el Juez goza de autonomía para imponer las penas y medidas de seguridad que estime justas, tomando en consideración los márgenes de punibilidad que para cada delito establezca la ley, la gravedad del ilícito de que se trate y el grado de culpabilidad del inculpado; sin embargo, y precisamente en atención al arbitrio del juzgador, la ley no fija denominaciones o categorías predeterminadas respecto de la graduación de la culpabilidad, sino que se limita a proporcionar reglas normativas para regular el criterio del Juez; de ahí que éste deba ser especialmente cuidadoso con la expresión que emplee para designar el grado de culpabilidad del enjuiciado, sin perder de vista que de acuerdo al principio de congruencia que rige en toda resolución judicial, el quántum de la pena (cualquiera que ésta sea) o medida de seguridad impuesta, debe ser proporcional a dicho grado, así como que para referirse a las diferentes graduaciones entre la mínima y la máxima se han empleado diversos vocablos convencionalmente aceptados, tales como "mínima", "equidistante entre la mínima y media", "media", "equidistante entre media y máxima" y "máxima"; sin que esto signifique que para mencionar los puntos intermedios entre estos parámetros, el Juez esté obligado a realizar combinaciones de los vocablos anteriores ad infinitum; por ende, basta que la expresión empleada por el juzgador permita determinar con congruencia, motivación y exhaustividad en cada caso concreto, y tomar en cuenta

el mínimo y máximo de la punibilidad del delito de que se trate, la correspondencia entre la pena concretamente impuesta y el grado de culpabilidad del sentenciado.

SÉPTIMO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO.

Amparo directo 267/2002. 8 de febrero de 2002. Unanimidad de votos. Ponente: Miguel Ángel Aguilar López. Secretaria: Ana Luisa Beltrán González.

Amparo directo 2827/2004. 28 de octubre de 2004. Unanimidad de votos. Ponente: Carlos Hugo Luna Ramos. Secretaria: Rosa Dalia A. Sánchez Morgan.

Amparo directo 2107/2005. 18 de agosto de 2005. Unanimidad de votos. Ponente: Ricardo Ojeda Bohórquez. Secretario: Jorge Antonio Salcedo Garduño.

Amparo directo 2077/2005. 25 de agosto de 2005. Unanimidad de votos. Ponente: Ricardo Ojeda Bohórquez. Secretario: Jorge Antonio Salcedo Garduño.

Amparo directo 2467/2005. 8 de septiembre de 2005. Unanimidad de votos. Ponente: Ricardo Ojeda Bohórquez. Secretario: Jorge Antonio Salcedo Garduño.

Ejecutoria:
1.- Registro No. 19836
Asunto: AMPARO DIRECTO 267/2002.
Promovente:
Localización: 9a. Época; T.C.C.; S.J.F. y su Gaceta; XXIV, Diciembre de 2006; Pág. 1139;

2.14 Las excusas absolutorias.

Es un elemento negativo del delito. Una causa de impunidad o excusas absolutorias, significa un caso en que el estado prácticamente renuncia a ejercer el derecho punitivo por causas políticas.

En esta se encuentran las causas personales de exclusión de la pena. Hacen decaer en forma excepcional una necesidad de pena que, en principio, está fuera de duda. Hace que desaparezca la pena, aún cuando el delito se haya cometido.

En este punto sería conveniente citar la siguiente tesis jurisprudencial.

Registro No. *921436*
Localización:
Novena Época
Instancia: Pleno
Fuente: Apéndice (actualización 2002)
Tomo II, Penal, Jurisprudencia SCJN
Página: 15
Tesis: 7
Jurisprudencia
Materia(s): Penal

EXCUSAS ABSOLUTORIAS Y EXCLUYENTES DE RESPONSABILIDAD. SUS DIFERENCIAS.-

Las excusas absolutorias son causas que al dejar subsistente el carácter delictivo de la conducta o hecho tipificado como ***delito*** *en la ley, impiden la aplicación de la pena, es decir, son aquellas en las que aun cuando se configure el* ***delito****, no permiten que se sancione al sujeto activo en casos específicos; en tanto que las excluyentes de responsabilidad se caracterizan por impedir que ésta surja. En otras palabras, en las citadas excluyentes la conducta tipificada en la ley no es incriminable desde el inicio; mientras que en las excusas absolutorias la conducta es incriminable, pero no sancionable, consecuentemente no relevan al sujeto activo de su responsabilidad en la comisión de la conducta típica, sino que determinan su impunibilidad.*

Acción de inconstitucionalidad 10/2000.-Diputados integrantes de la Asamblea Legislativa del Distrito Federal.-29 y 30 de enero de 2002.-Mayoría de siete votos de los señores Ministros Mariano Azuela Güitrón, Juventino V. Castro y Castro, José de Jesús Gudiño Pelayo, Humberto Román Palacios, Olga Sánchez Cordero de García Villegas, Juan N. Silva Meza y presidente Genaro David Góngora Pimentel respecto de la constitucionalidad de la fracción III del artículo 334 del Código Penal para el

Distrito Federal; y en relación con el artículo 131 bis del Código de Procedimientos Penales para el Distrito Federal, en virtud de que la resolución de su inconstitucionalidad no obtuvo la mayoría calificada de cuando menos ocho votos exigida por el último párrafo de la fracción II del artículo 105 constitucional, se desestimó la acción de conformidad con lo dispuesto en el artículo 72 de la ley reglamentaria de las fracciones I y II de dicho precepto constitucional.-En cuanto al criterio específico contenido en la tesis no hubo discrepancia entre los once señores Ministros.-Ponente: Olga Sánchez Cordero de García Villegas.-Secretario: Pedro Alberto Nava Malagón.

Semanario Judicial de la Federación y su Gaceta, Tomo XV, febrero de 2002, página 592, Pleno, tesis P./J. 11/2002; véase la ejecutoria y los votos en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XV, marzo de 2002, páginas 793 y 861, 862, 867, 878, 888, 896 y 904, respectivamente.

Por lo que cual se puede observar que en las excusas absolutorias puede existir la conducta y por ende configurarse en el tipo, sin embargo no va a ser sancionada o penada dicha conducta.

Carrancá y Trujillo clasifica las excusas absolutorias de la siguiente manera:[74]

- Excusas en razón de los móviles afectivos revelados.
- Excusa en razón de la copropiedad familiar.
- Excusas en razón de la maternidad consciente.
- Excusas en razón del interés social preponderante.
- Excusa en razón de poca peligrosidad del individuo.

Existen las excluyentes supralegales y son aquellas que sin estar expresamente previstas por la ley, destruyen alguno de los caracteres del delito o presupuestos de la punibilidad de la conducta típica.

[74] *Ibid*, p.368.

CAPÍTULO III. REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN MÉXICO Y OTROS PAÍSES.

En este punto de la presente tesis se abordará de una manera clara la forma en que se encuentran tipificados los delitos informáticos, la legislación a la que pertenecen y la forma en que están regulados.

Además se establecen los países en los que han sido tipificados, aún cuando es claro que no resulta fácil por tratarse de bienes intangibles y de difícil comprobación y persecución. No hay una tipificación especifica en la mayoría de los países, existe una creciente tecnología y es difícil su tipificación porque puede tratarse de un delito que produjo efectos en otro país, entonces nos enfrentamos a otro problema que es la jurisdicción.

1. El delito informático en México.

Los delitos informáticos es un tema tratado de forma inusual ya que como se trata de conductas difíciles de entender, perseguir y castigar no se les da el tratamiento idóneo. Un punto importante de abarcar en cuanto a estos tipos de delitos es el tema de la responsabilidad. La responsabilidad se genera de ciertas conductas que afectan el interés general y por consiguiente el Estado debe penalizar y perseguir.

La forma en que este tipo penal es tratado en México no es usual debido a que la tecnología es desbordante, siempre se encuentra un paso delante de las regulaciones que pudieren existir y que se van creando.

Por lo anterior es importante observar como es que desarrollan el tipo de “delitos informáticos” en las legislaciones vigentes de nuestro país.

1.1 La Legislación Penal Federal y Estatal.

En materia Federal podemos encontrar un capítulo respectivo a los llamados delitos informáticos.

En el Código Penal Federal se encuentra establecido en el título noveno denominado “Revelación de secretos y acceso ilícito a sistemas y equipos de informática”, en el capitulo II en los artículos 211 bis 1 al 211 bis 7.

Los delitos informáticos se encuentran en legislaciones estatales aún cuando cuentan una diversidad de denominaciones. En algunas otras no se encuentran contemplados como se puede observar más adelante.

Por lo cual se establece a continuación una relación de cada uno de los Estados que conforman la República mexicana y la forma en que contemplan este tipo de delitos.

En los párrafos siguientes se establecerá de manera breve lo que refieren al respecto de delitos informáticos en los Códigos Penales de cada Estado.

Aguascalientes.

Legislación Penal para el Estado de Aguascalientes.

Se encuentra regulado un aspecto en el libro primero denominado: “De las figuras típicas” “Titulo primero de las figuras típicas dolosas, capitulo décimo segundo Tipos penales protectores de la confidencialidad”.

> ”Artículo 79. La revelación de secretos consiste en el aprovechamiento de archivos informáticos de uso personal o en la revelación de una comunicación reservada que se conozca o que se haya recibido por motivo de empleo, cargo o puesto, sin justa causa, con perjuicio de alguien y sin consentimiento de la víctima.

Al responsable …”

Si bien del artículo anterior no se aprecia que se trate de delitos informáticos si lo es el hecho de obtener una información considerada como secreta obtenida de un archivo informático. Que se puede entender como una acción de obtener algo ilícito por un medio informático. Podría pensarse que este precepto sólo establece lo que conocemos como el ilícito de revelación de secretos, sin embargo entra en la categoría de delitos informáticos cuando menciona este medio.

Baja California.

Código Penal para el Estado de Baja California.

> Articulo 175 bis.- A quien sin autorización o indebidamente, 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 multa equivalente de cien a trescientos días.
>
> Articulo 175 ter.- A quien sin autorización o indebidamente, copie o accese a 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 multa equivalente de cincuenta a ciento cincuenta días de salario mínimo vigente.

En este par de artículos se puede apreciar el hecho de introducirse sin autorización a equipos de informática que se encuentran protegidos traspasando barreras de seguridad y los altere.

Baja California Sur.

Código Penal para el Estado de Baja California Sur.

En este código no se encuentra nada al respecto sobre el tema que nos compete.

Coahuila.

Código Penal para el Estado de Coahuila.

Se encuentra regulado en libro segundo parte especial título segundo “delitos contra la seguridad publica” capítulo tercero “delitos contra la seguridad en los medios informáticos”. En los siguientes artículos:

> Artículo 281 Bis. Sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de particulares. Se aplicara prisión de tres meses a tres años y multa a quien:
>
> I. Sin autorización para acceder a un sistema informático y con perjuicio de otro, conozca, copie, imprima, use, revele, transmita, o se apodere de datos o información reservados, contenidos en el mismo.
> II. con autorización para acceder a un sistema informático y con perjuicio de otro, obtenga, sustraiga, divulgue o se apropie de datos o información reservados en el contenido.
>
> Si la conducta que en uno u otro caso se realiza es con el ánimo de alterar, dañar, borrar, destruir o de cualquier otra manera provocar la perdida de datos o información contenidos en el sistema, la sanción será de cuatro meses a cuatro años de prisión y multa.
>
> Artículo 281 bis 1. Circunstancias agravantes de los delitos anteriores. Las penas previstas en el artículo anterior, se incrementarán en una mitad más:
> I. Si el agente actuó con fines de lucro.
> II. Si el agente accedió al sistema informático valiéndose de información privilegiada que le fue confiada en razón de su empleo o cargo, o como responsable de su custodia, seguridad o mantenimiento.
>
> Artículo 281 bis 2. Sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de una entidad pública. Se aplicará prisión de seis meses a seis años y multa a quien:

I. Sin autorización, acceda, por cualquier medio a un sistema informático, de una entidad publica de las mencionadas en el párrafo segundo del articulo 194, para conocer, copiar, imprimir, usar, revelar, transmitir o apropiarse de sus datos o información propios o relacionados con la institución.
II. Con autorización para acceder al sistema informático de una entidad publica de las mencionadas en el párrafo segundo del articulo 194, indebidamente copie, transmita, imprima, obtenga sustraiga, utilice divulgue o se apropie de datos o información propios o relacionados con la institución.

Si la conducta que en uno u otro caso se realiza, tiene la intención dolosa de alterar, dañar, borrar, destruir, o de cualquier otra forma provocar la perdida de los datos o información contenidos en el sistema informático de la entidad pública, la sanción será de uno a ocho años de prisión y multa.

Si el sujeto activo del delito es servidor publico, se le sancionará, además, con la destitución del empleo, cargo o comisión e inhabilitación para ejercer otro hasta por seis años.

Artículo 281 bis 3. Circunstancias agravantes en los delitos anteriores. Las penas previstas en el artículo anterior se incrementarán en una mitad más:
I. Si el agente obro valiéndose de alguna de las circunstancias agravantes previstas en el artículo 290 bis 1.
II. Si el hecho constitutivo de delito fue cometido contra un dato o sistemas informáticos concernientes al régimen financiero de las entidades publicas que se mencionan en el artículo 194, o por funcionarios o empleados que estén a su servicio.
III. Si la conducta afecto un sistema o dato referente a la salud o seguridad publica o a la prestación de cualquier otro servicio publico.

Artículo 281 bis 4. Norma complementaria en orden a la terminología propia de los delitos contra la seguridad de los medios informáticos. A los fines del presente capítulo, se entiende por:
I. Sistema informático: todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos para

> generar, enviar, recibir, recuperar, procesar o almacenar información de cualquier forma o por cualquier medio.
> II. Dato informático o información: toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático.

Nos enmarca básicamente la seguridad sobre la que se encuentran protegidos ciertos mecanismos e información y la obtención de datos que podrían tener como finalidad el obtener un lucro, dando como resultado pérdidas para los dueños de esta información.

Colima.

Código Penal para el Estado de Colima.

En este Código se menciona conductas referentes a la pornografía lo cual es tomado por varios autores como una posibilidad de que esto se encuadre en lo que es la conducta del delito informático, sin embargo no se encuentra tipificado como tal.

Chiapas.

Código Penal para el Estado de Chiapas.

Se encuentra en el Libro Segundo Parte Especial Título Décimo Noveno “Delitos de Revelación de Secretos y de Acceso Ilícito a Sistemas y Equipos de Informática” Capítulo II “Acceso Ilícito a Sistemas de Informática”.

> Artículo 439. Al que sin autorización modifique, destruya, o provoque perdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo o sistema de seguridad o al que no tenga derecho a accesar, se le impondrá una sanción de uno a cuatro años de prisión y de cuarenta a doscientos días multa.

Al que, estando autorizado o tenga derecho de acceso a los sistemas o equipo de informática protegido por algún mecanismo o sistema de seguridad, innecesariamente o en perjuicio de otro destruya, modifique, o provoque pérdida de información que contengan los mismos, la pena prevista en el párrafo anterior, se aumentara en una mitad.

Articulo 440. Al que, sin autorización accese, modifique, copie, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública protegida por algún sistema o mecanismo de seguridad se le impondrá una sanción de dos a seis años de prisión y de doscientos a seiscientos días de multa.

Articulo 441. Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, innecesariamente o en perjuicio de otro o del servicio publico modifique, destruya o provoque perdida de información que contengan se impondrá prisión de tres a ocho años y de trescientos a ochocientos días multa.

Articulo 442. Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia publica, sin autorización copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y de cien a trescientos días multa.

Articulo 443. Los delitos previstos en este titulo serán sancionados por querella de parte ofendida.

De los artículos precedentes se puede apreciar el hecho de modificar, alterar o destruir a través de medios informáticos cierta información así como obtención de la misma cuando los mecanismos se encuentran protegidos por lo que causan una violación a los mismos.

Chihuahua.

Código Penal para el Estado de Chihuahua.

No existe regulación al respecto.

Distrito Federal.

No hay nada relativo a este tipo penal como tal en dicho Código, sin embargo menciona lo referente a la utilización de medios electrónicos para la obtención y falsificación de tarjetas de crédito.

LIBRO SEGUNDO PARTE ESPECIAL

TÍTULO VIGÉSIMO CUARTO DELITOS CONTRA LA FE PÚBLICA

CAPÍTULO I PRODUCCIÓN, IMPRESIÓN, ENAJENACIÓN, DISTRIBUCIÓN, ALTERACIÓN O FALSIFICACIÓN DE TÍTULOS AL PORTADOR, DOCUMENTOS DE CRÉDITO PÉBLICOS O VALES DE CANJE.

Artículo 336. Se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa al que, sin consentimiento de quien este facultado para ello:

I. Produzca, imprima, enajene, distribuya, altere o falsifique tarjetas, títulos o documentos utilizados para el pago de bienes y servicios o para disposición de efectivo;

II. Adquiera, utilice, posea o detente tarjetas, títulos o documentos para el pago de bienes y servicios, a sabiendas de que son alterados o falsificados;

III. Adquiera, utilice, posea o detente, tarjetas, títulos o documentos auténticos para el pago de bienes y servicios, sin consentimiento de quien este facultado para ello;

IV. Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios;

V. Acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo;

VI. Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma; o

VII. A quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente este facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios, o de los titulares de dichos instrumentos o documentos.
VIII. Produzca, imprima, enajene, distribuya, altere, o falsifique vales utilizados para canjear bienes y servicios.

Si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentaran en una mitad

En los Códigos Penales para los Estados de **Durango y Hidalgo.** No se encuentra regulado el tipo penal que se está analizando.

Guanajuato.

En el Código Penal para el Estado de Guanajuato menciona lo siguiente en su artículo:

Artículo 231.- Se aplicará de diez días a dos años de prisión y de diez a cuarenta días multa, a quien indebidamente:

I.- Abra, intercepte o retenga una comunicación que no le este dirigida.
II.- Accese, destruya o altere la comunicación o información contenida en equipos de cómputo o sus accesorios u otros análogos.
No se impondrá pena alguna a quienes ejerciendo la patria potestad o la tutela, ejecuten cualquiera de las conductas antes descritas, tratándose de sus hijos menores de edad o de quienes se hallen bajo su guarda.
Se requerirá querella de parte ofendida cuando se trate de ascendientes y descendientes, cónyuges o concubinos, parientes civiles o hermanos.

En este apartado refiere al acceso, alteración o destrucción de información.

Guerrero.

Artículo 165. Se impondrán las mismas penas previstas en el artículo 163 a quien:

I. Se apodere de una cosa propia, si esta se halla por cualquier titulo legitimo en poder de otro, y
II. Aprovechando energía eléctrica, algún fluido, programas computarizados, señales televisivas o de Internet, sin consentimiento de la persona que legalmente pueda disponer de aquellas.

Aquí solo se menciona aprovechamiento de programas computarizados sin establecer ninguna otra especificación.

Jalisco.

En el Código Penal para el Estado libre y soberano de Jalisco no se establece como tal pero maneja un aspecto relativo a obtención ilícita de información electrónica. Mencionando el tipo que se puede apreciar.

Libro segundo de los delitos en particular.
Título sexto Revelación de secretos y la obtención ilícita de información electrónica.

> Artículo 143 bis. Al que sin autorización y de manera dolosa, copie, modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días de multa.
>
> Las penas previstas en este artículo se incrementaran en una mitad cuando el sujeto pasivo del delito sea una entidad pública o institución que integre el sistema financiero.

Además hay un artículo en el cual se establece la hipótesis del delito de secuestro, sin embargo en este mismo artículo se menciona un punto referente al tema que nos compete.

Artículo 194. Comete el delito de secuestro quien prive ilegalmente de la libertad a otro con la finalidad de obtener rescate o de causar daño o perjuicio. Por rescate se entiende todo aquello que entrañe un provecho indebido y a cuya realización se condiciona la libertad del plagiado. Al responsable de este delito se le impondrá una pena de dieciocho a treinta y cinco años de prisión y multa por el importe de mil a dos mil días de salario mínimo.

…

k) Para lograr sus propósitos, se valga de redes o sistemas informáticos internacionales o de otros medios de alta tecnología, que impliquen marcada ventaja en el logro de su fin;

Estado de México.

No hay capítulo relativo al tema tratado, aún cuando las conductas que podrían encuadrar en el tipo que se estudia se podrían encontrar en el siguiente apartado.

CÓDIGO PENAL DEL ESTADO DE MÉXICO**.**

LIBRO SEGUNDO
TITULO PRIMERO DELITOS CONTRA EL ESTADO
SUBTITULO CUARTO DELITOS CONTRA LA FE PUBLICA
CAPITULO IV FALSIFICACION Y UTILIZACION INDEBIDA DE TITULOS AL PORTADOR, DOCUMENTOS DE CREDITO PUBLICO Y DOCUMENTOS RELATIVOS AL CREDITO

Artículo 174.- Se impondrán de cuatro a diez años de prisión y de ciento cincuenta a quinientos días de salario mínimo de multa al que:

I. Produzca, imprima, enajene aun gratuitamente, distribuya, altere o falsifique tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo, sin consentimiento de quien este facultado para ello;

II. Adquiera, utilice, posea o detente indebidamente, tarjetas, títulos o documentos para el pago de bienes y servicios, a sabiendas de que son alterados o falsificados;

III. Adquiera, utilice, posea o detente indebidamente, tarjetas, títulos o documentos auténticos para el pago de bienes y servicios, sin consentimiento de quien esté facultado para ello;

IV. Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios; y

V. Acceda indebidamente a los equipos de electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente este facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios.

Si el sujeto activo es empleado o dependiente del ofendido, las penas aumentarán en una mitad.

En el caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo se aplicaran las reglas del concurso.

El presente artículo se refiere al hecho de falsificar u obtener indebidamente tarjetas de crédito a través de la utilización de ciertos medios electromagnéticos, lo cual puede ser considerado como una de las hipótesis que bien podrían encuadrar en los delitos a que se hace referencia en el presente trabajo.

Además en los Estados de **Michoacán, Morelos y Nayarit** no se encuentran regulado ni se hace mención a este tipo de ilícitos.

Nuevo León.

Código Penal para el Estado de Nuevo León. Lo regula en su apartado siguiente:

Libro segundo

Parte especial

Título Vigésimo segundo de los delitos por medios electrónicos.

> Articulo 427.- A quien indebidamente accese a un sistema de tratamiento o de transmisión automatizado de datos, se le impondrá de 2 meses a 2 años de prisión y multa de 200 a 1000 cuotas.
>
> Artículo 428.- A quien indebidamente suprima o modifique datos contenidos en el sistema, o altere el funcionamiento del sistema de tratamiento o de transmisión automatizado de datos, se le impondrá de 2 a 8 años de prisión y multa de 300 a 1500 cuotas.
>
> Artículo 429.- A quien indebidamente afecte o falsee el funcionamiento de un sistema de tratamiento o de transmisión automatizada de datos, se les impondrá de 2 a 8 años de prisión y multa de 350 a 2000 cuotas.

Básicamente se refiere al acceso no autorizado a través de medios electrónicos causando una alteración a los mismos.

Oaxaca, Puebla, **Querétaro**, no tienen contemplado los ilícitos informáticos.

Quintana Roo

Código Penal del Estado de Quintana Roo.

> LIBRO SEGUNDO
>
> SECCION TERCERA DELITOS CONTRA LA SOCIEDAD
>
> TITULO TERCERO DELITOS CONTRA LA FE PÚBLICA

CAPITULO II FALSIFICACION DE DOCUMENTOS Y USO DE DOCUMENTOS FALSOS

Articulo 189 bis. Se impondrá hasta una mitad más de las penas previstas en el artículo anterior, al que:

I. Produzca, imprima, enajene, aún gratuitamente, distribuya o altere tarjetas, títulos, documentos o instrumentos utilizados para el pago de bienes y servicios o para disposición en efectivo, sin consentimiento de quien esté facultado para ello.
II. Adquiera, posea o detente ilícitamente tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo a sabiendas de que son alterados o falsificados.
III. Copie o reproduzca, altere los medios de identificación electrónica, cintas o dispositivos magnéticos de documentos para el pago de bienes o servicios o para disposición en efectivo.
IV. Accese indebidamente los equipos y sistemas de computo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes o servicios o para disposición de efectivo.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente este facultada para emitir tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición en efectivo.

Si el sujeto activo es empleado o dependiente del ofendido, las penas aumentarán hasta una mitad más.

En el caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo se aplicarán las reglas del concurso

En este artículo se refiere a la alteración de tarjetas de crédito así como el acceso liso y llano a los sistemas computarizados.

San Luis Potosí, no tiene contemplado los ilícitos informáticos.

Sinaloa.

Es el pionero en legislar al respecto ya que en 1992, el congreso local del estado de Sinaloa legisló por vez primera sobre estos en México, contemplándolos como uno de los delitos de patrimonio, siendo este el bien jurídico tutelado.

Código Penal para el Estado de Sinaloa.
Libro segundo
Parte especial
Sección primera delitos contra el individuo 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 computadores 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.

En el Código Adjetivo de la materia Penal para el Estado de Sinaloa se encuentra regulado de manera clara cuales son los delitos informáticos, así como las sanciones a que se harán acreedores los que cometan el tipo de conductas de las aquí enunciadas.

Es uno de los pocos Códigos que lo establecen de forma clara encuadran el tipo manejándolo como un daño patrimonial.

Sonora. No hay regulación sobre el aspecto del cual tratamos en este Código.

Tabasco.
Código penal del estado de tabasco.

Libro segundo parte especial.
Título Decimoprimero Delitos contra la seguridad de la comunicación. Capítulo V. Violación de la comunicación privada.

> Articulo 316. Al que intervenga la comunicación privada de terceras personas, a través de medios eléctricos o electrónicos, se le aplicara prisión de uno a cinco años.

Este artículo hace referencia básicamente a una violación a la intimidad utilizando los sistemas electrónicos como un medio vulnerando con ello la intimidad del individuo.

Por otro lado también se encuentra este “tipo penal” en el siguiente título:

Título Decimotercero bis delitos contra la seguridad en los medios informáticos y magnéticos.

> Artículo 326 bis. Al que intercepte, interfiera, reciba, use o ingrese por cualquier medio sin la autorización debida o, excediendo la que tenga, a una computadora personal, o a un sistema de red de computadoras, un so9porte lógico de programas de computo o base datos, se le impondrán de seis meses a dos años de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 326 bis 1. a quien se autorización modifique, destruya o deteriore en forma parcial o total, archivos, bases de datos o cualquier otro elemento intangible contenido en computadoras personales, sistemas de redes de computo, soporte lógicos, o cualquier otro medio magnético, se le sancionara con penas de dos a ocho años de prisión y de cuatrocientos a mil doscientos días multa.

Cuando el activo tenga el carácter de encargado del manejo, administración o mantenimiento de los bienes informáticos dañados, las penas se incrementaran en una mitad más.

Articulo 326 bis 2. Se impondrán penas de dos a seis años de prisión y de cuatrocientos a mil días multa, al que copie o imite los originales de cualquier dato, archivo o elemento intangible contenido en una computadora personal o en un sistema de redes de computadoras, base de datos, soporte lógico, siempre que para ello se requiera autorización y no la obtenga.

Las mismas sanciones se aplicaran al que utilice o aproveche en cualquier forma, los bienes informáticos falsificados, previstos en este titulo

Articulo 326 bis 3. Cuando los ilícitos previstos en este titulo se cometan utilizando el equipo de computo de terceras personas, las penas se incrementaran en una mitad.

Tamaulipas.

Se encuentra regulado en el Código penal para el estado de Tamaulipas.

Libro segundo parte especial
Titulo séptimo delitos de revelación de secretos y de acceso ilícito a sistemas y equipos de informática.

Se encuentra en el Capítulo I denominado “Revelación de Secretos”, en los artículos siguientes:

Artículo 206. Al responsable del delito de revelación de secretos se le impondrá una sanción de un año a tres años seis meses de prisión y multa de veinte a sesenta días salario.

Artículo 207. Cuando la revelación punible sea hecha por personas que presten servicios profesionales o técnicos, o cuando el secreto revelado o publicado sea de carácter industrial, la sanción será de dos a cinco años de prisión y multa de treinta a ochenta días salario.

Artículo 207 bis. Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo de seguridad o que no tenga derecho de acceso a él, se le impondrá una sanción de uno a cuatro años de prisión y multa de cuarenta a ochenta días salario.

Artículo 207-ter. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a seis años de prisión y multa de doscientos a seiscientos días salario.

Artículo 207-ter. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a seis años de prisión y multa de doscientos a seiscientos días salario.

Articulo 207-quater. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a cinco años de prisión y multa de cien a trescientos días salario.

Artículo 207-quinquies. Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente modifique, destruye o provoque pérdida de información que contengan se impondrá una

sanción de tres a ocho años de prisión y multa de trescientos a ochocientos días salario.

Articulo 207-sexies. Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y multa de cien a trescientos días salario.

Los delitos previstos en este título serán sancionados por querella de la parte ofendida.

Artículo 208. Para los efectos de este título y el subsecuente se considera servidor público toda persona que desempeñe un empleo, cargo o comisión de cualquier naturaleza para:

I. Los tres poderes del Estado;
II. Los ayuntamientos de los municipios del estado;
III. Los organismos descentralizados de las entidades referidas en las dos fracciones que anteceden.

Se impondrán las mismas sanciones previstas para el delito de que se trate a cualquier persona que participe en la perpetración de alguno de los delitos previstos en este título o el subsecuente.

Otro artículo en el cual se hace referencia al uso indebido de los sistemas de cómputo es el siguiente:

Libro segundo parte especial
Título décimo noveno delitos contra el patrimonio de las personas
Capítulo I Robo

Articulo 400. Se sancionará con la pena del robo:
…

IV. El apoderamiento material de los documentos que contengan datos de computadoras o el aprovechamiento o utilización de dichos datos, sin consentimiento de la persona que legalmente pueda disponer de los mismos.

En la fracción anterior se denota como robo la conducta de aprovechamiento de sistemas computarizados, es decir, lo engloba en otra conducta ya existente como una hipótesis y no como otro tipo de delito.

Tlaxcala.

En CODIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE TLAXCALA. No se encuentra regulación alguna al respecto.

Veracruz.

En el código penal para el estado libre y soberano de Veracruz se encuentra en el libro segundo.

TÍTULO IV DELITOS CONTRA LA INTIMIDAD PERSONAL Y LA INVIOLABILIDAD DEL SECRETO.

En su capítulo III. Delitos Informáticos.

Artículo 181.-Comete delito informático quien, sin derecho y con perjuicio de tercero:

I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; o

II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red.

Al responsable de este delito se le impondrán de seis meses a dos años de prisión y multa hasta de trescientos días de salario. Si se cometiere con fines de lucro las penas se incrementaran en una mitad.

Básicamente el delito informático es el introducirse a través de un medio informático a una información que se encuentre por estos medios de una forma ilícita es decir, sin autorización y realice una serie de actividades que van desde la simple intromisión a datos como la modificación o destrucción de los mismos.

Yucatán.

Hace mención a la utilización de los sistemas de cómputo como un medio para la transmisión de la pornografía infantil.

> TÍTULO SEPTIMO DELITOS CONTRA LA MORAL PÚBLICA
> CAPITULO II CORRUPCION DE MENORES E INCAPACES, TRATA DE MENORES Y PORNOGRAFIA INFANTIL
> Artículo 211. Al que procure o facilite por cualquier medio que uno o mas menores de dieciocho años, con o sin su consentimiento, los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de cuatrocientos a quinientos días-multa.
>
> Al que fije, grabe o imprima actos de exhibicionismo corporal, lascivos o sexuales en que participen uno o mas menores de dieciocho años, se le impondrá la pena de diez a catorce años de prisión y de cuatrocientos a quinientos días-multa. La misma pena se impondrá a quien con fines de lucro o sin el, elabore, reproduzca, venda, arriende, exponga, publicite o transmita el material a que se refieren las acciones anteriores…

Zacatecas.

En el Código Penal para el Estado de Zacatecas no se encuentra regulado lo referente a los delitos informáticos.

De acuerdo a lo observado en los Códigos Penales de los Estados analizados con anterioridad se puede apreciar una serie de formas de tipificar dicha conducta así como los bienes jurídicos tutelados o protegidos por los mismos.

En los Códigos penales de Aguascalientes y Tabasco establecen dichas figuras entre los delitos contra la seguridad en los medios informáticos y magnéticos.

Baja California los establece en los delitos contra la inviolabilidad del secreto; Chiapas en los delitos en contra de las personas en su patrimonio; Colima, Puebla, Querétaro, Zacatecas y Morelos los localizan dentro los delitos contra la moral pública, contra la libertad y la violación de otras garantías y Tamaulipas en los delitos de revelación de secretos y de acceso ilícito a sistemas y equipos de informática.

Por lo anterior es de concluirse que no todos cuentan con estas conductas tipificadas, aún cuando deberían estarlo en virtud de que este tipo de ilícitos se encuentran cada vez con mayor frecuencia.

1.2 Ley Federal de los Derechos de Autor.

"Se define al derecho de autor como el derecho que la ley reconoce al autor de una obra para participar en los beneficios que reproduzcan la publicación, ejecución o representación de la misma".[75]

Por lo cual, es bastante entendible el hecho de que este tipo de delitos formen parte de los "delitos informáticos", ya que muchas veces estamos ante la presencia de bienes intangibles y es necesario que cuenten con una protección.

[75] Viñamata Paschkes Carlos, "La propiedad intelectual", Editorial Trillas, México, 1998, p.27

Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la ley Federal de Derechos de Autor del 24 de Diciembre de 1996, que entro en vigor el 24 de marzo de 1997, por lo que de lo anterior se puede desprender que entra en los ilícitos que se abordan debido a que esta ley menciona programas computacionales que son básicos y necesarios para quienes cometer un ilícito o realizar algún tipo de conducta que lesiones un bien jurídicamente tutelado.

Resulta difícil el establecer una relación entre los delitos informáticos y la propiedad intelectual, es claro que se pueden cometer violaciones a la propiedad cuando se comete uno de estos delitos, sin embargo en el mundo fáctico resulta difícil observar el alcance y la validez que pueden tener algunas normas.

"En materia de derechos de autor el principio fundamental consiste en que la ley reconoce a favor del autor, es decir del titular del derecho, la potestad de impedir la reproducción o explotación de la obra sin autorización".[76]

Esta se dio con el objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión.

Existe una gran diversidad de conductas que se podrían encuadrar en el tipo que se aborda en el presente trabajo, referentes a bienes tutelados en La Ley Federal de Derechos de Autor, como son las patentes, marcas, programas, etc., los cuales pueden ser utilizados en las redes burlando a sus autores intelectuales.

[76] Jalife Daher Mauricio, "Uso y valor de la propiedad intelectual", Editorial Gasca Sicco, 2004, p.51

2. Países que contemplan en su legislación los delitos informáticos.

Los delitos informáticos son contemplados en las legislaciones de diversos países, algunos en sus códigos penales, y algunos otros están regulados por leyes especiales.

2.1 Alemania.

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

- Espionaje de datos.
- Estafa informática.
- Alteración de datos. En el cual se comprende cancelar, inutilizar o alterar datos.
- Sabotaje informático. Entendiendo la destrucción, alteración, deterioro o inutilización de sistemas de datos.
- Utilización abusiva de cheques o tarjetas de crédito.
- Falsificación de datos probatorios. Tanto ideológica como de documentos.

Un dato importante de mencionar es que el gobierno alemán pretendía limitar el acceso a ciertos sitios, solicitando fueran bloqueados desde su origen; pero eso atentaría contra la libertad de expresión.

2.2 Austria.

La **Ley de reforma del Código Penal**, del 22 de diciembre de 1987, en el artículo 148, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla

sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

Por otro lado en su artículo 126 contempla la destrucción de datos incluyendo además de los personales a los programas.

2.3 Chile.

Chile fue el primer país latinoamericano en sancionar una **Ley contra delitos informáticos**, la cual entró en vigencia el 7 de junio de 1993.

En la ley Nº 19.223 se estableció que la destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

La presente ley tiene como finalidad proteger a un nuevo bien jurídico como es: "*la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan*".[77]

Esta ley prevé cuatro artículos al respecto de los delitos informáticos. En el Artículo 1º, se describe el tipo legal vigente, en el cual se establece que es una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.

Artículo 2. El que con el ánimo de apoderarse usar o conocer algún tipo de información lo intercepte, interfiera o acceda a esta información.

[77] Acurio del Pino Santiago, página http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf , 13/09/08

En tanto, el Art. 3º tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información y el artículo 4° el que revele o difunda de forma maliciosa datos contenidos en un sistema de información.

Asimismo, se establece la pena a la que se harán acreedores los responsables de estos ilícitos informáticos, además si el que incurre en estas conductas es responsable de los sistemas de información que son vulnerados la pena aumentará.

No hace mención del delito de copia ilegal de programas, ya que este se encuentra en la ley 17336 sobre propiedad intelectual.

2.4 Estados Unidos.

Este país adoptó en 1994 del **Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030)** que modificó al **Acta de Fraude y Abuso Computacional de 1986.**

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un caballo de Troya y en qué difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. Definiendo dos niveles para el tratamiento de quienes crean virus:

a. Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.
b. Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

La nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

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

En Julio de 2000, el Senado y la Cámara de Representantes de Estados Unidos 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 en los que se encuentran los mensajes electrónicos y contratos establecidos mediante Internet- entre empresas y entre estas y los consumidores.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad.

Se realizaron enmiendas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos que son más propicios de verse afectados por estos delitos, además se crearon sanciones

pecuniarias de $10, 000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos.

El objetivo era la protección a la intimidad y a la base de datos que se encuentra en sistemas computarizados.

En uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos de forma enumerativa y no limitativa comúnmente los llamados virus o gusanos los cuales son instrucciones designadas a contaminar grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

La mayoría de los Estados han tipificado los delitos informáticos algunos ejemplos son: Arizona Computer Crimes Law, Iowa Computer Crime Law y Kansas Computer Crime Law.

En el *United States Code* o Código de los Estados Unidos el cual es una recopilación de legislación federal vigente tipifica una serie de delitos que afectan los sistemas de computación del gobierno federal y a quienes necesitan utilizar computadoras localizadas en más de un Estado.

Entre los principales delitos tipificados se encuentran:

- ✓ Hacking seguido de descubrimiento de información protegida por razones de seguridad nacional o relaciones con el extranjero o información de circulación restringida por la ley.
- ✓ Hacking con el objeto de hacerse de un archivo financiero o de un usuario de tarjeta.
- ✓ Hacking con objeto de obtener información de un departamento o agencia del Estado estadounidense.

- ✓ Hacking con el objeto de obtener información protegida por una entidad financiera.
- ✓ Hacking con intención de fraude.
- ✓ Transmisión dolosa de un programa, información, código o comando que cause un daño indebido a una computadora protegida.
- ✓ Acceso ilegítimo a una computadora que negligentemente cause un daño.
- ✓ Acceso a una computadora protegida que cause objetivamente un daño.
- ✓ Venta, transferencia, disposición u obtención de control con la intención de defraudar.
- ✓ Transmisión con la intensión de una extorsión.

El Estado de Nueva Cork modifica su ley penal sobre fraude informático y entra en vigor el 1 de noviembre de 1993.[78] Con la cual impone penas de acuerdo al valor del daño causado.

2.5 España.

En el ***Nuevo Código Penal de España***, aprobado por la Ley Orgánica 10/1995, de 23 de Noviembre y publicado en el BOE número 281, de 24 de Noviembre de 1995. En esta ley el art. 263 establece lo referente a daños en propiedad ajena, en donde también se podrían catalogar los delitos informáticos. En tanto, el artículo 264-2) establece que 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 delictual (Violación de secretos/Espionaje/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.

[78] B. Bierce Willian, *"*El delito de violencia tecnológica en la legislación de Nueva York*",* *Derecho de la Alta Tecnología*, Año VI, Número 66, Febrero, 1994, p.20.

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.

También se reconoce el Fraude Informático, consistente en la manipulación informática o artificio con ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

En el delito de daños se contemplan los supuestos de destrucción, alteración, inutilización, o cualquier otra modalidad por la que se dañen los datos, programas o documentos electrónicos contenidos en redes, soportes, o sistemas informáticos. Lo anterior en virtud a la importancia que puede tene los datos contenidos de manera digital tanto de personas físicas como de personas morales.

El artículo 211 establece que los delitos de calumnia e injuria se reputarán hechos con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante. Por lo que se incluyen en este tipo de mensajes los que se manejan a través de la web en www.

El artículo 212 establece la responsabilidad solidaria del propietario del medio informativo a través del que se haya propagado la calumnia o injuria. En el caso de Internet, la responsabilidad civil solidaria alcanzaría al propietario del servidor en el que se publicó la información constitutiva de delito, aunque debería tenerse en cuenta, en este caso, sí existió la posibilidad de conocer dicha situación, ya que por lo general es mucha la información contenida en este medio y en ocasiones es difícil revisarla toda, además de que no se puede controlar la información recibida en los sitios del Internet.

El artículo 400 introduce el delito consistente en la fabricación o tenencia de útiles, materiales, instrumentos, programas de ordenador o aparatos destinados específicamente a la comisión de estos delitos.

El artículo 278 establece el delito mediante el cual con el fin de descubrir un secreto, se apoderase por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo.

El artículo 239 considera llaves falsas las tarjetas magnéticas o perforadas así como los mandos o instrumentos de apertura a distancia, considerando por lo tanto delito de robo la utilización de estos elementos, el descubrimiento de claves y la inutilización de sistemas específicos de alarma o guarda con el fin de apoderarse de cosas muebles ajenas.

En el Código Penal español de 1995 se pueden encontrar las siguientes conductas:[79]

- ✓ Ataques que se producen contra el derecho a la intimidad, estos es, descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados en ficheros o soportes informáticos.
- ✓ Infracciones a la propiedad intelectual a través de la protección a los derechos de autor encontrándose en este la copia y distribución no autorizada de programas, así como copia ilegal de los mismos.
- ✓ Falsedades. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad.
- ✓ Sabotajes informáticos. Ya mencionado con anterioridad como daño en propiedad ajena y radica principalmente en daño mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos.

[79] Nava Garcés Alberto Enrique, “Análisis de los delitos Informáticos”, Editorial Porrúa, México, 2005.

- ✓ Fraudes informáticos. Con la manipulación de datos o programas para la obtención de lucro de manera ilícita.
- ✓ Amenaza. Esta puede llevarse a cabo mediante cualquier medio de información.
- ✓ Calumnia e injurias. Cuando se propaguen por cualquier medio semejante a la imprenta o radiodifusión.
- ✓ Pornografía infantil. En esta conducta desde su producción hasta su venta, distribución y exhibición por cualquier medio de este tipode material.

2.6 Francia.

En enero de 1988, este país dictó la ley número 88-19 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.

De lo analizado en los países anteriores se puede apreciar que varios de ellos tienen regulación muy expresa en una diversidad de leyes que tipifican los llamados delitos informáticos, con los cuales se les da una vigencia y se establecen en el derecho positivo de cada una de sus legislaciones.

Es de recalcar que estos ilícitos día con día toman una gran relevancia por lo cual es necesario ir haciendo reformas o agregando las conductas que pueden configurarlos.

Además se pueden dar tipos comunes que utilicen como medio o herramienta la computadora, redes y otros mecanismos que los haga ya no encuadrar en los tipos que se encuentran establecidos.

CAPÍTULO IV. DELITOS INFORMÁTICOS: NECESIDAD DE UNA REFORMA A NIVEL NACIONAL E INTERNACIONAL.

En este capítulo se observará la necesidad de establecer una regulación tanto en el ámbito nacional como internacional debido al auge que esta tomando la tecnología y por consiguiente el crecimiento en número de los delitos informáticos.

Lo anterior debido a que se ha perdido una gran cantidad de dinero debido a los ilícitos de este tipo que se cometen a lo largo del globo.

Se establecerán las principales diferencias entre la legislación mexicana y algunos países de derecho comparado.

La necesidad imperante de crear no sólo regulación nacional sino internacional, así como organismos e instituciones que tengan la capacidad técnica, jurídica y económica para perseguir y castigar estos ilícitos que dejan grandes pérdidas.

1. Sus semejanzas y diferencias: México y países que los regulan.

El establecer un comparativo es de importancia significativa ya que con esto se puede tener una idea más clara de lo que son este tipo de delitos, para así establecer en qué se parecen al de nuestro sistema o la posibilidad de modificar nuestra legislación de una manera eficiente, para cubrir las necesidades.

A continuación se señalará de manera clara lo más importante y trascendente en diferencias y similitudes en cuanto delitos informáticos en relación a México y otros países.

Estos cuadros son elaborados tomando como referencia los Códigos Penales Federales de los países que se analizan o la ley especial que ha regulado los

delitos informáticos, no así enfocándose en los diversos Códigos que pudieran encontrarse en los diversos Estados de cada país analizado.

México	Alemania
Semejanzas	
1. Se encuentra regulado el aspecto de alteración de datos o acceso ilícito a sistemas y equipos de informática con el fin de destruir, copiar o modificar la información existente en los sistemas informáticos.	1. Se regula en su ley lo relativo a la alteración de datos y el sabotaje informático.
Diferencias	
1. No se ha mencionado en la ley lo referente a la utilización de falsificación de datos en relación a los medios probatorios dentro de un proceso.	1. Se ha regulado la falsificación de datos probatorios.

México	Austria
Semejanzas	
1. Se encuentra regulado el aspecto de alteración de datos o acceso ilícito a sistemas y equipos de informática con el fin de destruir, copiar o modificar la información existente en los sistemas informáticos.	1. Menciona lo referente a la introducción, cancelación o alteración de datos o por actuar en el curso de procesamiento de datos.
Diferencias	
1. En el caso de México sólo son penas especiales cuando se trata de personas que trabajan en	1. Tiene sanciones especiales para quienes cometen ilícitos utilizando las computadoras o alteran, cancelan o

instituciones financieras y manejan información relativa a estos estados financieros, así como trabajadores del Estado.	introducen datos, cuando utilizan su profesión de especialistas en sistemas.

México	**Chile**
Semejanzas	
1. Se encuentra regulado el aspecto de alteración de datos o acceso ilícito a sistemas y equipos de informática con el fin de destruir, copiar o modificar la información existente en los sistemas informáticos. 2. Además se castiga con una pena extra a quienes del Estado o de los Sistemas Financieros accedan a esta información para alterarla o causarle algún daño.	1. Destrucción o inhabilitación de un sistema ó que la conducta impida, obstaculice o modifique su funcionamiento. Además el que intercepte o interfiera en una información. 2. También menciona el hecho de que si quien incurre en estas conductas son personas responsables de esa información se aumentará la pena. Aún cuando esta no es limitativa en cuanto a que tipo de información se refiere.
Diferencias	
1. En esta se menciona la copia ilegal de programas.	1. No se menciona en su ley especial la copia ilegal de programas. Esta se encuentra en la ley sobre propiedad intelectual.

México	Estados Unidos
Semejanzas	
1. Se encuentra regulado el aspecto de alteración de datos o acceso ilícito a sistemas y equipos de informática con el fin de destruir, copiar o modificar la información existente en los sistemas informáticos. 2. Además se castiga con una pena extra a quienes del Estado o de los Sistemas Financieros accedan a esta información para alterarla o causarle algún daño.	1. En sentido amplio no se establece de forma clara la forma en que puede ser vulnerada la información existente en los sistemas informáticos, lo que menciona es en sí la protección a las bases de datos, para que pueda ser de una forma amplia. 2. Habla del hacking con el objeto de hacerse de un archivo financiero.
Diferencias	
1. No se hace mención específica a los virus. 2. No hace mención específica de la pena que se impondrá por la forma dolosa o culposa de cometerla. 3. No hace mención específica a firmas electrónicas, en nuestra legislación, más bien este punto se encuentra regulado en la cuestión relativa a pruebas.	1. En esta ley se contemplan de manera clara y específica lo referente a los actos de transmisión de virus. 2. Establece una pena diferente para quien comete un delito de manera intencional y otro para quien lo comete de manera imprudencial. 3. Hay una regulación específica en lo relativo firmas Electrónicas (Acta de Firmas electrónicas en el Comercio Global y Nacional).

4. La sanción que se establece únicamente es la relativa a la pena de prisión, sin contemplar otro tipo de penas.	4. Se crean inclusive sanciones pecuniarias para quienes cometen ilícitos en la materia a la que hacemos referencia.

México	**España**
Semejanzas	
1. Se encuentra regulado el aspecto de alteración de datos o acceso ilícito a sistemas y equipos de informática con el fin de destruir, copiar o modificar la información existente en los sistemas informáticos.	1. Se encuentra regulado en el aspecto de daño en propiedad ajena a quien por cualquier medio destruye, altere, inutilice o de cualquier otro modo dañe los datos, programas y documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.
2. Se hace mención de pena especial para quienes trabajan para el Estado.	2. Se hace mención de una pena especial para quienes son funcionarios públicos y cometen este tipo de ilícitos.
Diferencias	
1. Se hace mención especial para quienes cometen ilícitos en materia informática cuando laboran para instituciones financieras.	1. No se hace mención especial para quienes cometen delitos en materia informática cuando trabajan para instituciones financieras.
2. Se encuentra regulado en un solo capítulo del Código Penal Federal en el apartado de acceso ilícito a	2. Se encuentran regulados en diversos apartados de su Código Penal, en lo referente a fraude

sistemas y equipos de informática, además de algunas legislaciones estatales en donde se contemplan como tal “delitos informáticos”.	informático, delito de daños, calumnia e injurias, ataques contra la intimidad y protección intelectual entre otras.

México	**Francia**
Semejanzas	
1. Se encuentra regulado el aspecto de alteración de datos o acceso ilícito a sistemas y equipos de informática con el fin de destruir, copiar o modificar la información existente en los sistemas informáticos.	1. Menciona en su ley relativa lo referente a alteración del funcionamiento de un sistema operativo, así como supresión y modificación de datos en un sistema o en la forma de procesamiento del mismo.
Diferencias	
1. No hace ninguna diferencia entre el aspecto doloso y culposo.	1. Establece un tipo doloso y uno culposo.

De los países que estudiamos con anterioridad se podrían tomar ciertas conductas que son importantes y que se podrían tipificar ya sea creando una lista de los posibles delitos o los ya existentes teniendo como utilización los sistemas computacionales.

Así como el hecho de que se incrementará o fuera una sanción especial para personas que tengan como profesión la especialidad en sistemas. Aunado a esto, el tratamiento especial que se la da a ciertas conductas como lo es lo referente a

los virus que cada día están más en auge, así como un capítulo denominado como tal, en donde también se encuentren lo relativo a sanciones tal vez un poco más severas y congruentes al tipo de acceso y daño causado.

Sería preciso el hecho no sólo de establecer conductas limitativamente, sino que existe la posibilidad de que otros tipos de delitos ya existentes se puedan cometer con uso de cualquier computadora y por tanto encuadren este tipo.

2. Insuficiencia de la legislación en México en esta materia.

Para que exista el cuerpo del delito debe encuadrarse y contar con el tipo correspondiente.

"El cuerpo del delito es la actualización en el mundo fáctico de la conducta descrita en la ley penal como prohibida, considerando":[80]

a) Sólo sus elementos materiales u objetivos.
b) Los normativos.
c) Los dos anteriores y además los subjetivos específicos.

Es decir, el tipo penal es la descripción de una conducta a la cual el legislador asocia la punibilidad. Además de tener un tipo penal debe haber calidad de sujeto activo, sujeto pasivo, objeto material, resultado material, medios utilizados, circunstancias de tiempo, lugar, modo y ocasión.

Por lo tanto es difícil la comprobación del cuerpo del delito. Siempre que se sostenga la conducta es típica, también se estará afirmando que esta comprobando el cuerpo del delito respectivo, aún cuando la acreditación de este

[80] Sosa Ortiz Alejandro, "El cuerpo del delito. La problemática en su acreditación", primera edición, Editorial Porrúa, México, 2003.

no siempre implique que la conducta sea típica, porque puede estar demostrado y no actualizarse.

Otro punto sería establecer la responsabilidad que se da en este tipo delitos, tendría que tomarse en cuanta el grado de afectación que provocan.

Es decir, establecer de manera clara la conducta para que pueda recaer en el tipo penal específico y así reunir los requisitos previstos para que se considere de esta forma.

Una vez que se enlisten los tipos, se establecerían los elementos que acredite la responsabilidad y por ende la sanción.

3. Regulación jurídica y medidas que se contemplan a nivel internacional.

La Organización de las Naciones Unidas estableció una clasificación sobre los delitos informáticos: se tipificaron tres tipos de delitos:

1. Fraudes. Estos derivados de la manipulación de las computadoras o de datos informáticos.
2. Falsificaciones informáticas. Esto es, alteración de datos o documentos almacenados en un sistema que se encuentra computarizado.
3. Daños o modificaciones de programas o datos computarizados. Consistentes en modificar, suprimir, etc. Datos con el fin de que se obstaculice o altere un buen funcionamiento.[81]

[81] Simon Hocsman Heriberto, “Negocios en Internet”, Editorial Astrea, Buenos aires, 2005, p.258-259.

El Consejo de Europa realizo una convención de ciberdelitos, estableció un convenio preliminar en una reunión llevada a cabo el 25 de mayo de 2001, realizada en Estrasburgo.

En Noviembre de 2001 en Budapest se llevó a cabo por el consejo de Europa la Convención de ciberdelitos. La cual tiene dos objetivos:

1. La introducción de conductas tipificadas con términos similares.
2. La coordinación y cooperación entre policías y administradores de los países que se adhieran a ella.[82]

En este texto en su capítulo II se establecen las medidas que se deben tomar para castigar estos delitos. El convenio contempla normas tanto de derecho material como de derecho procesal.

Clasifica los delitos informáticos de la siguiente forma:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos. En los de confidencialidad siempre que estos se realicen de manera dolosa, sin permiso del titular; integridad es decir que no haya una intercepción de algún dato privado o de sistemas; disponibilidad lo referente a su producción, venta y distribución.
2. Delitos relacionados con el uso de computadoras. Delitos ya conocidos pero haciendo uso de las computadoras y sus sistemas como lo son: la falsificación y el fraude.
3. Delitos relacionados con los contenidos. Contenidos ilícitos como lo es la pornografía.
4. Delitos relacionados con la violación de los derechos de autor y derecho afines. Cuando se cometen actos con carácter comercial y por medio de sistemas informáticos.

[82] *Ibid* p.259.

Asimismo establecen una serie de medidas procesales contra este tipo de ilícitos:

a) La pronta preservación de los datos informáticos almacenados.
b) Orden de suministrar datos informáticos.
c) Allanamiento del lugar donde se encuentren y secuestro de datos informáticos almacenados.
d) Recopilación de datos informáticos en tiempo real.
e) Intercepción de datos de contenidos.

a) La pronta preservación de los datos informáticos almacenados. Estableciéndose que cada país de acuerdo a su autoridad competente ordene u obtenga la preservación de datos informáticos que se crea que se pueden perder o modificar. También pudiéndose obligar a una persona que cuente con acceso a esta información para que la conserve y preserve dentro de 90 días pudiendo ser renovable dicho permiso y podría ser o no de acuerdo a como se decida un procedimiento confidencial.

b) Orden de suministrar datos informáticos. En este se permite ordenar a una persona que se encuentre dentro del territorio del país, suministrar datos informáticos específicos que dicha persona posea o controle, u ordenar a un proveedor que ofrezca servicios informáticos, estableciendo tipo, técnicas, servicio, identidad o cualquier información con la instalación de equipos de comunicaciones.

c) Allanamiento del lugar donde se encuentren y secuestro de datos informáticos almacenados. Cada parte puede allanarse y secuestrar el sistema informático o medio de almacenamiento, obtener una copia, impedir el acceso o eliminar datos.

En el inciso d) Recopilación de datos informáticos en tiempo real. Esto asociado con comunicaciones transmitidas dentro de un territorio.

e) Intercepción de datos de contenidos. Facultar a las autoridades competentes para recopilar o registra por medios técnicos, dentro de su territorio los datos de contenidos de comunicaciones específicas efectuadas en su territorio por un medio informático así como a los proveedores.

En la Convención en el tema de **jurisdicción** para no entrar en conflicto adopta los principios de territorialidad y nacionalidad para atribuir la jurisdicción en estos delitos. Si más de un Estado reclama la jurisdicción sobre el asunto las partes deben efectuar consultas para determinar la más apropiada para llevar acabo el procedimiento penal tratando de armonizar los dos principios adoptados.

También dispone un capítulo sobre cooperación internacional, extradición y asistencia mutua.

Se ha planteado la creación de un programa de gobierno digital el cual es un proyecto de políticas públicas en el cual se imagina escenarios, se programan acciones y se actúan relaciones eficientes dentro de la administración y con relación a los ciudadanos y a las empresas.[83]

Creación de cibertribunales. Su propósito es servir de mediadores en los litigios derivados del uso del Internet. Estos permiten a las partes elegir de entre diversos expertos, aquellos que propondrán soluciones a los conflictos, sustentados en los textos internacionales más avanzados en la materia.[84]

Experiencias de ciberjusticia:

[83] Téllez Valdés Julio, *op.cit.*, p.46.
[84] *Ibid*, p.47

Virtual Magistrate. Se inauguró en 1996, es un servivio de arbitraje en línea resultante de la colaboración entre el Cyberspace law Institute (CLI) y el *Nacional Center for automated Information Research* (NCAIR) . Su objetivo era resolver las controversias que se dieran entre los usuarios y los operadores de la red.

Este procedimiento de arbitraje era voluntario y se efectuaba por correo electrónico. El proyecto se sigue en la Universidad de Chicago-Kent.

On-line Ombuds Office (Oficina de mediadores en línea). Es una iniciativa del Center for Information Technology and Dispute Resolution de la Universidad de Massachussets. Se da desde 1996 ofrece servicios de mediación para determinados conflictos que se generan en Internet.

Caber Tribunal. Era un proyecto experimental elaborado por el *Center Recherche en Droit Publique* (CRDP) de la Universidad de Montreal, en 1996.Este proyecto determinaba si era viable utilizar mecanismos alternativos para resolver conflictos generados en entornos electrónicos.

Otro ejemplo de medidas que se han contemplado en el campo internacional es el dado en Singapur quien enmendó su Ley sobre el Uso Indebido de las Computadoras. Son más severos los castigos impuestos a todo el que interfiera con las "computadoras protegidas" --es decir, las que están conectadas con la seguridad nacional, la banca, las finanzas y los servicios públicos y de urgencia-- así como a los transgresores por entrada, modificación, uso o intercepción de material computadorizado sin autorización.

En el Manual de las Naciones Unidas de 1977 se insta a los Estados a que coordinen sus leyes y cooperen en la solución de ese problema. El Grupo de Trabajo Europeo sobre delitos en la tecnología de la informática ha publicado un Manual sobre el delito por computadora, en el que se enumeran las leyes

pertinentes en los diversos países y se exponen técnicas de investigación, al igual que las formas de buscar y guardar el material electrónico en condiciones de seguridad.

El Instituto Europeo de Investigación Antivirus colabora con las universidades, la industria y los medios de comunicación y con expertos técnicos en seguridad y asesores jurídicos de los gobiernos, agentes del orden y organizaciones encargadas de proteger la intimidad a fin de combatir los virus de las computadoras o "caballos de Troya". También se ocupa de luchar contra el fraude electrónico y la explotación de datos personales.

En 1997, los países del Grupo de los Ocho aprobaron una estrategia innovadora en la guerra contra el delito de "tecnología de punta". El Grupo acordó que establecería modos de determinar rápidamente la proveniencia de los ataques por computadora e identificar a los piratas, usar enlaces por vídeo para entrevistar a los testigos a través de las fronteras y ayudarse mutuamente con capacitación y equipo. También decidió que se uniría a las fuerzas de la industria con miras a crear instituciones para resguardar las tecnologías de computadoras, desarrollar sistemas de información para identificar casos de uso indebido de las redes, perseguir a los infractores y recabar pruebas.

El Grupo de los Ocho ha dispuesto ahora centros de coordinación abiertos 24 horas al día, siete días a la semana para los encargados de hacer cumplir la ley. Estos centros apoyan las investigaciones de otros Estados mediante el suministro de información vital o ayuda en asuntos jurídicos, tales como entrevistas a testigos o recolección de pruebas consistentes en datos electrónicos.

Organización de Estados Americanos. En la Tercera Cumbre de las Américas, en la ciudad de Québec, Canadá, en 2001, los líderes que participaron se comprometieron a seguir la conectividad en las Américas debido al gran uso que hacen de la tecnología.

La Internet ha generado amenazas que ponen en peligro a toda la comunidad mundial de usuarios de Internet. La información que transita por Internet puede ser manipulada y mal utilizada para invadir la privacidad y defraudar a los usuarios La destrucción de los datos que residen en las computadoras conectadas por Internet puede obstaculizar las funciones del gobierno e interrumpir en una diversidad de servicios e infraestructuras.

Existen amenazas a través de las redes de tecnología, las cuales afectan a todos los sectores de la sociedad tanto a entes públicos como privados, no pueden ser manejadas por un solo gobierno puesto que muchas veces interfieren de un país a otro como lo reconoció la OEA en la Asamblea General en la resolución AG/RES. 1939 (XXXIII-O/03) (Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética), por lo cual es necesario desarrollar una estrategia integral para la protección de las infraestructuras de información que adopte un enfoque integral, internacional y multidisciplinario.

La OEA está comprometida con el desarrollo e implementación de esta estrategia de seguridad cibernética y en respaldo a esto, celebró una Conferencia sobre Seguridad Cibernética en Buenos Aires, Argentina, del 28 al 29 de julio de 2003 que demostró la gravedad de las amenazas a la seguridad cibernética para la seguridad de los sistemas de información esenciales, las infraestructuras esenciales y las economías en todo el mundo, y que una acción eficaz para abordar este problema debe contar con la cooperación intersectorial y la coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales.

La Estrategia Interamericana Integral de Seguridad Cibernética se basa en los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL),

y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA).

"La Estrategia reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad a fin de crear una cultura de seguridad cibernética".[85]

La Estrategia también reconoce que un marco eficaz para la protección de las redes y sistemas de información que integran la Internet y para responder a incidentes y recuperarse de los mismos dependerá en igual medida de que:

1. Se proporcione información a los usuarios y operadores para ayudarles a asegurar sus computadoras y redes contra amenazas y vulnerabilidades, y a responder ante incidentes y a recuperarse de los mismos.
2. Se fomenten asociaciones públicas y privadas con el objetivo de incrementar la educación y la concientización, y se trabaje con el sector privado –el cual posee y opera la mayoría de las infraestructuras de información de las que dependen las naciones—para asegurar esas infraestructuras.
3. Se identifiquen y evalúen normas técnicas y prácticas óptimas para asegurar la seguridad de la información transmitida por Internet y otras redes de comunicaciones, y se promueva la adopción de las mismas;
4. Se promueva la adopción de políticas y legislación sobre delito cibernético que protejan a los usuarios de Internet y prevengan y disuadan el uso indebido e ilícito de computadoras y redes.[86]

[85] Acurio del Pino Santiago, *op cit*., 13/09/08
[86] *Idem.*

4. Necesidad de incorporar una reglamentación en México y crear una regulación a nivel internacional.

Es necesario crear una regulación en el tema de delitos informáticos, es de suma importancia establecer un tipo.

Un principio básico en el derecho es *Nullum Crimen Sine Tipo y Nullum Crimen Sine Lege* (No hay crimen sin tipo y no hay crimen sin ley), por lo cual es necesario establecer el tipo exacto.

Asimismo para respetar y preservar el artículo 14 Constitucional.

Resulta de una manera difícil el hecho de que no haya una tipificación para los delitos que tratamos pero es de una labor inmensa basándonos en el hecho de los aspectos característicos de las conductas criminales enfocadas a estos ilícitos, tal como las contempla Antonio Enrique Pérez Luño en su libro "Ensayos de Informática Jurídica" las cuales denomina de la siguiente manera:

PECULIARIDADES DE LA CRIMINALIDAD INFORMÁTICA:

1. En el plano de la dogmática jurídico penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales o la aparición de nuevos delitos impensables antes del descubrimiento de las nuevas tecnologías; por ejemplo la posibilidad de que existan fraudes en los que el engaño se realiza sobre una máquina y no sobre una persona; de robos de servicios de ordenador, que es realizado en las cosas, o de hurtos de tiempo de ordenador sin que exista un ánimo de lucro, sino el mero propósito lúdico por quién realiza, y sin que se prive al titular de la cosa de su posesión.

2. Por tratarse de un sector sometido a constantes fluctuaciones e innovaciones tecnológicas, sus categorías son asimismo efímeras y cambiantes.

3. La criminalidad informática se caracteriza por las dificultades que entraña descubrirla, probarla y perseguirla. Es decir la dificultad de descubrir las conductas informáticas delictivas, además de la facilidad de penetrar en algunos sistemas informáticos y la personalidad especial de algunos de los delincuentes que pueden considerarse como un subtipo de la delincuencia de cuello blanco.

4. La propia precariedad y anacronismo del sistema jurídico penal refuerza la tendencia a no denunciar estos delitos, para evitar la alarma social o el desprestigio que de su conocimiento podría derivarse, lo que dificulta el conocimiento preciso del número de delitos perpetrados y la planificación de las adecuadas medidas legales sancionadoras o preventivas.

5. La insuficiencia de los instrumentos penales del presente para evitar y castigar las distintas formas de criminalidad informática, lo que supone un reto para la política criminal de criminalidad de los próximos años.

6. La dificultad de tipificar penalmente situaciones sometidas a un constante cambio tecnológico, la manifiesta insuficiencia de las sanciones en relación con la gravedad y el daño de los crímenes informáticos y la propia inadecuación de los medios penales tradicionales para remediar esta situación, determinan que, el Derecho penal informático sea un ejemplo manifiesto de Derecho penal simbólico. [87]

De lo anterior se puede resaltar que se entra en conflicto desde el momento en que se trata de tipificarla, perseguirla y comprobarla, para así poner una pena y encontrar correctivos y mejor aún medidas preventivas.

Existen un sin fin de actividades en la actualidad en las cuales encontramos la necesidad de un regulación y de encontrar una seguridad al efectuarlas. Ya que

[87] http://www.fing.uach.mx/MatDidactico/Legislacion/deliinfo.htm, 8 de abril de 2009.

en conductas que nos pueden resultar cotidianas podemos encontrar que es imperioso poner reglas.

Por ejemplo, es bien sabido que ahora la Internet es una de las fuentes más usadas como medio de comunicación para asuntos tanto personales como de trabajo, etc. Tomando en cuenta que quien usa este sistema lo hace tomando en cuenta que necesita gozar de cierta privacidad.

La privacidad es un punto clave en el desarrollo del individuo el interés de tener un espacio personal, libre de interferencias ya sea de personas así como de organismos públicos y privados.

En donde podemos encontrar la privacidad de información (interés que tiene un individuo de controlar o influenciar una información), privacidad en Internet (se encuentra el correo electrónico, criptografía, la esteganografía que sirve para ocultar datos y el anonimato para que no se sepa en que punto fue envíada información), privacidad de comunicación personal (es decir, un flujo de información entre personas sin necesidad de encontrarse en el mismo punto en el mismo momento) y privacidad de datos personales (esto es cuando los datos de un individuo se encuentran resguardados por un sitema este debe de comprometerse de manera responsable a custodiarlos para que personas ajenas no tengan derecho a información confidencial de sobre la situación específica de cada individuo.

Es de suma importancia la creación de acuerdos internacionales a través de los cuales se podría regular de manera más explícita los casos en los que existe un problema de jurisdicción, puesto que en ocasiones se han presentado casos en los cuales no se puede aplicar una sanción debido a que el ilícito fue cometido en más de un Estado.

De lo anterior tenemos el siguiente ejemplo:

En 1992, los piratas de un país europeo atacaron un centro de computadoras de California. La investigación policial se vio obstaculizada por la doble tipificación penal --la carencia de leyes similares en los dos países que prohibían ese comportamiento-- y esto impidió la cooperación oficial, según informa el Departamento de Justicia de los Estados Unidos. Con el tiempo, la policía del país de los piratas se ofreció a ayudar, pero poco después la piratería terminó, se perdió el rastro y se cerró el caso.

Asimismo, en 1996 el Servicio de Investigación Penal y la Agencia Federal de Investigación (FBI) de los Estados Unidos le siguió la pista a otro pirata hasta un país sudamericano. El pirata informático estaba robando archivos de claves y alterando los registros en computadoras militares, universitarias y otros sistemas privados, muchos de los cuales contenían investigación sobre satélites, radiación e ingeniería energética.

Los oficiales del país sudamericano requisaron el apartamento del pirata e incautaron su equipo de computadora, aduciendo posibles violaciones de las leyes nacionales. Sin embargo, los dos países no habían firmado acuerdos de extradición por delitos de informática sino por delitos de carácter más tradicional. Finalmente se resolvió la situación sólo porque el pirata accedió a negociar su caso, lo que condujo a que se declarara culpable en los Estados Unidos.

De lo anterior podemos observar que en algunos casos se puede rastrear e identificar a los que cometen este tipo de delitos pero ¿Qué sucede cuando no se sabe que país puede aplicar su ley? Pues resultaría muy difícil realizar extradición.

Otros casos importantes acerca de delitos informáticos son los siguientes:

1. Zinn, Herbert, Shadowhack.
Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de "Shadowhawk", fue el primer sentenciado bajo el

cargo de Fraude Computacional y Abuso en 1986. Zinn tenia 16 y 17 cuando violo el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US $174,000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publicó contraseñas y instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US$10,000. Se estima que Zinn hubiera podido alcanzar una sentencia de 13 años de prisión y una fianza de US$800,000 si hubiera tenido 18 años en el momento del crimen.

En el caso anterior podemos observar que no solamente obtuvo una sanción de cárcel sino una pecuniaria y mejor aún no sólo fue la aplicación de la pena sino el hecho que lo detectaron, lo detuvieron y fue así como se detuvo para que siguiera causando pérdidas.

2. Poulsen Kevin, Dark Dante.

Diciembre de 1992 Kevin Poulsen, un pirata infame que alguna vez utilizó el alias de "Dark Dante" en las redes de computadoras es acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusa a Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y encara hasta 10 años en la cárcel.

Siguió el mismo camino que Kevin Mitnick, pero es más conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a "ganar" un Porsche en un concurso radiofónico, si su llamada fuera la 102, y así fue.

Poulsen también crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional.

Esto fue lo que lo llevó a su estancia en la cárcel, 5 años, fue liberado en 1996, supuestamente "reformado". Que dicho sea de paso, es el mayor tiempo de estancia en la cárcel que ha comparecido un hacker.

De esta forma se denota que se aplicará una sanción para quien cometa estos ilícitos, evidentemente obteniendo un lucro.

3. Murphy Ian, Captain Zap.
En julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba "Captain Zap", gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o de la casa blanca. En ese entonces Ian Murphy de 24 años de edad, conocido en el mundo del hacking como "Captain Zap,".

Mostró la necesidad de hacer mas clara la legislación cuando en compañía de un par de amigos y usando una computadora y una línea telefónica desde su hogar viola los accesos restringidos a compañías electrónicas, y tenía acceso a ordenes de mercancías, archivos y documentos del gobierno. "Nosotros usamos a la Casa Blanca para hacer llamadas a líneas de bromas en Alemania y curiosear archivos militares clasificados" Explicó Murphy. "El violar accesos nos resultaba muy divertido". La Banda de hackers fue finalmente puesta a disposición de la ley". Con cargos de robo de propiedad, Murphy fue multado por US $1000 y sentenciado a 2 ½ años de prueba.

Es necesario establecer penas específicas para los tipos que se van suscitando, puesto que muchas veces algunos de los que cometen este tipo de

conductas delictivas únicamente lo hacen por el deseo de bromear sin creer causar daño alguno, siendo esto un error pues no sólo causan daños sino que pueden afectar la seguridad de las personas.

> *4. Morris Robert.*
> *En noviembre de 1988, Morris lanzó un programa "gusano" diseñado por él mismo para navegar en Internet, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de muchísimas computadoras y que más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causo a las víctimas muchos días de productividad perdidos, y millones de dólares. Se creó el CERT (Equipo de respuesta de emergencias computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de servicio comunitario y US $10,000 de fianza, bajo el cargo de Fraude computacional y abuso. La sentencia fue fuertemente criticada debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris más que el daño causado. El gusano producido por Morris no borra ni modifica archivos en la actualidad.*

El anterior es un ejemplo claro de lo que pueden ocasionar los virus y la necesidad de regularlos, ya que no sólo afectan a algunos sino a varios usuarios de este tipo de sistemas, inclusive trasgrediendo fronteras.

5. Creación de organismos e instituciones especializadas para su regulación y control.

Existen una serie de instituciones que ayudan en cierta manera a recibir quejas en el ámbito de delitos informáticos. Por ejemplo se encuentra la *CyberCop Holding Cell*, este es un servicio de quejas online.

Hay países que cuentan con grupos especializados en seguir la pista a los delincuentes cibernéticos. Uno de los más antiguos es la Oficina de Investigaciones Especiales de la Fuerza Aérea de los Estados Unidos, creada en 1978. Además existe la "Organización Internacional de Evidencia computacional, la Sección de delitos informáticos y Propiedad Intelectual del departamento de Justicia de los Estados Unidos de América"[88].

Otro es el de Investigadores de la Internet, de Australia, integrado por oficiales de la ley y peritos con avanzados conocimientos de informática. El grupo australiano recoge pruebas y las pasa a las agencias gubernamentales de represión pertinentes en el Estado donde se originó el delito

Sería importante crear la figura del auditor en materia de delitos informáticos, con una función de verificar, de planear y para observar y perseguir esta clase de ilícitos, para lo cual debe contar con ciertas características y habilidades.

Sería clave crear un organismo especializado en la persecución e investigación del tipo "delitos informáticos", un organismo que cuente la capacidad técnica suficiente y dotado de personal con los conocimientos necesarios.

Estos organismos además de contar con una serie de características básicas deben crear una serie de medidas.

En medios preventivos es indudable la necesidad de los denominados *firewalls* o paredes de fuegos. Al instalar un buen cortafuegos o *firewall* se puede eliminar las amenazas a la seguridad del sistema. Estos actúan como un escudo o barrera entre la red interna y el exterior y proveen un nivel de seguridad mucho mayor al que es proporcionado por contraseñas o *passwords.*

[88] Álvarez Cabrera Carlos Samuel, *"*El arte de la computación forense*"*, *Derecho Penal Contemporáneo, Revista Internacional*, Número 10 Bogota Colombia, Enero-Marzo 2005, p.22.

En algunos países se han adoptado organismos de prevención de delitos informáticos, tales como:

- La Guardia Civil Española, es pionera en la investigación de delitos informáticos tendientes a su prevención. Allí, los guardiaciviles virtuales se encuentran con colegas de similares departamentos de las mejores policías del mundo tales como La Scotland Yard Británica, el FBI norteamericano, la PAF francesa o los herederos del KGB soviético, y otros agentes undercover de los servicios secretos de las potencias.
- En Estados Unidos ya florecen los investigadores privados que han sustituido el arma de fuego por el arma electrónica y que, en vez de "pies planos", empiezan a ser denominados "colas planas", pues casi toda la investigación la realizan a través de Internet, cómodamente sentados frente a su computadora.
- En Argentina La División computación de la Policía Federal conformado por doce efectivos a cargo del subcomisario patrullan la red con el objeto de detectar los ilícitos que proliferan a través de ésta. Algunas veces lo hacen a requerimiento de instituciones y otras por expreso pedido de la justicia.
- El Grupo de Investigación en Seguridad y Virus Informáticos (G.I.S.V.I.), creado en la Universidad de Buenos Aires en 1995 actualmente funciona en la Universidad de Belgrano, ha resuelto varios casos de ataques de virus a empresas con características de acciones de sabotaje informático.[89]

Un caso que valdría la pena recalcar es el que se verá a continuación por las razones que expondré.

> *. Smith, David.*
> *Programador de 30 años, detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo, "Melissa". Entre los cargos presentados contra él, figuran el de "bloquear*

[89] http://www.angelfire.com/la/LegislaDir/Organ.html, 8 de abril de 2009.

las comunicaciones publicas" y de "dañar los sistemas informáticos". Acusaciones que en caso de demostrarse en el tribunal podrían acarrearle una pena de hasta diez años de cárcel.

Por el momento y a la espera de la decisión que hubiese tomado el juez, David Smith esta en libertad bajo fianza de 10.000 dólares. Melissa en su "corta vida" había conseguido contaminar a más de 100,000 ordenadores de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas estadounidenses como la del Gobierno del Estado de Dakota del Norte y el Departamento del Tesoro.

En España su "éxito" fue menor al desarrollarse una extensa campaña de información, que alcanzo incluso a las cadenas televisivas, alertando a los usuarios de la existencia de este virus. La detención de David Smith fue fruto de la colaboración entre los especialistas del FBI y de los técnicos del primer proveedor de servicios de conexión a Internet de los Estados Unidos, América On Line. Los ingenieros de América On Line colaboraron activamente en la investigación al descubrir que para propagar el virus, Smith había utilizado la identidad de un usuario de su servicio de acceso. Además, como otros proveedores el impacto de Melissa había afectado de forma sustancial a buzones de una gran parte de sus catorce millones de usuarios.

Fue precisamente el modo de actuar de Melissa, que remite a los cincuenta primeros inscritos en la agenda de direcciones del cliente de correo electrónico "Outlook Express", centenares de documentos "Office" la clave para encontrar al autor del virus. Los ingenieros rastrearon los primeros documentos que fueron emitidos por el creador del virus, buscando encontrar los signos de identidad que incorporan todos los documentos del programa ofimático de Microsoft "Office" y que en más de una ocasión han despertado la alarma de organizaciones en defensa de la privacidad de los usuarios. Una vez desmontado el puzzle de los documentos y encontradas las claves se consiguió localizar al creador de Melissa. Sin embargo, la detención de Smith no significa que el virus haya dejado de actuar.

Compañías informáticas siguen alertando que aún pueden quedar miles de usuarios expuestos a sus efectos, por desconocimiento o por no

haber instalado en sus equipos sistemas antivíricos que frenen la actividad de Melissa u otros virus, que han venido apareciendo últimamente como Happy99 o Papa.

En el caso anterior podemos observar cómo de manera conjunta no sólo los organismos encargados de perseguir este tipo de lícitos hacen frente a estas conductas, sino que contaron con el apoyo de una empresa dedicada a proveer de este servicio, lo cual hace que haya una mayor seguridad o apoyo con quien cuenta con los medios necesarios para perseguir estos ilícitos.

Por tanto es necesaria la creación de un organismo, o sí es por el momento difícil la creación de un área dentro de algunos de los organismos ya establecidos que se dediquen a la investigación y persecución de estos delitos.

Así como especialidades en el ámbito jurídico que sean proporcionados a los servidores públicos encargados de impartir justicia, para que ellos a su vez puedan y creando jurisprudencia y normas que sirvan para una mejor aplicación de justicia a estos tipos de delitos.

En el caso de México se ha formado la Coordinación Interistitucional de combate a Delitos Cibernéticos formado por la Presidencia de la República, Procuraduría General de la República, , Procuraduría General de Justicia del Distrito Federal, el Centro de Investigación y Seguridad Nacional, la Secretaría de Defensa Nacional, la Secretaría de Marina, la Secretaría de Seguridad Pública. Además la UNAM, entre otras. Entre algunas de sus actividades esta el patrullar las redes, así como rastrear delitos que se cometen a través de medios electrónicos y crear bases de datos con las características de algunos delitos, especialmente el de pornografía infantil en la red.

Por lo que sería recomendable que tuviera más elementos y pudiera rastrear un mayor número de delitos por estos medios.

CONCLUSIONES.

El rápido avance tecnológico ha tenido como consecuencia que el uso de redes de información sea más asequible, así como el uso de equipos de cómputo.

El crecimiento tecnológico ha generado la existencia de los llamados delitos informáticos, los cuales tienen características propias, por lo cual se dificulta su entendimiento, tanto para conceptualizarlo, así como para enmarcarlo en el ámbito legislativo, ya que resulta difícil el equiparar de lo que puede existir en una realidad llamémosla virtual y el mundo fáctico.

Por lo anterior se puede concluir lo siguiente:

1. En la presente tesis se abordó de una manera clara lo que es la teoría del delito, así como los elementos positivos y negativos que la constituyen, lo anterior, con la finalidad de poder analizar los delitos informáticos; desde conceptualizarlos hasta su formal integración.

Se puede desprender con respecto a la teoría del delito que es necesario una serie de elementos de aspectos positivos y negativos para que un delito se configure o no, por lo cual en los países en los cuales se han dado casos en donde se cometen el tipo de ilícitos informáticos tienen que cumplir con los requisitos establecidos en su derecho positivo.

2. El derecho comparado es de gran importancia ya que en base al mismo se pueden establecer las semejanzas y diferencias existentes en el derecho de cada país.

3. Debido al derecho comparado se puede observar que en todas las legislaciones que contemplan ilícitos informáticos el punto en el cual convergen es en el hecho de que la conducta implique copia, acceso, modificación o destrucción de información contenida dentro de un equipo informático o el uso de redes informáticas como medio para cometer ilícitos.

4. Una de las diferencias principales de nuestro país con los analizados en la presente tesis, es el hecho de que en algunos países tienen leyes específicas sobre delitos informáticos o por lo menos un apartado especial en sus legislaciones penales. Algunos de nuestros Estados han integrado un capítulo respectivo, pero lo más conveniente sería que se estableciera a nivel Federal.

5. Una de las semejanzas relevantes que se puede encontrar entre México con Chile, es lo relativo a la propiedad intelectual. Chile a pesar de tener una Ley de delitos informáticos, contemplan algunas hipótesis que se pudieran dar dentro de su ley de propiedad intelectual, este hecho es observado dentro de nuestra reglamentación, si bien no se menciona en nuestra Ley de Derechos de Autor los delitos informáticos, si existen bienes que son vulnerados que corresponden al ámbito de los delitos informáticos.

6. Otra de las semejanzas con lo establecido por las leyes de México, Austria, Chile y España es el hecho de que las personas sean responsables de la información que es vulnerada o tengan acceso a ésta por cuestión del cargo que desempeñan, ó son profesionales en estos sistemas informáticos, hace que la pena que se les vaya a imponer aumente.

7. En cuanto a las diferencias principales radican en que algunas legislaciones solamente se mencionan lo relativo a la alteración o destrucción de datos mientras que otras no solo contemplan este hecho sino que también pueden ser vulnerados cuando son utilizados como medio de prueba.

8. El derecho comparado juega un papel importante ya que nos permite conocer mejor nuestras leyes y las leyes que existen en otros países, y como son abordados estos ilícitos para poder tomarlos en cuenta y así tomar figuras que pudieran sernos de utilidad para la prevención, seguimiento y persecución del delito informático.

9. En los defectos que podemos encontrar en nuestra legislación es que no se encuentre regulado un capítulo específico de “Delitos informáticos”; por lo cual, lo que aquí se sostuvo es la insuficiencia de nuestra legislación en delitos informáticos y la necesidad de crear una apartado específico.

10. De lo analizado anteriormente se puede observan con suma claridad el hecho de las deficiencias que nuestra legislación guarda con otras y más que eso, la necesidad de establecer bases para una mejor reglamentación de los delitos informáticos.

Por lo cual las siguientes son propuestas que pueden ayudar a una mejor detección de los delitos informáticos, así como su seguimiento y erradicación dentro de lo que va permitiendo el rápido avance y uso de la tecnología.

A) Es de suma importancia la creación de una regulación a nivel nacional.

Específicamente la incorporación de un capítulo relativo a delitos Informáticos en el Código Penal Federal, en el cual se señale de manera clara lo que es un delito informático, así como las hipótesis de las conductas que puedan ser consideradas dentro de este tipo de ilícitos.

Lo anterior con el objetivo de que sea uniforme la legislación a nivel nacional.

B) Creación Tratados Internacionales.

La creación de tratados internacionales por medio del cual se establezcan: tipos, sanciones así como hipótesis de los ilícitos y las jurisdicciones aplicables.

Esto con la finalidad de que no haya problemas al momento de establecer el derecho aplicable y la forma en que este deberá ser ejercitado, principalmente para resolver el problema de jurisdicción y la diversidad de opiniones que pueden existir en el hecho de establecer que tipos penales pueden ser incluidos en los delitos informáticos.

C) La creación de una serie de medidas preventivas para no ser afectado mediante este tipo de ilícitos.

Esto mediante la elaboración de un reglamento creado por una autoridad capacitada para tal efecto.

Por otro lado, una estrategia por medio de la cual la población que utiliza los equipos de cómputo, puedan protegerse y resguardar sus equipos y su información. Es decir, una educación respecto a la utilización de medios de información y de uso de redes de manera adecuada.

D) La creación de organismos que tengan la capacidad técnica y jurídica para la persecución de los sujetos activos de estos ilícitos informáticos.

Es decir la creación de una entidad o dependencia del gobierno que cuente con la capacidad técnica y subsidios necesarios para poder dar una persecución adecuada a estos ilícitos.

Desde la investigación, así como el rastreo de los sujetos activos de los ilícitos.

E) Personal capacitado.

Una serie de personas que puedan laborar en este campo que cuenten con conocimientos tecnológicos, jurídicos y que cuenten con cursos en donde puedan ser preparados de una manera adecuada para poder desempeñar un buen papel demostrando las habilidades adquiridas y con un gran sentido de ética y justicia.

Es decir, personal administrativo con conocimiento en sistemas y equipo de cómputo que pueda rastrear a los sujetos activos, hasta autoridades que tengan los conocimientos jurídicos para la aplicabilidad de leyes específicas en el ámbito del Derecho.

BIBLIOGRAFÍA.

1. ALTMARK, Daniel Ricardo, "Informática y Derecho", Reimpresión, Ediciones de Palma, Buenos Aires, 1991.
2. ARILLA BAS Fernando, "Derecho Penal. Parte General", Editorial Porrúa, México, 2001.
3. BELTRAMONE Guillermo y ZABALE Ezequiel, "El Derecho en la Era Digital", Editorial Juris, Argentina, 1997.
4. BERCHELMANN ARIZPE Antonio, "Derecho Penal Mexicano" "Parte General", Editorial Porrúa, México, 2004.
5. BIBIANA Luz Clara, **"**Manual de Derecho Informático**"**, Editorial Jurídica Nova Tesis, Argentina, 2001.
6. BRIZZIO Claudia R. **"**La informática en el Nuevo Derecho", Ediciones Abeledo-Perrrot, Buenos Aires Argentina, 2000.
7. CARRANCA Y TRUJILLO Raúl y CARRANCÁ Y RIVAS Raúl, "Derecho Penal Mexicano. Parte General", Vigésimo primera edición, Editorial Porrúa, México, 2001.
8. CAMPOLI Gabriel Andrés, "Derecho Penal Informático en México", Instituto Nacional de Ciencias Penales", México, 2004.
9. CARBALLAR José Antonio, "Internet. Libro del navegante", Tercera edición, Editorial Ra-Ma, España, 2002.
10. CASTELLANOS Tena Fernando, "Lineamientos Elementales de derecho Penal", Trigésima Segunda Edición, Editorial Porrúa, México, 1993.
11. CORREA Carlos M., y otros, "Derecho Informático", Ediciones DEPALMA, Buenos Aires, 1994.
12. DE MARCELO RODAO Jesús, "Piratas Cibernéticos, Cyberwars, Seguridad Informática e Internet", Segunda edición, Editorial Ra-MA, Madrid, 2003.
13. DIAZ ARANDA Enrique, "Derecho Penal, Parte General", Editorial Porrúa, México, 2004.
14. FERREYR Gonzalo, "Internet. Paso a paso hacia la autopista de la información", Alfaomega Grupo editor, México, 1996.

15. GARCÍA MEJIA Pablo, **"**Princípios de Derecho de Internet", Editorial Tirant Lo Billanch, Valencia, 2002.
16. GARCÍA RAMÍREZ Sergio y ADATO GREEN Victoria, "Prontuario del Proceso Penal Mexicano", Décima Edición, Editorial Porrúa, México, 2002.
17. GOODMAN Marc, "Cibercriminalidad", INACIPE, México, 2003.
18. GUIBOURG Ricardo A., "Informática Jurídica Decisoria", Ediciones Astrea de Alfredo y Ricardo DEPALMA, Buenos aires, 1993.
19. HARLEY Hahn y RICK Stout, "Internet. Manual de referencia", Mc Graw – Hill – Interamericana, España-México, 1999.
20. HERNÁNDEZ ISLAS Juan Andrés, "Mitos y Realidades de la Teoría del Delito", Editorial Jahia, México, 2006.
21. JALIFE DAHER Mauricio, "Uso y valor de la propiedad intelectual", Editorial Gasca Sicco, 2004.
22. JIMENEZ DE ASÚA Luis, "Teoría del Delito", IURE editores, México, 2003.
23. LÓPEZ BETANCOURT Eduardo, "Delitos en Particular. Tomo IV", Primera edición, Editorial Porrúa, México, 2004.
24. LUZÓN PEÑA Diego Manuel, "Enciclopedia Penal Básica", Granada, 2002.
25. MEZGER Edmund, "Derecho penal, Tomo I, parte general", Valleta ediciones, Buenos Aires, 2004.
26. MIR PUIG Santiago, "Delincuencia Informática", Primera edición, Editorial PPU, Barcelona, 1992.
27. MOLINA SALGADO Jesús Antonio, "Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial", Primera edición, Editorial Porrúa, México, 2003.
28. NAVA GARCÉS Alberto Enrique, "Análisis de los delitos Informáticos", Editorial Porrúa, México, 2005.
29. PARDINI Anibal A., "Derecho de Internet", Ediciones La Rocca, Buenos Aires, 2002.
30. RIGHI Esteban y FERNÁNDEZ Alberto, "Derecho Penal. La ley, el delito, el proceso y la pena", Reimpresión, Editorial Hammurabi, Buenos Aires, 2005.

31. RODRÍGUEZ Luis Angel, "Seguridad de la Información en Sistemas de Cómputo", México, 1995.
32. SANTAMARÍA RAGA José Mario y SANTA MARÍA RAGA Sergio, "Introducción a la Computación", México, 2002.
33. SIMON HOCSMAN Heriberto, "Negocios en Internet", Editorial Astrea, Buenos Aires, 2005.
34. SIRVENT GUTIÉRREZ Consuelo y VILLANUEVA COLÍN Margarita, "Sistemas Jurídicos Contemporáneos", Harla, México, 2004.
35. SOSA ORTIZ Alejandro, "El Cuerpo del Delito. La problemática en su acreditación", primera edición, Editorial Porrúa, México, 2003.
36. STRATENWERTH Gûnter, "Derecho penal. Parte general I", Editorial Hammurabi, Buenos Aires, Argentina, 2005.
37. TELLEZ AGUILERA Abel, "Nuevas Tecnologías Intimidad y Protección de Datos", Editorial EDISOFER S.L. Libros jurídicos, Madrid, 2001.
38. TELLEZ VALDES Julio, "Derecho Informático", tercera edición, Editorial Mc Graw Hill, México, 2004.
39. VERGARA TEJADA José Moisés, "Manual de Derecho Penal", Angel Editor, México, 2002.
40. VIÑAMATA PASCHKES Carlos, "La Propiedad Intelectual", Editorial Trillas, Cuarta edición, México, 2007.
41. WYATT Allen L., "La Magia del Internet", Mc Graw – Hill, México, 1995.
42. ZARICH Faustina "Derecho 2 Informático", Editorial Juris, Argentina, 2001.
43. ZWEIGERT Honrad y KOTZ Hein, "Introducción al derecho comparado", Editorial Oxford, 2002.

HEMEROGRAFÍA.

1. ÁLVAREZ CABRERA Carlos Samuel, *"*El arte de la computación forense*"*, *Derecho Penal Contemporáneo, Revista Internacional*, Número 10 Bogota Colombia, Enero-Marzo 2005, pp.19-37.
2. B. BIERCE WILLIAN, *"*El delito de violencia tecnológica en la legislación de Nueva York*"*, *Derecho de la Alta Tecnología*, Año VI, Número 66, Febrero, 1994, pp. 20-22.
3. DAZA GÓMEZ Carlos, *"*Teoría del delito*", Responsa*, Centro Universitario México, División de Estudios Superiores A.C., Año 3, Número 16, México, Agosto-Septiembre 1998, pp.3-6.
4. FORNAGUEIRA Andrea Isabel y ETIENNE Patricia Marcela, "Los virus informáticos y la protección penal de la información*"*, *Anuario 1993*, Universidad Nacional de Córdoba, Facultad de Derecho y Ciencias Sociales Córdoba, Argentina, 1993, pp. 137-151
5. LARA BERRIOS Bernardo y MORALES GODOY Misael, "Los delitos informáticos. ¿Nuevos tipos penales o nuevas formas comitivas de los delitos tradicionales?", *La Revista de Derecho*, Universidad Central de Chile, Facultad de Ciencias Jurídicas y Sociales, Año X, Número 6, Santiago, Chile, Enero-Junio 2004, pp.183-197.
6. LIMA VIANNA Tulio, *"*La era del control. Introducción crítica al derecho penal cibernético*"*, *Ciencias Penales*, Año 16, Número 22, Costa Rica, Septiembre, 2004, pp.43-59
7. PÉREZ MARTÍNEZ Alfonso, *"*Necesidad de tipificar el delito computacional en el Código de Defensa Social de Puebla*"*, *IUS Revista del Centro y Documentación Jurídica del Instituto de Ciencias Jurídicas de Puebla*, Año V, Número 98, México, Abril-Noviembre, 2001, pp. 40-43.
8. R. NIELSEN Daniel, *"*Los casos más usuales de criminalidad informática y cibernética*"*, *Revista Catalana de Seguretat Pública. Los nuevos retos en la investigación de delitos*, Editorial Escola de Policia de Catalunya, Número 3, Diciembre, 1998, pp.21-25.

9. TÉLLEZ VALDES Julio, *"*Los delitos informáticos: Situación en México*"*, *La Barra*, Revista de la Barra Mexicana, Colegio de Abogados, Número 14, México-Junio, 1997, pp.18-25.

LEGISLACIÓN.

1. Constitución Política de los Estados Unidos Mexicanos. Agenda de Amparo del D.F., Ediciones Fiscales ISEF, México, 2009.
2. Código Penal Federal, Agenda Penal del D.F., Ediciones Fiscales ISEF, México, 2008.
3. Código Penal para el Distrito Federal, Agenda Penal del D.F., Ediciones Fiscales ISEF, México, 2008.
4. Ley Federal del Derecho de Autor, Agenda mercantil, Ediciones Fiscales ISEF, México, 2008.

CIBERGRAFIA

1. ACURIO DEL PINO,
http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf, 13 de septiembre 2008.

2.CAMARGO PACHECO, María de Jesús,
http://cursweb.educadis.uson.mx/mcamargo/documentos/NOTAS%20PARA%20EDICION%20DERECHO%20PENAL%20I.doc, 3 de marzo 2008.

3. http://www.delitosinformaticos.com.mx/legislacion.htm, 20 enero de 2008.

4. http://www.fing.uach.mx/MatDidactico/Legislacion/deliinfo.htm, 8 de abril de 2009

5. http://www.angelfire.com/la/LegislaDir/Organ.html, 8 de abril de 2009.