872709

UNIVERSIDAD DON VASCO, A.C.

INCORPORACIÓN No. 8727-09 A LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

ESCUELA DE DERECHO

"ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA EN EL CÓDIGO PENAL DEL ESTADO DE MICHOACÁN"

T E S I S

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN DERECHO

P R E S E N T A

TRUD HINZPETER LARA

URUAPAN, MICHOACÁN, AGOSTO DEL 2004

SUBDIRECCIÓN DE CERTIFICACIÓN

ANEXO 45
FORMA PT01-A

UNIVERSIDAD
DON VASCO, A.C.

IMPRESIÓN DE TESIS INDIVIDUAL

C. DIRECTORA GENERAL DE INCORPORACIÓN Y REVALIDACIÓN DE ESTUDIOS, UNAM
P R E S E N T E:

HINZPETER	LARA	TRUD
APELLIDO PATERNO	MATERNO	NOMBRE(S)

NÚMERO DE EXPEDIENTE: 95601954-9

ALUMNO DE LA CARRERA DE: LICENCIADO EN DERECHO

CUMPLE CON LA REVISIÓN DE LA TESIS TITULADA:

"ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA EN EL CÓDIGO PENAL DEL ESTADO DE MICHOACÁN".

POR LO QUE SE AUTORIZA LA IMPRESIÓN DE LA MISMA.

URUAPAN, MICH., AGOSTO 2 DEL 2004.

TRUD HINZPETER.
FIRMA DEL SOLICITANTE

V° B°

ASESOR DE LA TESIS

LIC. FEDERICO JIMÉNEZ TEJERO
DIRECTOR TÉCNICO

DEDICATORIAS:

A mi padre:

Guillermo Hinzpeter Mazón

Por ser un hombre maravilloso quien toda la vida me ha brindado su apoyo en los momentos más difíciles de mi vida, quien con su ejemplo día con día me ha hecho ser mejor luchar por lograr todas aquellas metas que me he propuesto en mi vida, por otorgarme todo lo necesario para salir adelante, por inculcar en mi su educación y cariño; estando junto a mi en los momentos más difíciles para apoyarme, corregirme y alentarme a ser mejor.

Sobre todo por ser el mejor padre del mundo gracias papá.

A mi madre:

Dafne Ma. De Lourdes Lara Jaimes:

Por que siempre ha estado a mi lado, por haberme dado la vida y dedicar la suya a velar por mi bienestar, buscando siempre que sus hijas seamos las mejores; por no dejar que me diera por vencida nunca, luchar contra todo y todos por nosotros, gracias mamá.

A mis Hermanas:

Cariño, Ilse y Astrid

Con quienes crecí compartiendo mi vida, quienes me apoyaron siempre y estuvieron conmigo cuando las necesite, brindándome su apoyo y cariño.

A los Licenciados:

José Aguilar Fabela y Rosa Ma. García Bejar

Que siempre estuvieron conmigo en los momentos que los necesite apoyándome, corrigiéndome y enseñándome cuando lo necesitaba.

Por que siempre estuvieron conmigo en la realización de este trabajo brindándome su amistad, cariño y respaldo en todo momento, dedicando parte de su tiempo sin pedir nada a cambio.

A todos mis maestros de la Escuela de Derecho, quines me apoyaron y ayudaron a superarme días con día.

A los directivos de esta Escuela quienes día con día tenían que velar y luchar por nosotros, buscando la manera de sacarnos adelante.

Agustín Espinosa Sepúlveda y a mis amigos:

Quienes en todo momento estuvieron conmigo luchando y apoyándome en todos los momentos en que los necesitaba junto a mi.

Por alentarme a no darme por vencida y superar todos los retos que me ponía la vida.

INDICE

INTRODUCCIÓN

Los medios de comunicación y tecnológicos han ido avanzando de manera significativa a través de los años , con el inicio de la era informática se han encontrado grandes beneficios; como lo es la gran rapidez con que en estos momentos puedes comunicarte con personas que no se encuentran cercanas a uno.

De igual forma los sistemas informáticos han venido a representar uno de los primeros medios de trabajo de las personas, ya que son más eficientes y más rápidos; muchas de las veces han venido a suplir la mano del hombre.

Existe una gran necesidad de hacer que el derecho penal, en especifico el Código Penal del Estado de Michoacán, regule el acceso ilícito a sistemas y equipos de informática, ya que éste no lo contempla, siendo un problema que en la actualidad nos afecta a la gran mayoría de las personas, pues que los avances que ha tenido la informática, como lo es el Internet como medio de comunicación, el uso de la computadora en el trabajo, así como para guardar documentos de carácter personal, se han vuelto vitales para el desenvolvimiento del trabajo, escuela, de la comunicación en general; viniendo a facilitar en gran medida la realización del trabajo.

Dada la necesidad de utilizar estos equipos o sistemas de informática en nuestra vida diaria, también se ha creado la manera de protegerlos con la

finalidad de que no pueda accederse a estos sistemas sin autorización del dueño, o que no se llegue a conocer la información que se encuentre protegida por los mecanismos de seguridad.

Sin embargo existen personas ajenas o como comúnmente se les ha venido nombrando los HACKERS, quienes se dedican a cometer conductas que nos perjudican como es el acceder a los sistemas, llegando a conocer la información que en ellos se contiene.

Al existir una reglamentación en el Código Penal del Estado, se lograría la regulación de la conducta y con ello la forma de sancionarlos, evitando que se siga afectando a todas aquellas personas que son víctimas del acceso ilícito a sistemas o equipos de informática protegidos por algún mecanismo de seguridad: o que se conozca la información contenida en los sistemas o equipos de informática, por personas que tienen conocimientos en el ramo o las que sin tenerlo realizan estas conductas con o sin el propósito de afectar a las personas físicas .

Por lo que con la realización de este trabajo se buscó explicar de una manera más clara cuales son las consecuencias de la comisión de estas conductas. de que manera podrían ser reguladas, señalara específicamente quienes son los sujetos que las cometen, así como las diferentes legislaciones que las contemplan.

Buscando lograr por último que se tipifique en el Código Penal del Estado el acceso ilícito a sistemas y equipos de informática, transgrediendo medidas de seguridad, señalando como conductas tanto el acceso no autorizado, como el conocimiento de la información protegida por mecanismos de seguridad.

De lo anterior podemos afirmar que dentro de el **PLANTEAMIENTO DEL PROBLEMA** se ha considerado que el derecho debe irse adecuando a las necesidades que día con día van surgiendo, ya que la informática va avanzando de forma más acelerada que el derecho penal, por lo que resulta evidente que los avances tecnológicos constituyen un factor que ha ido cobrando vital importancia en el campo del derecho como ciencia que regula las relaciones de las personas que viven en sociedad, este debe ser actual y acorde a las necesidades con el fin evitar la destrucción y violación del hardware y el software, otorgando una protección jurídica eficaz, ya que dichos medios pueden otorgar datos e informaciones que de ser conocidas afectarían en gran medida a la persona a la cual pertenecen, dado el contenido de la información y la perdida que puede llegar a producirse por dichas violaciones; así mismo podemos ver que en la actualidad dado los avances que existen, que se constituyen, aproximadamente desde el año 1998 hasta nuestros tiempos año 2003.

La forma más común de comunicarnos y llevar acabo nuestro trabajo, es con ayuda de las computadoras, desarrollándose con ello más continuamente

las conductas antes mencionadas provocando perdidas tanto en la información y en la confidencialidad de la misma., por poner un ejemplo se da el acceso no autorizado a los sistemas de informática los cuales tienes comunicaciones confidenciales con personas y que llegan a ser conocidas, por aquellas personas que transgreden los medios de seguridad contenidos y que por lo general son personas que tienen conocimiento en esa área o simplemente tienen aptitudes.

Se otorgo una **JUSTIFICACIÓN PERSONAL**, en la cual se especificaba que existe una gran necesidad de hacer que el derecho penal, en especifico el Código Penal del Estado de Michoacán, regule el acceso ilícito a sistemas y equipos de informática, ya que éste no lo contempla en ningún momento, siendo un problema que en la actualidad nos afecta a la gran mayoría de las personas, pues que los avances que ha tenido la informática, como lo es el Internet como medio de comunicación, el uso de la computadora en el trabajo por mencionar algunos, se han vuelto vitales para el desenvolvimiento del trabajo, escuela, de la comunicación ya que han venido a facilitar en gran medida la realización del trabajo, dada la necesidad de utilizar estos equipos o sistemas de informática en nuestra vida diaria, con dicho avance también se ha creado la manera de afectar los sistemas y equipos de informática, por personas ajenas o como comúnmente se les ha venido nombrando los HACKERS.

Al existir dicha reglamentación se lograría la regulación de la conducta y con ello la forma de sancionarlos, evitando que se siga afectando a todas aquellas personas que son víctimas del acceso o conocimiento de la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad; por personas que tienen conocimientos en el ramo o las que sin tenerlo realizan estas conductas con el propósito de afectar a las personas físicas.

Llegando de esta manera a concluir una justificación la cual es dada con el trabajo que se practico, buscando documentar el objetivo general que se planteó para la realización del trabajo, el cual consistía en "analizar las legislaciones actuales, con la finalidad de lograr verificar la necesidad que existe de reglamentar el acceso ilícito a sistemas y equipos de informática, como figura autónoma, en el Código Penal del Estado de Michoacán". Verificando que nos encontramos en una situación en la que existe la necesidad apremiante de lograr que se sancione a los sujetos que cometen este tipo de conductas ya que afectan a las personas físicas sobre las cuales recaen estas figuras.

Como objetivos particulares dentro de este trabajo fueron el "Identificar con claridad las conductas que se buscan regular". Considerándose en ella lo referente al que sin autorización acceda o tenga conocimiento de la información contenida en los sistemas y equipos de informática protegidos por algún mecanismo de seguridad.

Como segundo de los objetivos tenemos el "Determinar las sanciones que podrán imponerse a dichas conductas". Dentro de las cuales nos basamos en gran medida para la imposición de las mismas en el Código Penal Federal, ya que este prevé varias conductas y su penalidad.

Por último el tercer elemento consistia en "Determinar mediante la comparación de legislaciones la forma de regular las conductas con el fin de evitar que se sigan cometiendo". De tal suerte que se realizo una comparación de las diferentes legislaciones internacionales, así como de las nacionales entre las cuales encontramos al Código Penal Federal y al Código Penal del Estado de Sinaloa; identificando de que manera prevén las conductas estas legislaciones y cual es el bien jurídico tutelado, logrando de esta forma establecer cual es la manera más adecuada de legislar estas conductas.

Llegando de esta forma de esta forma a establecer que de acuerdo a la hipótesis planteada en un principio la cual consistía en saber si "es necesaria la reglamentación del acceso ilícito a sistemas o equipos de informática con la finalidad de que sea considerado como figura autónoma en el Código Penal del Estado, a fin de regular y sancionar dicha conducta." Estableciendo se que de acuerdo al investigación documental que se realizó si existe una necesidad apremiante de que sea regulada, ya que a pesar de que existe una regulación en materia Federal, no es posible sancionarla por medio de los órganos del estado, ya que la legislación estatal no prevé en ninguna

forma esta conducta; de igual forma no existe ningún tipo de información al respecto de ella.

Respecto de esta figura no existe amplia información en los libros por lo cual gran parte del desarrollo del tema se baso en los trabajos que se encuentran en Internet en paginas que se han creado especialmente para crear una conciencia sobre este tipo de problemas que se acarrean con los delitos informáticos; los cuales se encuentran realizados por diversos profesionales en la materia de derecho y de la informática, los cuales únicamente realizan análisis sobre el tema y los problemas que se acarrean precisamente por la falta de reglamentación que existe.

Así por ultimo tenemos que los diversos capítulos que se analizaran dentro de este trabajo buscarán justificar de manera especifica, la necesidad que existe de regular estas conductas a fin de que ya no se sigan cometiendo y que puedan ser perseguidas y sancionadas por nuestros órganos del estado.

CAPITULO 1. ANTECEDENTES HISTÓRICOS

Desde los tiempos más remotos el ser humano ha buscado la mejor forma de comunicarse con otros de su misma especie, aun cuando éstos se encuentren en lugares lejanos. La historia de la comunicación está marcada por los adelantos tecnológicos de cada época y lugar.

En un principio, la comunicación que se establecía con otros pueblos lejanos era mediante la voz, viajeros que recorrían grandes distancias con la finalidad de llevar y traer mensajes e información. Con la aparición de la escritura se inicia una nueva era, sin embargo los mensajes seguían siendo enviados de igual manera, era un proceso lento y difícil.

Con el inicio de la era tecnológica, se dispuso de un medio con el cual fue posible establecer una comunicación a distancia y casi instantánea por medio de códigos y claves de sonido: el telégrafo; posteriormente la comunicación humana se vio beneficiada con la invención del teléfono permitiendo el uso de la voz, más adelante vino la radio, la televisión y con ello las computadoras.

Estos grandes inventos son la base de los adelantos tecnológicos que disfrutamos hoy en día en cuanto a comunicación, desde el envío y recepción de un fax hasta la comunicación instantánea en cualquier lugar del mundo por medio

de Internet.

Internet es hoy en día una infraestructura informática extendida ampliamente, su influencia alcanza no sólo al campo técnico de las comunicaciones entre computadoras (redes), también a toda la sociedad en la medida en que su empleo se incrementa cada vez más para llevar a cabo procesos como el comercio electrónico, la adquisición de información y la interacción entre la comunidad o comunidades remotas.

Para llegar a los niveles de comunicación que hoy se logran gracias a Internet, se han dedicado años de investigación y perfeccionamiento del tipo de transmisión. Las primeras redes de cómputo comenzaron a operar a mediados de los años 70's y la forma de comunicación entre dos computadoras era manual, se empleaba una cinta magnética o una pila de tarjetas perforadas, las cuales necesitaban ser insertadas a la otra computadora mediante la intervención humana, es decir, no funcionaban automáticamente como hoy se hace.

Más tarde, este proceso se perfecciono y se logró transmitir información mediante cables conectando 3 o más computadoras, surgiendo así las redes, esta comunicación se establecía a muy baja velocidad y además había un gran inconveniente, las computadoras que formaban la red tenían que funcionar a la perfección porque a la menor falla de cualquiera de ellas la red dejaba de operar y

era necesario desconectarla para dejar funcionando a las demás.

A partir de este momento, comienza una evolución tecnológica con las primeras investigaciones de conmutación de paquetes entre redes. Internet, en un principio fue un proyecto militar de los Estados Unidos.

1.1 INTERNACIONALES

En el año de 1996 los medios de comunicación y algunas empresas interesadas en obtener nuevos mercados comenzaron a hablar del Internet como si se tratase de un fenómeno que se acabara de producir.

Esto no es así ya que estos orígenes se dan desde 1969, ya que en plena guerra fría entre los países occidentales y la URSS y sus naciones satélites, el Departamento de Defensa de los Estados Unidos, estaba preocupado por las consecuencias que podría tener un corte en sus sistemas de comunicaciones que cada vez iban alcanzando mayor importancia para la defensa del país.

En 1969 la Advanced Research Projects Agency (ARPA) del Pentágono creó la primera red llamada ARPANET, la cual constaba sólo de cuatro computadoras conectadas, una en la Universidad de California en los Ángeles

(UCLA), otra en el Instituto de Investigaciones de Stanford (SRI), una más en la Universidad de California en Santa Bárbara (UCSB) y la última en Universidad de UTHA. Para el año de 1971, ya se contaba con 11 nodos más, y en el año siguiente ya había un total de 40. En ese año se tiene registrado el primer mensaje enviado y recibido por correo electrónico de Ray Tomlinson, pero fue hasta el segundo mensaje de prueba cuando se estableció que todos los mensajes que se enviaran deberían emplear el signo @.

Los investigadores norteamericanos pensaron que los sistemas de comunicaciones debían tener una estructura de tela de araña de forma que si una vía quedaba bloqueada se pudiese seguir enviando la información a través de las restantes. Esto de tal forma que todas las computadoras estuvieran conectadas entre sí, logrando que al momento que alguna fuera bloqueada o dejara de funcionar quedarán las restantes para seguir enviando y recibiendo información.

El crecimiento de esta red iban envolviendo a globo terráqueo hizo que se incorporaran como usuarios gentes de distinta procedencia especialmente del mundo universitario, creando una propia filosofía de lo que ya se empezó a llamar Internet.

En 1974 los investigadores Vint Cerf y Robert Kahn, redactaron un documento titulado A protocol for Packet Network Internetworking, donde

explicaban como podría resolverse el problema de comunicación entre los diferentes tipos de computadoras, dichos estudios fueron aplicados 8 años después, creándose de esta forma la Transmition Control Potrocol-Internet Protocol (TCP-IP, protocolo de control de transmisión / protocolo de Internet), este protocolo fue adaptado de inmediato como estándar por el Departamento de Defensa de los Estados Unidos, quien este mismo año se separó de ARPANET y creó una red propia llamada MILNET. Asimismo, surgieron nuevos organismos que le dieron el termino Internet, tal y como ahora se le conoce mundialmente.

El protocolo TCP/IP es un sistema de comunicación muy sólido y robusto bajo el cual se integran todas las redes que conforman Internet; durante su desarrollo se incrementó notablemente el número de redes locales de agencias gubernamentales y de universidades que participaban en el proyecto, dando de esta manera, origen a la red de redes más grande del mundo.

Las funciones militares de un principio se separaron y se permitió el acceso a la red a todo aquel que lo requiriera, sin importar de que país proviniera, siempre y cuando fuera para fines académicos o de investigación, por tal razón Internet tuvo su etapa de desarrollo dentro de las Universidades. Hasta este momento la velocidad de transferencia entre nodos, era de 56 kilobits por segundo.

La red que dio origen a la red de redes, ARPANET dejó de funcionar en 1990, pero ya existían varios organismos encargados de Internet, en Europa existía el CERN (European High-Energy Particle Physics Lab), dicho organismo dos años más tarde crearía al hoy conocido World Wide Web (WWW), para lo que empleó tres recursos: HTML (Hypertext Markup Lamguage), HTTP (Hypertext Transfer Protocol) y un programa cliente llamado Web Browser.

Internet como ahora lo conocemos encierra una idea técnica clave, la de arquitectura abierta de trabajo en red, así como múltiples redes independientes, de diseño casi arbitrario. En una red de arquitectura abierta, las redes individuales pueden ser diseñadas y desarrolladas separadamente, donde cada una puede tener su propia y única interfaz. Cada red puede ser diseñada de acuerdo con su entorno específico y los requerimientos de los usuarios, no existen restricciones en los tipos de red que pueden ser incorporadas ni tampoco en su ámbito geográfico.

En 1993 se funda Netscape, compañía que lanza al mercado un navegador con el cual Internet pasa de una fase escrita a una gráfica, lo que ayudó a popularizar esta tecnología. Más adelante surgieron otros navegadores en el mercado como el Explorer de Microsoft. A partir de entonces, el crecimiento de Internet ha sido impresionante, en enero de 1993 tan sólo había 100 sitios WWW, para enero de 1996 ya existían 90 mil. Todo este crecimiento ha sido propiciado por los fines comerciales que persiguen la mayoría de las empresas que lo

forman, de esta manera entramos a la nueva era comercial de Internet.

La difusión del Internet y su crecimiento, de carácter exponencial, han hecho de ésta un lugar idóneo para los negocios. Es el vehículo ideal para diseminar ideas, imágenes, propaganda e información de todo tipo de forma tan interactiva como se desee.

(Lic. Jorge Orozco Flores, 1998:184-199)

Como es de todos sabido, Internet es la red de redes más grande del mundo, criterios de selección de recursos electrónicos dentro de la cual existen millones de programas, artículos, bases de datos e información actualizada.

Se ha considerado a través del tiempo al Internet como el sistema internacional de comunicaciones digitales, el cual emerge de un conglomerado de miles de redes que interactúan a través de un número de protocolos comunes alrededor de todo el mundo. En ella, la información no se encuentra almacenada de manera centralizada, sino distribuida a través de redes que interactúan empleando como arquitectura el modelo cliente/servidor que provee un mayor control al usuario final en la interacción.

En sus orígenes, Internet fue diseñada como un sistema para comunicarse fácilmente pero nunca se pensó que la proliferación de los recursos electrónicos, al paso del tiempo iba a ser exponencial. Actualmente, los recursos disponibles en esta red son innumerables ya que cualquiera que tenga una conexión a Internet puede colocar un recurso nuevo en cualquier momento sin avisar a nadie. En Internet se genera diariamente mucha información y no hay control de lo que se coloca en la red, lo que ha ocasionado la existencia de un incremento desmesurado de la información, prevaleciendo aquella con un enfoque comercial.

Efectivamente, si analizamos el tipo de información que se encuentra en Internet podemos corroborar lo señalado por Gorman (1998) en el sentido de que entre los cientos de miles de recursos electrónicos que existen en Internet, únicamente alrededor de un 5 a un 6 por ciento son de valor académico.

Asimismo, un análisis llevado por Cohen (2001) sobre las características de los recursos que se añaden en Yahoo encontró que 80 por ciento de los sitios nuevos que son incorporados corresponden a sitios comerciales, páginas personales, sitios recreativos, sitios con información regional o para viajeros.

No obstante lo anterior, Internet se ha convertido en una herramienta popular utilizada por un considerable número de los estudiantes de nuestras universidades e instituciones de educación superior para localizar información que

apoye la realización de sus trabajos académicos. Con esa finalidad utilizan los denominados motores de búsqueda tales como: Yahoo, Lycos, Infoseek, Excite, Altavista, Metacrawler, Who-where, Hot-bot, Albert, entre otros.

Cada uno de ellos cuenta con una base de datos, las cuales son creadas por seres humanos y/o programas automatizados llamados "arañas" o "robots." Nicholson (1997) menciona que los motores de búsqueda pueden ser de tres tipos: directorios, de texto completo o de resúmenes. Los motores de búsqueda de tipo directorio incluyen encabezamientos de materia para la navegación los cuales generalmente son asignados por seres humanos. Ningún texto es tomado del documento o página que se indica sino que cada una de éstas es examinada y ubicada dentro de una lista jerárquica de encabezamientos de materia.

Por otro lado, la volatilidad de los recursos electrónicos es considerada como uno de los principales problemas inherentes a este tipo de información. Al respecto, Krol (1995) hace referencia a que el promedio de vida de un recurso de Internet es de aproximadamente cuatro años. Como se ha mencionado anteriormente, los recursos electrónicos que se encuentran en la red son numerosos y muchos de ellos no tienen ningún control de calidad. Asimismo, su descripción no incluye ningún elemento que indique el tipo de recurso de que se trata o cual es su contenido, lo que permitiría tomar una decisión acertada acerca de su obtención o consulta.

1.2 NACIONALES

Fue el primer país latinoamericano en conectarse a Internet, lo cual ocurrió a finales de la década pasada, en febrero de 1989, a través de los medios de acceso e interconexión de teléfonos de México, compañía mexicana que había constituido el monopolio telefónico del país hasta el once de agosto de 1996.

Los primeros enlaces de Internet en el país, que tuvieron fines exclusivamente académicos, por cierto, se establecieron en el Instituto Tecnológico de Estudios Superiores de Monterrey, el Instituto Politécnico Nacional, la Universidad de Guadalajara y la Universidad de las Américas en Puebla.

En lo que respecta a México, la historia de Internet comienza a finales de la década de los 80's. En el año de 1987, el Instituto Tecnológico y de Estudios Superiores de Monterrey, en el campus Monterrey (ITESEM) se conectó a BITNET a través de líneas conmutadas por medio de una línea privada analógica de 4 hilos a 9600 bits por segundo, en 1989 lo hizo a Internet al enlazarse por medio de la Universidad de Texas en San Antonio (UTSA), por la misma línea privada.

La Universidad Nacional Autónoma de México accedió a Internet por medio de una conexión vía satélite de 56 Kbps con el Centro Nacional de Investigación

Atmosférica de Boulder, Colorado, siendo éste el segundo nodo de Internet en México. Después se interconectaron ambas universidades mexicanas usando líneas privadas analógicas de 9600 bitsps, velocidad suficiente para proveer correo electrónico, transferencia de archivos y acceso remoto.

Poco a poco se fueron incorporando a Internet otras instituciones educativas mexicanas como son: Universidad de Chapingo en el Estado de México, el Centro de Investigación de Química Aplicada de Saltillo, el Laboratorio Nacional de Informática Avanzada de Jalapa, Veracruz, los cuales se conectaban al ITESEM para salir a Internet.

Para este entonces, en México ya existía un organismo llamado RED-MEX, formado por la academia y dirigida por una organización civil, donde se discutían las políticas, estatutos y procedimientos que habrían de regir y dirigir el camino del control de la red de comunicación de datos de México.

Tiempo más tarde, surgió otro organismo denominado MEXNET que reunía representantes legales de cada institución, el cual incluía a varias universidades de distintos lugares del país. Dicha organización, en 1992, establece una salida de 56 kbps al de Internet.

En 1993 la CONACYT se conecta a Internet mediante un enlace satelital al NCAR (Centro Nacional de Investigación Atmosférica), se establece como el primer NAP (Network Access Point), al intercambiar tráfico entre dos diferentes redes. A finales de este año en México ya se contaba con distintas redes: MEXNET, Red UNAM, Red ITESEM, RUTYC (desaparece el mismo año), BAJANET, Red total CONACYT y SIRACYT.

Fue en 1994, con la fundación de la Red Tecnológica Nacional (RTN), integrada por MEXNET y CONACYT, que se generó un enlace a 2 MEGABITSp/s.

En el mismo año, Internet se abre en el ámbito comercial en México, con lo cual se inicia una nueva era de desarrollo para nuestro país que beneficia a todas las personas, empresas o instituciones que deciden participar en el proyecto desde sus inicios, ya que hasta entonces sólo instituciones educativas y de investigación tenían acceso a la súper carretera de la información.

A finales de 1995 se crea el Centro de Información de Redes de México (NIC-México) el cual se encargó de la coordinación y administración de los recursos de Internet asignados al país, como son la administración y delegación de los nombres de dominio bajo ".mx".

En 1996, se registran cerca de 17 enlaces contratados con TELMEX para uso privado, asimismo se consolidan los principales ISP (proveedores de servicios de Internet) en el país, de los casi ya 100 ubicados a lo largo y ancho del territorio nacional.

Para el año de 1997 existen más de 150 ISP's, ubicados en los principales centros urbanos: Ciudad de México, Guadalajara, Monterrey, Chihuahua, Tijuana, Puebla, Laredo, Saltillo, Oaxaca, entre otros.

Actualmente, Internet es utilizado tanto por instituciones educativas y gubernamentales, empresas privadas y personas de todo el mundo, entre quienes se llevan a cabo intercambios constantes de información dando origen a la llamada globalización de la comunicación. Hasta el día de hoy, gracias a Internet, se puede recibir información al instante de cualquier parte del mundo, agilizando y facilitando de esta forma el proceso comunicativo a distancia. De esta manera hemos llegado a superar los obstáculos de la comunicación a través de los años, los últimos 50 años han sido de gran avance, ahora sólo queda preguntarnos

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

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

La "era de la información", impone en nuestro país, al igual que en el mundo globalizado, nuevas formas de organización, en los negocios, el mundo de la academia, los gobiernos y, cada vez más, en todas las actividades habituales a pesar de que la cultura de la informática y de la información en México se encuentran aún en sus inicios, hoy en día la tecnología de la información constituye para muchas empresas y universidades nacionales un instrumento insustituible para la realización de trabajos específicos.

El uso de la computadora como instrumento o herramienta de trabajo, según datos del INEGI, es incipiente, en 1994 sólo existían 2.2 computadoras personales por cada cien habitantes, lo que ubica a nuestro país en el lugar numero veintiocho a nivel mundial en este aspecto.

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

1.3 MICHOACÁN

En Michoacán no existe ningún tipo de antecedente del Internet o de la informática por lo cual podemos ver que aún cuando este avance ha sido de los más importantes en el mundo, no se ha tenido el cuidado de verificar cuales han sido los aspectos más relevantes dentro de este estado.

De igual forma vemos que no existe ningún tipo de legislación al respecto, ya que al no existir ninguna conciencia acerca de este fenómeno trascendental mucho menos de los efectos que puede traer consigo como son los beneficios de una comunicación más ágil y sin fronteras; y de igual forma una afectación grave de dicha información.

La información que es guardada en equipos de informática la mayoría de las veces es confidencial, por lo que vemos que en estos tiempos ya existen diversos medios de seguridad que protegen esa información contenida en estos sistemas.

Como vemos dentro de el Código Penal de Michoacán, no se encuentra legislada ninguna figura que tenga como fin el prevenir el hecho de que pueda accederse a sistemas de informática, así como que con este acceso de conozca información contenida en ellos. Llevándonos con ello a que no exista algún medio

para castigar a aquellas personas que lleguen a acceder y/o conocer la información que en ellos se contiene.

Ya que puede existir una conducta en la cual únicamente se acceda al sistema pero no se llegue a conocer esa información contenida en estos sistemas de informática, pero puede traer consigo el hecho de que se conozca información de carácter personal de la persona a la cual se esta agraviando con el acceso.

Por último solo puedo decir que durante todo el avance que han tenido los medios de comunicación, en este tiempo uno de los más importantes ha sido el Internet ya que ha permitido que exista una comunicación más rápida y sin fronteras.

Si bien es cierto vemos que uno de los países que más tiempo tiene llevándolo acabo y por lo tanto tiene el mayor avance es Estados Unidos de América, y de él se fueron desenvolviendo todos los demás.

De esta manera podemos ver lo importante que es el hecho de que exista una regulación que pueda prevenir todos aquellos perjuicios que se han venido causando a través de las redes, y que sea conocida y muchas veces divulgada la información que se contiene en estos equipos, accesando de manera ilícita a ellos y a la información que en ellos se encuentra causando un perjuicio a la persona

por violársele su derecho a la privacidad.

Lo que se busca es que el derecho realmente vaya avanzando a la par con los avances tecnológicos, ya que al no existir una norma que regule todo lo referente a los sistemas y equipos de informática, cada vez van a ir en aumento todas las conductas ilícitas que se puedan relacionar con ellas; como lo es el acceder a estos sistemas, lo que puede llevar a conocer la información que se contiene en ella y con ello cometerse un ilícito; ya que las personas no tienen seguridad de que la información que se encuentra en ellos sea protegida de tal forma que las personas que transgredan esos mecanismos de seguridad, sean castigadas por la ley penal.

Se puede lograr que estas conductas sea prevenidas y castigadas, ya sea al prevenir que aquellas personas que las realizasen ya no lo hagan pues sabrán que serán sancionadas por ello, así como que si la persona llega a cometerlo se le castigue; si nos ponemos analizar estas conductas podemos ver que realmente este es un problema que nos afecta a todos, ya que como lo mencione en líneas precedentes, tanto el uso del Internet como el de los sistemas informáticos, es elemental en la vida diaria, para todas las personas y en casi todos los trabajos ya que son medios de comunicación muy ágiles.

CAPITULO 2. CONCEPTOS GENERALES DE INFORMÁTICA

Una vez que se han analizado todos los antecedentes que existen en cuanto al Internet, así como al uso de las computadoras en las que vimos que desde tiempos muy remotos fueron utilizados para que se pudiera lograr una comunicación más ágil entre las personas, buscando con ello que se lograra el economizar, ya que es más fácil hacer uso del Internet para mandar la información necesaria, así como utilizar los sistemas de informática para trabajar.

El uso de las computadoras, así como del Internet cada vez se ha hecho más frecuente, logrando que sea elemental en la vida de todas las personas; ya que por este medio se puede transmitir información así como recibirla; pero uno de los problemas que se han desenvuelto a la par de estos instrumentos, han sido las conductas que se realizan y que pueden causar un perjuicio. Por ellos se buscará analizar aquellos conceptos que nos puedan ser útiles para comprender las conductas que posteriormente se analizaran, por poner un ejemplo podemos decir que el hacker es una figura muy importante dentro de este tema ya que por lo regular son las personas que cometen las conductas, de las cuales se busca su regulación.

Dentro de este capitulo se abarcara todos aquellos aspectos que sean de gran relevancia para el entendimiento del tema, como aquellos conceptos básicos

necesarios para comprender algunos de los temas que van a ser tocados.

Esto con la finalidad de evitar el hecho de que sean explicados nuevamente en el transcurso del trabajo que se esta realizando.

2.1 ACCESO:

Localizar, cargar en la memoria o preparar para su ejecución alguna operación.

Permiso que tiene el usuario en relación con los discos, archivos, registros y procedimientos de entrada.

2.2 CÓDIGO DE ACCESO:

Combinación única de caracteres, por lo general letras o números, utilizada en las comunicaciones como medio de identificación para tener acceso a un equipo remoto.

En una red o en un servicio en línea, suele referirse al nombre o a la

identidad del usuario y su contraseña.

2.3 INTERNET:

Red gigante que interconecta una innumerable cantidad de redes locales de computadoras.

Es la red de redes.

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

Es un medio de comunicación que tendrá un profundo efecto social.

Desde el punto de vista social es un medio de comunicación bilateral, directa y hasta el momento libre, entre los individuos; más ágil que lo que puede resultar el teléfono, ya que permite el intercambio de textos y multimedia.

Un tipo de comunicación múltiple ya que la información que se transmite

puede ser un tipo de comunicación múltiple ya que la información que se transmite puede ser a un solo individuo determinado por medio del correo electrónico o dejarla a disposición de todos en la red.

Red de datos ideada para transmitir imagen y voz.

2.4 CIBERESPACIO:

Término utilizado sobre redes de equipos informáticos en el cerebro.

Se refiere al campo colectivo de la comunicación asistida mediante equipos informáticos.

Término creado por William Gibson en su novela de ciencia ficción "Neuromancer" para describir el mundo de los ordenadores y la sociedad creado entorno a ellos.

2.5 CIBERNÉTICA:

Ciencia de la comunicación y el control.

Término acuñado para describir la ciencia de control y comunicación en animales y en máquinas. El concepto se basa en una teoría que afirma que los seres vivos se adaptan a su entorno y llevan a cabo sus propósitos a través de las reacciones a estímulos procedentes de su ámbito de relación.

2.6 INFORMÁTICA:

Neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en el año de 1962.

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

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

Tratamiento automático de la información.

2.7 COMPUTADORA:

Máquina automatizada de propósito general, integrada por los elementos de entrada, un procesador central, dispositivos de almacenamiento y elemento de salida, ello nos da la pauta para considerar sus elementos fundamentales a nivel operacional.

Máquina compuesta de elementos físicos, en su gran mayoría electrónicos, capaces de realizar una serie de trabajos a gran velocidad y con gran precisión, siempre que se le den las instrucciones adecuadas.

2.8 CORREO ELECTRONICO:

Traducción literal de 'Electronic Mail'. Sistema de mensajería informática que presenta grandes ventajas con respecto al correo tradicional. Entre ellas, la inmediatez en el envío y recepción de la información, la posibilidad de adjuntar infinidad de documentos de todo tipo (archivos de audio, de texto, imágenes) y de enviar el mensaje a varios receptores de forma simultánea.

Sistema mediante el cual un ordenador puede intercambiar mensajes con otros usuarios de ordenadores (o grupos de usuarios) a través de redes de

comunicación.

2.9 EXPLORER:

Navegador diseñado por Microsoft para su uso con Windows 95. Las versiones mejoradas están disponibles también para otros sistemas operativos.

2.10 PASSWORD:

Palabra inglesa que se traduce al español como contraseña

2.11 FIREWALL:

La llamada pared de fuego es un sistema que se coloca entre una red local e Internet.

La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala.

Además estos sistemas suelen incorporar elementos de privacidad y autentificación entre otros.

2.12 HACKER:

Se conoce con este nombre a aquellos usuarios de la Red que se infiltran en sistemas informáticos protegidos.

Por lo general, el único objetivo que motiva su actuación es dejar constancia de que han penetrado en el sistema, informando a veces de los fallos de seguridad que les han permitido entrar.

Actualmente, el término se identifica con el de pirata informático, es decir, delincuente informático que opera a través de la Red.

Aunque la diferencia es que el hacker busca entrar en el sistema y demostrar que es superior a su administrador, mientras que el pirata informático busca su propio lucro o, incluso, destrozar el sistema.

2.13 CRACKER:

Persona que se introduce sin la autorización pertinente en el ordenador de otra persona o en el sistema de redes de una institución o empresa con el fin de romper las barreras de seguridad establecidas.

Puede tener distintas finalidades. A veces, el cracker persigue su propio beneficio y, en otras ocasiones, simplemente se siente retado por el desafío que la intrusión significa ya que pone en evidencia la fragilidad de los sistemas informáticos de algunas webs de Internet.

Persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones en contraste con los hackers y suelen disponer de muchos medios para introducirse en un sistema.

La gran diferencia con el **hacker** es que éste último no realiza el acto por maldad, mientras que el cracker siempre quiere ocasionar algún tipo de daño u obtener algún tipo de contrapartida a su favor.

2.14 HACKTIVISMO:

Es la actividad que llevan a cabo los **hackers** y que se orienta a fines políticos. Sigue la ética **hacker**, y se introduce en los ordenadores de los Gobiernos que han atentado contra los Derechos Humanos.

2.15 WEB:

Servidor de información WWW.

Se utiliza también para definir el universo W W W en su conjunto y significa World Wide Web.

Sistema de información distribuido, con mecanismos de hipertexto creado por investigadores de Suiza.

Los usuarios pueden crear, editar y visualizar documentos de hipertexto. Sus clientes y servidores pueden ser accedidos fácilmente.

2.16 PROVEEDOR:

Persona o empresa que provee de los artículos necesarios para cubrir tus necesidades.

2.17 PROVEEDOR DE LA CONEXIÓN A INTERNET:

Empresa o profesional que facilita al usuario su conexión a la Red.

Su ordenador debe estar conectado permanentemente a la red y debe estar disponible las 24 horas del día y siete días a la semana para que los usuarios se puedan conectar vía telefónica.

2.18 PROVEEDOR DE CONTENIDOS:

Quien facilita información en la red de usuarios. Esta información puede ser de carácter gratuito o previo pago.

2.19 USUARIO:

Es aquella persona que se conecta a la red y en definitiva paga por sus servicios.

2.20 PROGRAMA:

Conjunto de ordenes que se dan a una computadora para realizar un proceso determinado.

2.21 SISTEMA INFORMÁTICO:

Conjunto de elementos necesarios como la computadora, terminales, impresora, etc; para la realización y exploración de aplicaciones informáticas.

2.22 HARDWARE:

Conjunto de elementos materiales que componen un sistema informático.

2.23 SOFTWARE:

Es la parte lógica que dota al equipo físico de capacidad para realizar cualquier tipo de trabajo, tiene su origen en ideas y procesos desarrollados por el elemento humano, plasmado en un soporte determinado hardware.

2.24 RED:

Campo abandonado para el intercambio de programas dado que, por lo menos en sus inicios, la mayoría de sus usuarios procedían del mundo informático en los campus universitarios.

Así pues tenemos que los conceptos descritos tienen la finalidad de poder aclarar aquellos conceptos que si bien es cierto son comunes en la vida diaria muchas veces no llegamos a comprender totalmente que es lo que significan o que es lo que realmente se denomina bajo ese nombre.

Vemos que los conceptos descritos anteriormente nos podrán ayudar a tener una mejor compresión de los términos que va a ser utilizados para realización del trabajo.

Se puede observar que dichos conceptos son muy útiles para conocer que es lo que se entiende por sistemas de informática, así como que se considera acceder a un sistemas, de igual forma se especifica que son los códigos de acceso que son utilizados generalmente cuando se encuentra navegando en Internet; por ultimo para conocer algunos de los tantos mecanismos de seguridad que son utilizados por estos sistemas. Siendo elemental para el estudio del acceso o conocimiento de la información contenida en equipos o sistemas de informática, trasgrediendo medidas de seguridad, buscando primeramente conocer que es lo que se considera un acceso, un mecanismo de seguridad, etcétera.

La mayoría de los mecanismos de seguridad que se utilizan en estos sistemas son otorgados por los proveedores de los programas, por lo que también fue importante tratarlos dentro de este capitulo.

Uno de los más importantes son los hackers ya que son las figuras principales en la comisión de estas conductas, y que la mayoría de las veces son personas profesionales en la materia; y hasta los mismos proveedores de los sistemas, ya que son los que plasman los mecanismos de seguridad y los que mejor que nadie pueden conocer su uso.

Más adelante veremos como serán utilizados y sobre que versará cada una de sus funciones para nuestro tema.

CAPITULO 3. EL DELITO

Una vez que se han analizado todos aquellos conceptos que se consideran como básicos para conocer todos aquellos factores que pueden influir en la realización del acceso ilícito a sistemas de informática, conociendo de manera general que se entiende por cada uno de ellos, con la finalidad de que más adelante se puedan comprender mejor estos factores.

Dentro de este capitulo se buscara hacer una descripción de todo lo referente al delito en general, así como sus elementos buscando se logre abordar todo lo referente al mismo, tratando de buscar la mejor forma de relacionar el delito en general con el delito informático; llegando de esta manera a conocer lo que constituirá mi propuesta.

De igual forma de abordarán quienes son los sujetos que intervienen en la realización de los mismos, y como pueden sancionarse estas conductas.

Lo que constituye la función principal de este capitulo es el buscar comprender todos aquellos elementos que constituyen un delito, para de tal forma poder analizar cuales conductas que llegan a constituir un delito informático, relacionándolas con aquellos medios de los cuales pueden hacer uso para su comisión como lo es el Internet y los sistemas de informática que si bien es cierto

han sido uno de los problemas que más relevancia ha tenido en nuestros tiempos ya que los hacker como común mente han sido denominados son delincuentes los cuales llegan a violentar nuestros derechos al violar esos medios de seguridad con la finalidad de acceder a la información o bien simplemente hacerla desaparecer.

Y con la realización del mismo llegar a comprender como se puede legislar el acceso y/o conocimiento de la información contenida en estos sistemas de informática, con la finalidad de que no se acceda ilícitamente a los mismos llegando a conocer la información de cualquier carácter que contengan en ellos.

3.1 DEFINICIÓN JURÍDICA DEL DELITO:

De acuerdo con el artículo 7º del Cogido Penal del Estado de Michoacán, "el Delito es el acto u omisión que sancionan las leyes penales."

En el campo penal la conducta comprende la acción u omisión, es decir el actuar o abstenerse de actuar.

Sebastián Soler considera que "hay acción, toda vez que en un comportamiento corporal es jurídicamente referible en alguna forma a la voluntad de un hombre". *(Soler Sebastián, 1992: 276)*

Para Sebastián soler toda acción comprende tanto la acción como la omisión por comprender tanto la conducta humana como el resultado. Pero no es lo mismo toda vez que al ejercer una acción se esta realizando una conducta o acto previsto por la ley y prohibido por la misma; pero a diferencia al llevar a cabo una omisión se encuentra en presencia de la no realización de un acto previsto por la ley y que debe cumplirse.

La acción se define como aquella actividad que realiza un sujeto, produciendo consecuencias en el mundo jurídico, produciendo una alteración o cambio en el mismo.

En sentido estricto la acción es la actividad voluntaria realizada por el sujeto, esta actividad produce un resultado existiendo un nexo causal entre la conducta y el resultado.

A dicho resultado le sigue una sanción que le otorgue la ley penal, es decir debe existir una figura delictiva la cual esta penada por la ley penal; de acuerdo a el bien jurídico que tutele.

La omisión es una inactividad que realiza el sujeto, es cuando la ley espera una conducta del individuo y este deja de hacerla.

Según Cuello Calón, la omisión es la inactividad voluntaria cuando existe el deber jurídico de obrar. De lo que resulta que al dejar de obrar se esta incumpliendo con una norma jurídica y que traerá como resultado una sanción.

3.2 DEFINICIÓN DOCTRINAL DEL DELITO

Para González Quintanilla, el Delito es un comportamiento típico, antijurídico y culpable.

Para Ignacio Villalobos, "el Delito es un acto humano típicamente antijurídico y culpable". *(Villalobos Ignacio, 1975: 650)*

De amabas definiciones señaladas anteriormente se puede desprender del análisis de las mismas el hecho de que no encuentran como parte de el delito la sanción penal lo que constituye la punibilidad en el delito, ubicándola únicamente como una figura antijurídica, la cual se encuentra prevista en la ley penal como constitutiva de algún delito y que se lleva acabo adquiriendo con ella una responsabilidad por ir en contra de la ley, pero a la cual no le recae una sanción.

Para Carrara el delito es considerado como la infracción de que la ley de un

Estado prevé, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, ya sea positivo o negativo, imputable a una persona y políticamente dañoso.

Como se puede ver de la definición dada por Carrara el delito es una conducta que la ley de un Estado prevé anteriormente a la comisión del mismo, la cual puede ser imputable a una persona ya sea por que la haya cometido por voluntad o por alguna omisión que haya tenido en el cumplimiento de alguna norma y que con ello cause un daño a la sociedad.

Edmundo Mezger en su Tratado señala que el delito es la acción típicamente antijurídica y culpable; sin embargo nuevamente deja fuera de su definición la punibilidad no considerando a esta como un elemento del delito sino como una consecuencia de la comisión del mismo. Más tarde el mismo la modifica centrando el concepto a lo siguiente: acto típicamente antijurídico y culpable, imputable a un hombre y sometido a una sanción penal.

Jiménez Asúa considera que "el delito es el acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal". *(Jiménez de Asúa Luis; 1986: 207)*

Jiménez Asúa considera que además de todas los elementos utilizados por Edmundo Mezger, también debe de incluirse en la definición las condiciones objetivas de las cuales se derivara la imposición de la pena ya que son condiciones que se van a llevar acabo por el juez al momento de imponer la pena; por lo que no lo consideramos como un elemento propiamente del delito, sino únicamente una parte determinante de la punibilidad.

De esta forma podemos sacar a conclusión que los elementos principales que integran al delito son: La conducta o ausencia de conducta, la tipicidad o atipicidad, antijuridicidad o causas de justificación, culpabilidad o inculpabilidad y la punibilidad o excusas absolutorias; de las cuales se hablara específicamente a continuación.

3.2.1 ELEMENTOS DEL DELITO

De las definiciones anteriormente citadas, nos muestran como elementos del delito según su concepción positiva y negativa las siguientes:

3.2.2.1 LA CONDUCTA

Elemento básico del delito que es la conducta, se define como el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito.

La realización de un acto voluntario, el cual trae aparejado un resultado, dicho acto puede ser de hacer una conducta o de omitir realizar aquella acción que esta prevista en la ley como obligatoria y que al omitir realizarla de manera voluntaria se llega a la realización de una conducta constitutiva de un delito.

La conducta es aquella acción u omisión prevista en la ley penal y sancionada por la misma.

Un acto, es el comportamiento humano positivo o negativo que produce un resultado. Será positivo cuando sea una acción, consistente en un hacer; y será negativo cuando sea una omisión consistente en un no hacer.

aspecto negativo de la conducta es la ausencia de la conducta, la cual abarca la ausencia de la acción o de omisión de la misma, en la realización de un ilícito.

Derivado de ello se prevé que no podrá sancionarse a aquella persona que no haya infringido la ley ya sea por no cometer el delito o por no realizar una omisión en el cumplimiento de la norma.

Buscando ejemplificar esta ausencia de conducta tenemos que el Código Penal del Estado de Michoacán señala en sus artículo 12 Fracción I que será causa excluyente de incriminación: "El violar la ley penal por fuerza física irresistible o en cualquier otro caso en que haya ausencia de voluntad del agente".

En aquellos casos en que la ley penal sea violentada por algún motivo que no comprenda la voluntad del agente no constituirá una conducta propiamente ya que no existe la voluntad por parte de la persona de realizarla.

Es cuando no hay delito por no existir la voluntad de hacerlo y que además cuenta con una causa que lo justifica.

3.2.2.2 LA TIPICIDAD

La tipicidad es la adecuación de la conducta al tipo penal previsto por la ley penal.

Se establece que para que exista una conducta considerada como delito debe de estar previamente prevista en la ley penal, ya que en el caso de no encontrarse legislado no podrá imponerse una sanción.

Para que exista un delito la ley penal señala específicamente que es lo que comprende esa figura, ósea el tipo que se realiza de una conducta penal, la cual será sancionada.

Es importante hacer la diferencia entre lo que es tipo y la tipicidad; ya que el tipo comprende lo que es la descripción que hace la ley penal respecto de una conducta considerada como contraria a derecho; mientras que la tipicidad se refiere propiamente a la conducta realizada por el sujeto que se adecua al tipo previsto.

El aspecto negativo de la tipicidad es la atipicidad la cual es la falta de adecuación de la conducta al tipo penal previsto por la ley.

Atipicidad para Luis Jiménez de Asúa es "la ausencia de tipo que trae consigo la imposibilidad de dirigir la persecución contra el autor de una conducta no descriptiva en la ley aunque sea antijurídica". *(Jiménez de Asúa Luis; 1986: 221)*

La atipicidad es la falta de de adecuación de una conducta prevista en la ley, por lo que al no encontrarse estipulada en la ley o no concordar específicamente con la conducta o tipo que esta previsto no podrá sancionársele a la persona que la cometa, ya que la misma Constitución Política de los Estados Unidos Mexicanos especifica que para poder seguir un juicio en contra de una persona tendrá que ser contra una conducta previamente establecida en la Ley, al no encontrarse esta prevista en la ley o no adecuarse exactamente al tipo previsto no podrá juzgarse ni sancionarse a la persona que la cometa.

Pero a diferencia de la atipicidad podemos decir que la falta de tipo es la falta de descripción dentro de la norma penal de una conducta o hecho.

Siendo que el tipo es la conducta que se prevé en la ley penal y la tipicidad es la adecuación de una conducta realizada por una persona al tipo penal previsto por la ley.

3.2.2.3 LA ANTIJURIDICIDAD

La antijuridicidad es un elemento positivo del delito. Cuando una conducta es considerada como antijurídica, es por ser contraria a derecho y por tanto se le

denomina delito.

La antijuridicidad es lo contrario a derecho.

Se considera que para que una conducta sea antijurídica debe de ser contraria a derecho y no solo encuadrar en el tipo penal.

Se considera que una conducta es antijurídica, siempre que la ley penal la prevea y la defina como tal, y que no se encuentre en alguna de las causas de justificación, establecidas en la ley penal.

Para Sebastián Soler "la antijuridicidad o ilicitud consiste en la relación de contradicción entre el hecho y el ordenamiento jurídico general de una sociedad". *(Soler Sebastián, 1986: 276)*

Para que la conducta de un ser humano sea delictiva, debe contravenir las normas penales, es decir, ha de ser antijurídica.

Para que una conducta sea antijurídica no basta con que encuadre en el tipo penal, sino que este prevista por la ley penal, y no se encuentre protegida por alguna causa de justificación prevista en la misma ley penal.

La causa de justificación se da cuando en un hecho presumiblemente delictuoso falta la antijuridicidad, podemos decir que no hay delito, por la existencia de una causa de justificación, es decir, que el individuo ha actuado en determinada forma sin el ánimo de transgredir las normas penales.

Como ejemplo podemos decir cuando una persona mata a otra en defensa de su vida injustamente atacada, será una causa de justificación excluyéndose de tal manera la antijuridicidad en la conducta del hombre.

Para Asúa las causas con las que excluyen la antijuridicidad de la conducta que puede subsumirse a un tipo legal, esto es que aquellos actos u omisiones que revisten aspecto de delito, figura delictiva, pero en los que falta sin embargo, el carácter de ser antijurídico, de contrarios a derecho que es el elemento más importante

Las causas de justificación son las causas excluyentes de incriminación las cuales las prevé el artículo 12 del Código Penal Federal, entre las cuales podemos encontrar por mencionar algunas a la legitima defensa.

No hay delito, cuando exista una causa que lo justifique.

3.2.2.4 LA CULPABILIDAD

El concepto de culpabilidad dependerá de la teoría que se adopte; ya que un psicológista diría que la culpabilidad consiste en el nexo psicológico que une al sujeto con la conducta o el resultado material.

Un normativista opinaría que la culpabilidad es el nexo psicológico entre el sujeto y la conducta o el resultado.

El concepto de culpabilidad de un finalista sería el afirmar que la culpabilidad es la reprochabilidad de la conducta, sin considerar el dolo como elemento de la culpabilidad, sino de la conducta.

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

Para Sebastián Soler la culpabilidad "es la que señala el límite de lo que puede ser imputado al sujeto como su obra, y además la forma de esa imputación". *(Soler Sebastián. 1992: 277)*

La culpabilidad es todo acto que puede ser imputado a un sujeto que trae consigo un resultado, el cual va en contra de de las normas jurídicas; y tendrá que

ser imputado de acuerdo a la forma en que se realizo ya sea culposamente o dolosamente.

Para Jiménez Asúa el "Dolo existe cuando se produce un resultado típicamente antijurídico, con conciencia de que se quebranta el deber, con conocimiento de las circunstancias de hecho y del curso esencial de la relación de causalidad existente entre la manifestación humana y el cambio en el mundo exterior con voluntad de realizar la acción y con representación del resultado que se quiere o ratifica". *(Jiménez de Asúa,1995: 156)*

Cuello Calón considera que el dolo es la voluntad consciente dirigida a la ejecución de un hecho que es delictuoso.

Eduardo López Betancour dice que el dolo consiste en el conocimiento de la realización de circunstancias que pertenecen al tipo, y a la voluntad o aceptación de la realización del mismo.

Por lo que el dolo es cuando se quiere realizar aquella conducta que esta prevista en la Ley o que es contraria a la misma, con la conciencia de que al realizarla se esta transgrediendo a las normas, y existiendo la voluntad de realizarla.

La culpabilidad es un hecho de resultado imprevisto y que debió de haberse previsto.

Jiménez Asúa considera que la culpa es "cuando se produce un resultado típicamente, antijurídico por la falta de previsión del deber de conocer, no solo cuando ha faltado al autor la representación del resultado que sobrevenga, sino también cuando la esperanza de que no sobrevenga ha sido fundamento decisivo de las actividades del autor que se produce son querer el resultado antijurídico y sin ratificarlo". (*Jiménez de Asúa, 1986: 230)*

Cuello Calón expresa que existe culpa cuando obrando sin intención y sin la diligencia debida se causa un resultado dañoso, previsible y penado por la ley.

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

La culpa es aquella conducta que es realizada por una persona por no tener la precaución debida para haber previsto que de realizarla podría u omitir realizarla podría constituirse una conducta tipificada en la ley como delito y que será sancionada de a cuerdo a la misma.

La culpa es una conducta que no cuenta con la voluntad de causar una consecuencia contraria a la ley, sino que por lo contrario nunca se previo que se podía concluir en la misma, por no medirse las consecuencias que esta podría traes consigo.

La diferencia entre el dolo y la culpa, es que el dolo al momento de realizarse la conducta se tiene la intención o voluntad de producir la consecuencia que trae consigo, mientras que la en la culpa no existe la voluntad de realizar esa conducta.

El aspecto negativo de la culpabilidad es la inculpabilidad.

La inculpabilidad es la ausencia de culpabilidad; significa la falta de reprochabilidad ante el derecho penal, por faltar la voluntad o el consentimiento del hecho.

3.2.2.4.1 INIMPUTABILIDAD

Tiene una relación estrecha con la culpabilidad; ya que no puede ser culpable de un delito quien no es imputable.

La diferencia entre ininputabilidad e inculpabilidad es: que el inimputable es psicológicamente incapaz; en cambio, el inculpable es completamente capaz, pero ha obrado en su favor alguna causa que excluye la culpabilidad, tal como el error esencial de hecho o la coacción sobre la voluntad.

Las causas de inculpabilidad son las circunstancias que anulan la voluntad o el conocimiento.

Para Jiménez de Asúa la imputabilidad "es imputar un hecho a un individuo, es atribuírselo hacerle sufrir las consecuencias, hacerle responsable de él, ya que del hecho es culpable". *(Jiménez Asúa, 1986: 265)*

La imputabilidad al igual que la puniblidad no se considera parte de los elementos del delito por algunos autores, ya que consideran que únicamente es un condicionante para poder determinar el carácter con el que se actuó.

El Código Penal del Estado de Michoacán en su artículo 15 señala específicamente a quienes podrá imputárseles un delito y a la letra dice:

Artículo 15.-

Es imputable la persona que en el momento de realizar la conducta descrita en la ley como delito, está en capacidad de conocer su ilicitud y de autodeterminarse en razón de tal conocimiento.

Las sanciones penales sólo podrán aplicarse a las personas imputables y las medidas de seguridad a las inimputables.

De igual forma tenemos que el aspecto negativo de la imputabilidad es inimputabilidad.

La inimputabilidad consiste en la incapacidad de querer y entender en el mundo del derecho.

Jiménez Asúa expone que la inimputabilidad "es la falta de desarrollo y salud de la mente, así como trastornos pasajeros de las facultades mentales que privan o perturban en el sujeto la facultad de conocer el deber". *(Jiménez de Asúa, 1986: 266)*

El Código Penal del Estado de Michoacán por su parte hace referencia a estas causales de inimputabilidad las cuales deberá necesariamente concurrir

para que no pueda imputarse un delito.

Artículo 16. - Son causas de inimputabilidad:

1. La condición de persona menor de dieciséis años:

2. *(DEROGADA)*

3. El trastorno mental temporal o permanente en el momento de la comisión del hecho, a no ser que el agente hubiere provocado su trastorno mental; y;

4. La sordomudez y la ceguera de nacimiento, cuando haya falta total de instrucción

La inimputabilidad son aquellas causales en las que si bien el hecho es típico y antijurídico, no se encuentra el agente en condiciones de que le pueda atribuir el acto que perpetro, por todas las causa que ya vimos que la misma ley marca.

Por lo tanto la imputabilidad implica la capacidad de ser sujeto activo del delito, ósea, no es un comportamiento propio del delito sino una referencia al

delincuente.

La inimputabilidad supone que no existe la capacidad para poder comprender que la conducta que se esta realizando es contraria a derecho por lo cual no va a poder imputársele el delito a esa persona.

3.2.2.5 LA PUNIBILIDAD

Elemento secundario del delito consistente en el merecimiento de una pena, en función o por razón de la comisión de un delito; dichas penas se encuentran contempladas por el Código penal del Estado de Michoacán.

Cuello Calón expresa que la puniblidad no es más que un elemento de la tipicidad, ya que al estar la acción culminada con una pena, viene a constituir un elemento del tipo penal previsto por las normas penales.

Como podemos ver para Cuello Calón la punibilidad no llega a constituir un elemento del delito sino más bien lo considera como parte de uno de los elementos del delito, ya que el considera que la punibilidad debe de ir acorde al delito y que al momento de realizar el tipo de un hecho que será considerado un delito, se debe de considerar la pena que se aplicara a la persona que se haga

merecedora.

Guillermo Saucer, dice que la punibilidad es el conjunto de los presupuestos normativos de la pena, para que la ley y la sentencia, de acuerdo con las exigencias de la idea del derecho.

Ignacio Villalobos, tampoco considera a la punibilidad como elemento del delito, ya que el concepto de éste no concuerda con el de la norma jurídica; una acción o una abstención humana, son penadas cuando se califican de delictuosas, pero no adquieren este carácter por que se les sanciones penalmente. Las conductas se revisten de delictuosidad por su pugna con aquellas exigencias establecidas por el Estado para la creación y conservación del orden en la vida gregaria y por ejecutarse culpablemente. Más no se pueden tildar como delitos por ser punibles.

El aspecto negativo de la punibilidad son las excusas absolutorias.

Jiménez Asúa considera que las excusas absolutorias son "las acusas que hacen que un acto típico, antijurídico, imputable a un autor y culpable, no se asocie pena algunas por razones de utilidad pública". (*Jiménez Asúa, 1986: 262)*

Como podemos ver para Jiménez Asúa las excusas absolutorias son todas las causas que una vez que están hayan concurrido en la realización del delito, el autor del mismo no podrá ser castigado con una sanción penal, ya que estas lo absuelven de culpa.

En las excusas absolutorias a pesar de existir el delito y la culpabilidad en el actor del mismo, también concurren circunstancias que le dan una modalidad especial, por la cual este sujeto no va a ser castigado.

En todas las cusas que nuestro Código Penal Prevé como excusas son circunstancias en las que no obro como parte esencial la voluntad, ni la intención de realizarlas sino que por condiciones especiales fueron llevadas acabo.

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

3.3 CLASIFICACIÓN DE LOS DELITOS

3.3.1 ATENDIENDO AL ELEMENTO INTERNO O CULPABILIDAD.

Los delitos pueden ser de acuerdo al artículo 7º del Código Penal del Estado de Michoacán:

I. Dolosos;

II. Culposos.

El delito es doloso cuando el agente quiere o acepta el resultado, o cuando éste es consecuencia necesaria de la conducta realizada.

El delito es culposo cuando habiéndose previsto el resultado, se confió en que no se produciría; cuando se causó por impericia o ineptitud".

3.3.2 ATENDIENDO A SU DURACIÓN

El Código Penal Federal hace la Clasificación de los delitos atendiendo a su duración en su artículo 8º. que a la letra dice:

Artículo 8º .- El delito es:

I- Instantáneo

II- Permanente

III- Continuado

Será instantáneo, cuando la consumación se agota en el preciso momento en que se han realizado todos los elementos constitutivos.

Es permanente cuando la consumación se prolonga durante un tiempo indeterminado.

Es continuado cuando el hecho que lo constituye se integra con la repetición de una misma acción procedente de idéntica resolución del sujeto y con violación

del mismo precepto legal, en perjuicio de la misma víctima.

3.3.3 ATENDIENDO A SU FORMA DE PERSECUCIÓN

Los delitos atendiendo a su forma de persecución se clasifican en:

1- Oficio

2- Querella necesaria

Son de oficio todos aquellos que la ley penal considera como obligatorio para la autoridad iniciar el proceso penal.

Los delitos que son perseguidos de oficio tendrán la peculiaridad de que podrán ser denunciados por cualquier persona que tenga conocimiento del mismo, sin que exista la necesidad de que sea la persona afectada quien tenga la obligación de presentarla.

El Código de Procedimientos Penales del Estado en su artículo 17 menciona que en los delitos que son perseguidos de oficio, todas aquellas personas que tengan conocimiento del mismo tendrán la obligación de presentar

la denuncia.

ARTICULO 17.- "Obligatoriedad de la denuncia.- Toda persona que tenga conocimiento de la comisión de un delito que deba perseguirse de oficio, está obligada a denunciarlo ante el Ministerio Público o sus auxiliares".

De igual forma el Código de Procedimientos Penales del Estado especifica en su articulo 15 cuando se considera necesaria la querella, y a la letra dice:

ARTICULO 15.- "Querella necesaria.- Es necesaria la querella del ofendido solamente en los casos en que así lo determinen el Código Penal u otra Ley."

Será necesaria la presentación de la querella por aquella persona que resulte afectada por la comisión del delito, en todos aquellos casos en que la el Código Penal establezca claramente la necesidad de la presentación de la misma dentro de su tipo penal.

3.4 SUJETOS DEL DELITO

Para la comisión de las conductas antisociales denominadas delitos, encontraremos a uno o varios sujetos activos como también pasivos, los cuales

deben contar con características propias como son:

3.4.1 SUJETO ACTIVO

Es necesario que el sujeto activo sea una persona física, independientemente de su sexo, edad, lugar de origen y otras características que son necesarias.

Cada tipo, señala las calidades especiales que se necesitan para ser sujeto activo.

Una persona moral o jurídica no podrá ser sujeto activo de ningún delito, cabe señalar que en ocasiones, aparentemente es la institución la que comete un delito, pero siempre habrá sido una persona física la que ideó, actuó, en todo caso ejecutó el delito.

3.4.2 SUJETO PASIVO

Cualquier individuo puede ser sujeto pasivo en un principio, sin embargo, dadas las características de cada delito, en algunos casos el propio tipo señala en que circunstancias y quien puede serlo, por ejemplo en el delito que propiamente

de esta proponiendo se encontrara que el sujeto pasivo será aquella persona propietaria de un sistema de informática en el cual se contengan sistemas de seguridad, ya que no podrá ser victima de un delito aquella persona que no tenga un sistema de informática que será el instrumento de para llevar acabo la comisión del delito.

El sujeto pasivo es la persona física o moral sobre quien recae el daño o perjuicio causado por la conducta del delincuente.

Por lo general a éste también se le llama víctima u ofendido, en cuyo caso una persona jurídica puede ser sujeto pasivo de un delito, como los delitos patrimoniales y contra la nación.

Ahora vamos a estudiar la diferencia entre el sujeto pasivo del delito y del sujeto pasivo de la conducta.

El sujeto pasivo del delito es el titular del bien jurídico tutelado que resulta perjudicado.

El sujeto pasivo de la conducta es el individuo que de manera directa recibe un daño por parte del sujeto activo, pero el daño en sentido estricto, lo recibe el titular del bien jurídico tutelado.

3.5 CONCEPTO DE DELITO INFORMÁTICO

Carlos Sarzana, en su obra Criminalista y tecnología, los crímenes por computadora comprenden, cualquier comportamiento criminógeneo en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógenea, o como mero símbolo.

Para Hilda Callegari, el delito informático es aquel que se da con la ayuda de la informática o de técnicas anexas.

Rafael Fernández Calvo, define al delito informático como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título I de la Constitución Española.

María de la Luz Lima, dice que el delito informático en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea con método, medio o fin.

El Dr. Julio Téllez Valdes, menciona dos clasificaciones del Delito Informático para efectos de conceptualización, que parte de lo típico y lo atípico.

En el concepto típico de Delitos Informáticos nos dice que "son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin".

En el concepto atípico menciona que "son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin". *(Julio Téllez, 1996: 283)*

El Departamento de Investigación de la Universidad de México, señala como delitos informáticos a "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático".

Realizando una relación entre todas las definiciones dadas podemos concluir para nuestro propio concepto que los delitos informáticos son "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal y que en su realización se valen de las computadoras como medio o fin para su comisión".

Los delitos informáticos son aquellos en los cuales existe como instrumento para la ejecución de los mismos el uso de la computadora; en el delito que se esta proponiendo su legislación el cual es el acceso ilícito a sistemas y equipos de informática, trasgrediendo medidas de seguridad; es parte de los delitos informáticos ya que se utiliza como medio de ejecución las computadoras.

Dentro de este capitulo se realizó un desarrollo sobre lo que es el delito, sus elementos, clasificaciones que se hacen en cuanto a sus elementos; así como las definiciones tanto doctrinales, como la jurídica.

En los elementos del delito se dieron las explicaciones de cómo se llegaba a constituir este, que van desde la conducta hasta la punibilidad de los mismos, en ellos dentro de estos elementos analizamos lo que era la punibilidad que si bien es cierto no es considerada como un elemento del delito por algunos autores que analizamos y podemos decir que en base a las explicaciones que ellos exponen, se puede decir que la punibilidad en realidad es una consecuencia del delito, ya que no es un condicionante para que el delito se pueda dar.

De igual forma de determino también que la impunidad tampoco es un elemento del delito, ya que esta es solo una condición de capacidad para que se pueda llegar a sancionar al agente, pero que muy a pesar de que esta no exista la comisión del delito si se da solo que no va a poder ser atribuible al sujeto activo

cómo una capacidad para poder conocer que es lo que no debe de hacer o por el contrario cual es la actitud o conducta que debe tomar.

Se llego a la clasificación de los delitos atendiendo al el tipo de comisión de los delitos que existen, forma de persecución, y sujetos que intervienen.

Se busco dar una explicación de lo que comprende el delito en general, con todos sus elementos, para poder llegar a conceptualizar lo que es el delito informático, el cual es aquella conducta antisocial en la cual se utiliza un sistema y/o equipo de informática como medio para lograr un propósito determinado.

La finalidad de este conocimiento es el de conocer como las conductas que se cometen por este medio, cada día se van acrecentando constituyéndose como delitos informáticos, ya que los medios electrónicos o computadoras son sistemas que se utilizan en la vida diaria y que se han vuelto indispensables; logrando que se llegue a buscar la manera de llegar al conocimiento de los documentos que se encuentran en estos sistemas o simplemente acceder a estos sistemas, ya sea como un reto o con alguna finalidad.

Como podemos ver en este tiempo se dan las conductas de acceder ilícitamente a los sistemas de informática, así como conocer la información contenida en los mismos es el pan de cada día, anteriormente se había hecho

mención del hecho de que existían personas las cuales las podemos considerar los sujetos activos de estos delitos, los hackers, los cuales han llevado la comisión de estas conductas de manera impune ya que no existe una legislación que tenga como fin evitar que se realicen.

Vemos que dentro de estos delitos se dan una conducta en la cual el sujeto activo del delito tiene la voluntad de realizar ese acceso encaminada a un propósito, el cual puede ser únicamente acceder al sistema trasgrediéndose los mecanismos de seguridad, o realizar este acceso con la finalidad de conocer los datos que se contienen en este sistema.

No existe un tipo penal ya que estas conductas no se encuentran previstas en el nuestra ley penal, llevando con ello a que no se puedan castigar a estos sujetos por no existir una figura prevista con anterioridad y que tenga como fin evitar que se lleguen a cometer estos delitos; lo que nos lleva a ver que en nuestro estado existe una atipicidad respecto de estas conductas.

El delito informático es un delito que es antijurídico ya que es contrario a las normas de derecho. ya que en su comisión se violentad diversos derechos y libertades que tienen las personas; propiamente refiriéndonos a nuestra propuesta el llegar a acceder a un sistema informático y con ello llegar a conocer los datos o información contenida en ellos, constituye una violación al derecho a la privacidad,

así como a la intimidad.

Los sujetos que lleguen a cometer estos delitos tendrán que ser culpables, ósea responsables por las consecuencias que puedan cuasar con la comisión del delito, pero para que esta culpabilidad pueda establecerse debe existir previamente la adecuación de la conducta la cual esta causando un perjuicio, y con ello se le pueda fincar una responsabilidad al sujeto activo.

Por último la punibilidad de el delito sería el merecimiento de una pena por el agravio que pueda causarse a la victima del delito, buscando con ello, que no quede impune y evitar que se sigan cometiendo este tipo de conductas.

Lo que se buscó en la realización de este capitulo es entender de una manera más clara que es el delito en general y los elementos con que cuenta para de esta manera llegar posteriormente al estudio del delito informático, en el cual podemos encontrar la figura que se propone, de igual forma poder entender los capítulos que siguen de una manera más amplia.

CAPITULO 4. LEGISLACIÓN COMPARADA

En el capitulo anterior se estudio todo lo referente al delito, con la finalidad de saber que es lo que es un delito, los elementos que lo integran estudiando cada uno de ellos para llegar a conocer que es lo que integran los tipos penales.

La finalidad del conocimiento de estos elementos, así como de los sujetos que intervienen en ellos es para entender que es lo que prevé las legislaciones de otros países y como lo prevén.

Dentro de este capitulo veremos las formas en que los diversos países ha elaborado sus legislaciones para evitar y regular los diferentes tipos de delitos que se pueden llegar a cometer utilizando las computadoras.

Al realizar el estudio de estas legislaciones se abarcara únicamente lo referente al tema que nos concierne que es el acceso ilícito a sistemas y equipos de informática, transgrediendo medidas de seguridad.

También se verán los tipos de agravantes que se le pueden dar a este delito, ya sea por tener conocimientos o por que se divulgue dicha información contenida en el equipo al cual se este accediendo, o que la persona que la este

realizando sea un experto en la materia.

Las legislaciones que se estudiaran son legislaciones que se encuentran en vigor, que fueron creadas con el fin de prevenir estos delitos, y que en la actualidad siguen vigentes en estos países.

4.1 LEGISLACIÓN INTERNACIONAL

En este apartado se estudiara las legislaciones de los países que se han considerado más avanzados en cuanto a la prevención de los delitos informáticos.

4.1.1 ARGENTINA

Argentina cuenta con una Ley de Delitos Informáticos la cual entro en vigor el 21 de Noviembre del 2001, en la cual contempla varias figuras como son:

ACCESO ILEGÍTIMO INFORMÁTICO.-

Artículo 1:

Será reprimido con pena de 1,500 a 30,000 pesos, si no resultare un delito

más severamente penado, el que ilegítimamente y a sabiendas accediere, por cualquier medio, a un sistema o dato informático de carácter privado o público de acceso restringido.

La pena será de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información accedida ilegítimamente.

La fundamentación que Argentina utilizo para la creación de esta figura delictiva es lo que se explicara a continuación.

Se ha optado por incorporar esta figura básica en la que por acceso se entiende todo ingreso no consentido, ilegítimo y a sabiendas, a un sistema o dato informático.

Es una figura base porque su aplicación se restringe a aquellos supuestos en que no media intención fraudulenta ni voluntad de dañar, limitándose la acción a acceder a un sistema o dato informático que se sabe privado o público de acceso restringido, y del cual no se posee autorización así se concluye que están excluidos de la figura aquellos accesos permitidos por el propietario u otro tenedor legítimo del sistema.

Considerando apropiada la fijación de una pena de multa, ya que se trata

de una figura básica que generalmente opera como antesala de conductas más graves, por lo que no amerita pena privativa de la libertad, la que por la naturaleza del injusto habría de ser de muy corta duración.

DAÑO INFORMÁTICO.-

Artículo 2:

Será reprimido con prisión de un mes a tres años, siempre que el hecho no constituya un delito más severamente penado, el que ilegítimamente y a sabiendas, alterare de cualquier forma, destruyere, inutilizare, suprimiere o hiciere inaccesible, o de cualquier modo y por cualquier medio, dañare un sistema o dato informático.

El fundamento de esta figura es que busca en cuanto a la protección propiamente dicha de la integridad y disponibilidad de un sistema o dato informático, el artículo propuesto tiene por objeto llenar el vacío que presenta el tipo penal de daño

Dentro de la misma cuenta con un artículo en el cual contempla las disposiciones.

Al incluir los sistemas y datos informáticos como objeto de delito de daño se busca penalizar todo ataque, borrado, destrucción o alteración intencional de dichos bienes intangibles. Asimismo, la incriminación tiende también a proteger a los usuarios contra los virus informáticos, caballos de Troya, gusanos, cáncer routines, bombas lógicas y otras amenazas similares.

ARTÍCULO 6:

1) A los fines de la presente ley se entenderá por sistema informático todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.

2) A los fines de la presente ley se entenderá por dato informático o información, toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.

3) En todos los casos de los artículos anteriores, si el autor de la conducta se tratare del responsable de la custodia, operación, mantenimiento o seguridad

de un sistema o dato informático, la pena se elevará un tercio del máximo y la mitad del mínimo, no pudiendo superar, en ninguno de los casos, los veinticinco años de prisión.

Esta legislación quizás es una del las más completas al especificar como deben de darse los delitos de este orden, ya que especifica claramente que se entiende por cada una de las figuras que se va a prever dentro del tipo al cual se esta haciendo referencia.

Argentina es uno de los países que ha tomado importancia respecto del hecho de que existan personas que causen una alteración a los documentos que se encuentren dentro de un sistema informático, o del simple hecho de que los conozcan ya que muchos de ellos constituyen información confidencial para la persona y de los cuales se pueden derivar muchos delitos más.

4.1.2 ALEMANIA

A partir del 1 de Agosto de 1986, la fecha en que entro en vigor fue el 22 de enero de 1977 con la cual se adopto la Segunda Ley contra la Criminalidad Económica, la cual fue reformada el 20 de diciembre de 1990 y entro en vigor el 1 de junio de 1991 en la que se contemplan entre otras:

ALTERACIÓN DE DATOS ARTÍCULO 303 a:

Es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.

SABOTAJE INFORMÁTICO ARTÍCULO 303 b:

Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

Alemania es uno de los países que prevé los delitos pero que en realidad le hace falta especificar de manera más precisa que es lo que comprenderá la figura especificando claramente que es lo que se entiende por alteración o inutilización de datos.

4.1.3 AUSTRIA

Ley de reforma del Código Penal del 22 de diciembre de 1987, misma fecha en que entro en vigor dicha ley contempla los siguientes delitos:

DESTRUCCIÓN DE DATOS:

Artículo 126:

No solo datos personales sino también los no personales y los programas.

ESTAFA INFORMÁTICA:

Artículo 148:

Se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos.

Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

4.1.4 FRANCIA

La Ley 88/19 que entro en vigor el 5 de enero de 1988 sobre el fraude informático contempla:

Acceso fraudulento a un sistema de elaboración de datos.

Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

ARTÍCULO 462-3:

Que se realice una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamientos automatizado.

ARTÍCULO 462-4:

Que se realice 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 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.

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.

4.1.5 ESPAÑA

Dentro del código penal Español en lo referente a delitos informático encontramos los siguientes artículos relacionados con nuestro tema.

Ley-Orgánica 10/1995, de 23 de Noviembre/ BOE número 281, la cual entro en vigor el 24 de Noviembre de 1995.

ARTÍCULO 197

1- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

2- Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de

prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento. realizare la conducta descrita en el párrafo anterior.

3- Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

4- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

5- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión.

ARTÍCULO 201

1- Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3- El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta.

España es también un país que especifica claramente cuales son los tipos de conductas, que tipo de acceso o figura de tiene que dar, pero también hace especificaciones claras sobre cuales serán aquellos agravantes que se le puedan dar al delito, sobre el tipo de personas que pueden intervenir y que de acuerdo a esto van a ser sancionados.

Prevé como se va a tener que llevar acabo la denuncia del delito para que este pueda ser perseguido y castigado.

4.1.6 CHILE

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

Según esta ley, 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.

ARTÍCULO 1:

Cometa 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 3:

Al que realice una conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

4.2 NACIONALES

Dentro de este apartado estudiaremos lo referente a las legislaciones nacionales que prevén esta conducta, a nivel Federales y así mismo a nivel Estatal buscando encontrar las legislaciones que prevén estos tipos de delitos y buscando su explicación.

4.2.1 FEDERAL

El ordenamiento que nos toca estudiar es el Código Penal Federal que al momento es un Código el cual se encuentra vigente a la fecha y prevé la conducta del acceso ilícito a sistemas y equipos de informática de la siguiente forma:

El Código Penal Federal en su Libro Segundo, Titulo Noveno Revelación de Secretos y acceso ilícito a sistemas y equipos de informática; en su Capitulo

Noveno contempla:

ARTÍCULO 211 BIS 1:

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

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

4.2.2 ESTATAL

4.2.2.1 CÓDIGO PENAL DEL ESTADO DE SINALOA

El Código Penal de Sinaloa fue reformado en su totalidad abrogando el anterior, el 15 de noviembre de 1986, teniendo su ultima reforma el 28 de marzo del 2003.

Este código contempla específicamente un capitulo para los delitos informáticos, siendo el único Código Penal Estatal que lo contempla, dentro de su TITULO DÉCIMO Delitos contra el patrimonio, CAPITULO V denominado DELITO INFORMÁTICO, en el cual en su artículo 217 contempla lo siguiente:

Artículo 217:

Comete el delito informático la persona que dolosamente y sin derecho:

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

2- 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 del delito informático se le impondrá una pena de seis meses a dos años de prisión o de noventa a trescientos días de multa.

Cabe señalar que el Congreso del Estado de Sinaloa busca regular los delitos informáticos, y los encuadra buscando proteger como bien jurídico tutelado el patrimonio pero si bien es cierto no únicamente se vulnera ese bien jurídico sino también el derecho a la intimidad.

4.2.2.2 CÓDIGO PENAL DEL ESTADO DE MICHOACÁN

Dentro del Código Penal del Estado de Michoacán no se encuentra regulado el delito informático de ninguna forma ni tutelando ningún bien jurídico; es necesario que exista una conciencia sobre la necesidad de legislar estos delitos creando un tipo penal adecuado a estas conductas antisociales, siendo un freno a la comisión de los mismos, ya que pueden llegar a causar detrimentos en la sociedad y una violación al derecho a la intimidad que todos tenemos.

Los legisladores del Estado se han mantenido al margen sobre esta situación sin darse cuenta que es un problema que afecta a toda la sociedad y que va creciendo día con día.

A manera de conclusión sobre la legislación comparada podemos ver que los países mas adelantados o primer mundistas son los que realmente han

buscado una solución al problema de los delitos informáticos.

De lo cual podemos decir que Argentina es uno de los países que regula el acceso ilícito a sistemas y equipos de informática o datos informáticos de carácter publico y privado.

Es esta figura contempla que el hecho de que las personas tengan conocimiento de que están accediendo ilícitamente, como penalidad de impone de 1,500 a 30,000 pesos, siempre que no resulte del mismo un delito más grave.

Incrementa la pena si estos datos se llegaren a divulgar imponiéndole de 1 mes a dos años de prisión, poniéndole en este caso la pena de prisión cuando el simple acceso únicamente le impone el pago de una multa.

Argentina es un país que considera al acceso ilícito como una figura base para la comisión de más delitos, por lo que no le impone pena de prisión sino que esta se derivara de aquella conducta que resulte como consecuencia de este acceso.

Es una legislación que prevé claramente que se entiende por cada una de las figuras que contempla en su tipo penal, desarrollándolas claramente a fin de que no puedan crear una confusión. Prevé de igual forma el daño informático,

ósea toda aquella destrucción que se pueda causar tanto en los datos como en los sistemas.

Por su parte Alemania únicamente prevé la alteración de datos, castigando la consumación del delito y la tentativa del mismo; de igual forma prevé el sabotaje informático en el que se de la alteración del sistema de datos que contengan los sistemas informáticos. Sin tener el cuidado de prever claramente cuales serán las sanciones para estos delitos.

Austria dentro de su código penal prevé diversos delitos entre los cuales se encuentran la destrucción de datos, la estafa informática, y el hecho de que estos delitos sean cometidos por personas que sean profesionales en la materia.

Sin embargo al igual que Alemania no se detiene a prever como conducta ilícita el hecho de que se acceda al sistema, ya que como Argentina bien lo dice el simple acceso es la base para la comisión de los demás delitos.

Francia por su lado prevé el acceso fraudulento como figura de estos delitos, en los cuales prevé diversas conductas y sanciones tanto para el acceso, así como que resulte del mismo la supresión o modificación de los datos contenidos en el sistema.

También el que se impida el funcionamiento del sistema, que se introduzcan datos dentro de este sistema. Al simple acceso lo contempla al igual que Argentina y aumentara la pena prevista en el caso de que se mantenga dentro de este sistema.

El Código Penal Español es quizás el más completo en cuanto a que prevé exactamente la figuras que se van a legislar, las personas que se encuentran autorizadas para presentar la denuncia, cuales serán causas para que la pena del delito aumente, como en el caso de que se divulgue el conocimiento que se tiene por personas que s encuentren encargados de los sistemas de informática; y los casos en que la acción penal se extinguirá como es el que se otorgue el perdón al ofendido.

La penalidad señalada para el simple acceso a los sistemas, que modifique, altere o utilice en perjuicio del titular, se le impondrá prisión de uno a cuatro años y multa de doce a veinticuatro meses. Señala como un tipo de agravante el que ese acceso o alteración sea realizado por las personas encargadas de estos sistemas imponiéndole una pena de tres a cinco años y si se llegan a difundir estos datos se impondrá la pena en su mitad superior.

Chile por su parte dentro de su ley contra delitos informáticos, prevé la destrucción o inutilización de los datos contenidos en la computadora, así como

que se ingresen virus en ella, previendo como sanción de un año y medio a cinco años de prisión.

Así podemos decir que los países que se analizaron en este capitulo son en los que se encuentran legislados los delitos informáticos, sin embargo tienen algunas diferencia entre las cuales podemos encontrar que Argentina es un país en el que sus legisladores tuvieron el exacto cuidado de legislar el acceso ilícito a los sistemas, pero para ello señalo expresamente que se entiende por acceso, sistema, etc., Francia por su parte también realizo esta legislación de manera precisa, sin embargo por su parte España es un país que ha realizado de manera más precisa como debian de darse este tipo de delitos, quienes son quienes va a tener que presentar la denuncia, cuando se extinguirá la acción penal y muchas otras cosas necesarias para poder llevar a cabo la persecución y sanción de estos delitos.

Respecto de las legislaciones de Alemania y Austria, Austria fue un país que se baso en la legislación Alemana para realizar su legislación por lo cual se encuentran para mi gusto con el mismo problema ya que ninguno prevé el accedo ilícito, sino el fraude, alteración o inutilización de datos, pero sin ver que para que estas conductas se puedan dar tendrá que darse un acceso previo violentando los mecanismos de seguridad.

Si hacemos una comparación con el Código Penal Federal, vemos que este prevé como conductas la modificación, destrucción o pérdida imponiéndoles una sanción de 6 meses a 2 años de prisión y de cien a trescientos días de multa; y para el que conozca o copie esta información se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días de multa. Vemos que prevé diversa conducta que en su mayoría las contemplan, España, Francia y Alemania, pero la diferencia es que les da una penalidad menor y no prevé el modo en que esta podrán ser denunciadas como lo especifica España, ni señala que se entenderá por cada una de las conductas que prevé en la misma.

Argentina es el único país que no le otorga pena de prisión al sujeto activo de esta conducta ya que considera que es el acceso la base para la comisión de otros delitos de los cuales se desprenderá la sanción de pena de prisión.

Por último el Código Penal del Estado de Sinaloa, prevé el uso o alteración de una base de datos con la finalidad de defraudar u obtener dinero, bienes o información, concentrándose a la protección del patrimonio ya que es en este capitulo en el que lo contempla, otorgándoles una pena de seis meses a dos años de prisión o de noventa a trescientos días de multa; de igual forma contempla diversas figuras que contemplan los demás países pero su forma de castigar con pena de prisión es casi la misma que en Código Penal Federal.

Respecto de los demás países le da un enfoque diferente ya que la mayoría lo prevé como una violación a la intimidad de las personas, y Sinaloa como una afectación al patrimonio y su penalidad al igual que el Código Penal Federal es menor a la de los otros países exceptuando a Argentina.

Vemos que en la Republica Mexicana se han regulado estos delitos a nivel federal como lo pudimos apreciar en el Código Penal Federal; pero en materia local el único estado que ha hecho conciencia de este problema es el Estado de Sinaloa, pero lo hace tutelando únicámente el patrimonio sin tomar en cuenta el derecho a la intimida.

Por lo que a nosotros corresponde solo me queda decir que los Legisladores del Estado de Michoacán se han abstenido de buscar soluciones a este problema, siendo que es un problema que a todos nos afecta y que no se pueden mantener al margen por que el derecho debe de ir creciendo al parejo de los avances tecnológicos y no lo han hecho.

CAPITULO 5. ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA EN EL CÓDIGO PENAL DEL ESTADO DE MICHOACÁN

El acceso se puede dar cuando una persona utilizando una computadora y haciendo el uso del Internet. se introduce a un sistema de informática, usando diversos códigos por medio de los cuales transgreden los mecanismos de seguridad por medio de los cuales se encuentran protegidos estos sistemas y los programas, así como la información que se contienen en ellos; logrando con ello tener conocimiento de la información contenida en los mismos, la cual puede ser de carácter privado y personal, para el dueño del sistema, comprendiendo desde conversaciones personales. archivos en los cuales se contienen información confidencial de trabajo o archivos personales.

Este tipo de conductas se pueden dar navegando en Internet y que sin darte cuenta una persona se encuentra tratando de descifrar aquellas contraseñas que sirven como mecanismo de seguridad de tu computadora, ello con la finalidad de acceder únicamente y poder controlar tu computadora por medio de la que ellos estén utilizando, buscando o sin buscar conocer algún dato contenido en ella.

Estas conductas se dan en el entendido de que la persona sobre la cual

esta recayendo el acceso y conocimiento de la información no ha otorgado su autorización para que sea conocida. Los mecanismos de seguridad que protegen a estos sistemas son diversos programas por medio de los cuales se introducen contraseñas o passwod con la finalidad de establecer códigos de carácter personal para que no pueda accederse libremente al sistema y conocer lo que en el se contiene.

Sin embargo en Michoacán se ven continuamente estas figuras ya que se tiene como medio de trabajo la computadora, convirtiéndonos muchas veces en victimas de este delito; en el cual no puede ser sancionada la persona que lo cometa ya que Michoacán no cuenta con un legislación por medio de la cual pueda sancionarse a la persona; a pesar de que muy a menudo se dan estas conductas la legislación penal del Estado no hace referencia alguna sobre algún tipo de delito por medio del cual pueda sancionarse esta conducta.

Vemos que acceder significa que se cuenta con un permiso del propietario para hacer uso de los archivos, registros y procedimientos de entrada o códigos de acceso a un sistema de informática.

Mientras que el conocer información es el cuando por medio del acceso a un sistema se logra averiguar la naturaleza, calidades y relaciones de las cosas. Un mecanismo de seguridad comprende todo aquel código contenido en un

programa con el fin de evitar que este pueda ser conocido por sujetos que no cuentan con autorización para ello, protegiendo tanto la información como al, equipo en el cual se contienen; información referente a archivos personales como pueden ser conversaciones, trabajos escritos, manifestaciones o conceptos en un formato teniendo un carácter privado, para los particulares.

Como vemos esta conducta es muy común ya que en estos tiempos se da por medio de las personas llamadas hackers los cuales son sujetos que hacen uso de la red que se infiltran en sistemas informáticos protegidos, mientras que los Crackers son las personas que ya buscan introducirse sin autorización al ordenador de otra persona con el fin de romper las barreras establecidas y conocer lo que en él se contiene.

El acceso ilícito a sistemas y equipos de informática transgrediendo medidas de seguridad, es aquel en el que mediante el uso ilegitimo de passwod se logra la entrada a un sistema informático sin la autorización del propietario, lo cual conlleva muchas veces el conocimiento de la información contenida dentro de estos sistemas. Logrando dentro del uso ilegitimo de estas contraseñas transgredir esos mecanismos de seguridad que son instalados en los sistemas de informática con la finalidad de que no puedan conocerse los datos e informaciones que se contengan en los mismos.

Sin embargo estos sistemas llegan a ser violentados por personas que tienen un cierto conocimiento en la materia de informática, así como por aquellos que son considerados profesionales en la materia.

Los que comenten este tipo de conductas son personas que muchas veces no buscan en la comisión de los mismos lograr un beneficio, sino que simplemente intentan buscar los medios de probar sus habilidades accesando al sistema o a la información de más personas con la finalidad de conocerla, con cualquier finalidad; resultando perjudicial, ya que en la mayoría de la información que se encuentra en estos sistemas es de carácter confidencial, violentándose de esta forma su derecho a la intimidad, sin embargo hay personas que si lo hacen buscando su beneficio.

No ha sido imposible conocer la verdadera magnitud de estos delitos, ya que la mayor parte no son descubiertos o denunciados a las autoridades responsables, ya que no existe en nuestro estado algún tipo penal el cual lo prevea y sancione como delito, dejando desprotegidas a las víctimas de estos delitos.

Por lo que resulta que estas conductas no pueden ser sancionadas ya que los legisladores del estado no han tenido la debida conciencia de preverlas como delitos en el Código Penal del Estado, dando como resultado que al no existir uno

de los elementos del delito el cual es la tipicidad; entendiéndose como tal la adecuación que se realiza de la conducta a un tipo penal previsto en la ley, no existe el delito.

Para que una conducta sea considerada como delito debe de existir en la ley penal una figura, la cual conocemos como tipo que especifique de manera concreta que es lo que comprende esa figura.

Como vemos al no existir esta conducta del acceso ilícito a sistemas y equipos de informática trasgrediendo medidas de seguridad, tipificado en la ley penal, no puede sancionarse al sujeto que la cometa, siendo que la mayoría de las veces esta conductas conlleva el conocimiento de los datos contenidos en ellos, tanto el acceso como el conocimiento no pueden ser sancionados por la ley penal ya que nuestro estado no se prevé esta conducta como delictiva.

Lo que se propone es que se legisle el acceso ilícito a sistemas y equipos de informática, transgrediendo medidas de seguridad, como conductas delictivas por un lado que se sancione al que sin autorización acceda o conozca información protegida por algún mecanismo de seguridad.

Teniendo de esta manera que son dos las conductas propuestas, por un lado el simple acceso al sistema de informática, el cual se encuentre protegido por

mecanismos de seguridad, los cuales van a ser violentados para lograr acceder al mismo, siendo esto una conducta realizada por personas que tienen conocimientos en informática, ya que para poder llegar a descifrar los códigos de las contraseñas deben existir ciertos conocimientos o aptitudes en la materia; el acceso se puede dar de diversas formas, una de ellas es hacer uso del Internet y por medio de el llegar al conocimiento de la contraseña llegando a tener un control sobre el equipo; y la otra es cuando la persona se encuentra en presencia del equipo y busca acceder a el bajo cualquier fin.

Por otro lado que se prevea el conocimiento que se pueda tener de la información contenida en los mismos, ya que esta conducta se realiza una vez que se ha logrado acceder al sistema, pero la diferencia es que para que se de esta conducta conlleva la intención de conocer esa información, con cualquier propósito.

La información que se contenga dentro de esos sistema no tiene por que se conocida por nadie, ya que todos tenemos derecho a la privacidad, y muchas veces el conocimiento de esta información puede traer consigo consecuencias para el titular de la misma. De igual forma se pueden realizar diverso delitos derivados de ese conocimiento.

Las ventajas que se encontrarían con la legislación de estas conductas será el que pueda protegerse toda aquella información que se encuentre contenida en los sistemas, con la finalidad de proteger el derecho a la privacidad que tenemos todos, ya que con la realización de estas conductas puede causarse un agravio a la persona a la cual pertenecen.

En segundo termino será el proteger la seguridad que se busca al implementar mecanismos de seguridad en los sistemas, ya que por ese motivo se implementan los mismos en estos equipos de informática; teniendo consigo una forma de proteger para que derivado de estas conductas se puedan llegar a realizar más delitos, teniendo plena seguridad de que tu información así como tu sistema se encuentra protegido; logrando evitar que las personas que las cometen sigan realizando este tipos de conductas, ya que nos e considera que tengan algún propósito elemental para realizarlas.

Las desventajas que encontramos en relación a la legislación de estas conductas es que para crear esta legislación debe de existir un conocimiento previo por las autoridades tanto técnico en la materia de informática, como en lo legal; ya que si no se conoce de la materia, difícilmente se podrán aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular.

Se considera que uno de los problemas que más afecta a los legisladores en el Estado es la falta de preparación tanto de ellos como por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte del individuo de denunciar este tipo de ilícitos ya que no conocen el modo de realizarlo.

Una de la cosas que más influyen para no legislar a este respecto es que no existe una debido presupuesto para que puedan ser perseguidos estos delitos ya que se puede apreciar que los que cometen este tipo de ilícitos, son personas con conocimientos sobre la informática y cibernética, los cuales, se encuentran en lugares estratégicos o con facilidad para poder acceder a información de carácter delicado, la cuales pueden ser personas en lo particular, violentando de esta forma el derecho a la privacidad que tienen las personas, la cual, por la falta de una ley aplicable al caso concreto, no es denunciada quedando impune estos tipos de conductas antisociales.

Considerándose por tal motivo que las autoridades de la materia no se encuentran en condiciones idóneas para llegar al conocimiento de estos delitos, pues no cuentan ni con los medios y con los conocimientos necesarios para poder identificarlos.

Considerándose como bien jurídico tutelado la protección del derecho a la privacidad, la cual se encuentra violentada al acceder los sujetos a sus sistemas conociendo para ello los códigos puestos en las contraseñas, y de igual forma llegar al conocimiento de la información privada y de carácter personal de los particulares a los cuales afecten con su conducta.

Como pena se le podría imponer de tres meses a un año de prisión y de cincuenta a ciento cincuenta días de multa. Se le podrá imponer una sanción más alta si el sujeto activo que realizo la conducta es un profesional en la materia. El motivo de la sanción es con la finalidad de que las personas que cometen este tipo de ilícitos sufran una pena y reparen el daño que puedan cuasar al violentar ese derecho de privacidad que todos tenemos. Por lo que en la pena que se propone no es un pena alternativa, ya que prevé la pena de prisión y junto con ella una sanción pecuniaria.

De igual forma el Código Penal Federa Prevé el delito del acceso ilícito a sistemas y equipos de informática pero en el considera diversas conductas como son: en el Artículo 211 bis 1, al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por mecanismo de seguridad; y otra modalidad es al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por mecanismos de seguridad; de lo cual vemos claramente

que este Código prevé diversas modalidades de la conducta como lo es la destrucción, modificación o perdida de la información, y que esa información se conozca o copie; por lo que refiere a nuestra propuesta únicamente se prevén dos modalidades que son el acceso a sistemas y el conocimiento de la información contenida en ellos, transgrediendo medidas de seguridad; ya que realmente las demás modalidades que son contempladas por el Código Federal pueden ser resultados de las conductas que yo propongo, pudiéndose encuadrar en diversos delitos los cuales ya se encuentran previstos en el Código Penal del Estado.

En Código Penal Federal le impone a esta conducta como sanción, que la persona que resulte responsable del conocimiento de información sin autorización del titular, de tres meses a un año de prisión y de cincuenta a ciento cincuenta días de multa.

Como se ve a pesar de que en materia federal si se legislan diversas conductas, no prevé el simple acceso. auque el titulo del capitulo II se denomine Acceso ilícito a sistemas y equipos de informática; no contempla el simple acceso como conducta que se castigue por la ley penal, siendo una de las figuras que en este trabajo se busca que queden reguladas en el Código Penal del Estado.

Respecto a las legislaciones estudiadas se puede tomar comc base para la legislación de estas conducta, en lo previsto por Argentina. contempla el acceso

ilícito a sistemas y equipos de informática, como una figura base para la comisión de diversos delitos que de ellos pueden resultar, pero adicionando el conocimiento de la información, hacer una definición como la que realiza Argentina respecto de lo que se entenderá por sistema informático, datos informáticos, medidas de seguridad etc.

En cuanto a Alemania el hecho de que también se castigue la tentativa, de Australia el que se contemplen sanciones para quienes cometen este hecho utilizando su profesión; Francia sancionar tanto el acceso como el que la persona se mantenga en él y por ultimo de España el hecho de que se especifique claramente como deberá de presentarse la denuncia, quienes están autorizados para hacerlo y de que forma se extinguirá la acción penal; por considerar que es lo más elemental para crear este tipo penal.

Sinaloa por su parte es el único estado que regula los delitos informáticos de tal forma que debe de ser un ejemplo para Michoacán el que los legisladores de este estado se hayan preocupado por proteger los sistemas informáticos y los datos que en ellos se contengan; no estando de acuerdo en que únicamente se proteja el patrimonio en los mismos, ya que este tipo de conductas violenta en primer lugar la privacidad de las personas.

Considero que en Michoacán no se ha llegado a legislar en cuanto a esta materia por la falta de conocimiento de los efectos que pueden tener este tipo de conductas y los delitos que con ellas se pueden llegar a realizar; sin embargo un factor determinante en esto es la falta de conciencia y preparación de los legisladores en cuanto a esta materia para poder juzgar, de manera certera las consecuencias de estos actos.

El legislador no se ha dado cuenta de que no solo el derecho en genral es el que tiene que ir avanzando de acuerdo a las necesidades de cada tiempo, ya que debe de ir por delante de los cambios que existan y sino es posible por lo menos a la par con la finalidad de evitar que conductas como estas queden sin ningún castigo, y las personas las puedan cometer a su antojo; siendo aun más necesario que el derecho penal vaya siempre a la vanguardia ya que de ellos depende que no se sigan cometiendo conductas que afecten a los particulares a los cuales se les debe de otorgar una seguridad plena.

Como vemos en este caso y en especifico en esta materia penal la informática le ha ganado en desarrollo a nuestra legislación estatal, ya que parece que no se dan cuenta de que cada día este problema va en aumento.

Por lo cual existe la necesidad imperante de que estas conductas queden tipificadas como un delito, puesto que el bien jurídico que acostumbra protegerse

con la contraseña es lo suficientemente importante para que el daño producido sea grave; más aun cuando este tipo de información sea de carácter personal y que pueda causarse un perjuicio a la persona a la cual pertenezcan los mismos.

En nuestro país ninguna ley penal Estatal contempla los delitos informáticos, con exclusividad del Estado de Sinaloa, por lo que este problema es preocupante pues se esta teniendo un retrazo enorme a comparación de los avances tecnológicos que se van dando día con día, pues la ley penal tiene como objetivo el prever situaciones que puedan llegar a presentarse buscando al manera de evitarlas, logrando tipificar aquella conducta para que al momento en que se realice pueda ser sancionada; ya que como lo comentamos en conductas anteriores no puede sancionarse a una persona si la ley no prevé la conducta la cual se este realizando la cual deberá estar previamente prevista.

Tenemos que crearnos una conciencia del problema por el que estamos atravesando y que el derecho penal no esta avanzando de manera eficaz para evitar se sigan violentando derechos.

CONCLUSIONES

1ª- Después del estudio realizado dentro de este trabajo se llegó a la conclusión de que es necesario regular el acceso ilícito a sistemas y equipos de informática como delito en nuestro Estado.

2ª - Consecuentemente que se agregue un tipo penal, a nuestro Código Penal del Estado ya que no se encuentra previsto como delito.

3ª- Del estudio realizado a diversos países, como son Francia, Argentina, España, Alemania, Chile, es necesario prever la conducta ya que debemos prevenir que se sigan realizando, ya que la mayoría de estas legislaciones ya lo contemplan como delito.

4ª- Las legislaciones nacionales lo contemplan, pero dentro de las Estatales únicamente el Estado de Sinaloa, siendo necesario que sea previsto por nuestro Estado a fin de que puedan ser sancionadas las personas que realicen este tipo de conductas.

5ª- Por último específicamente en nuestro trabajo se llega a la conclusión de que es necesario que se legisle tanto el acceso al sistema transgrediendo

medidas de seguridad, así como el conocimiento de los datos contenidos en el sistema.

PROPUESTA

Lo que yo propongo que se regule en Código Penal de Estado de Michoacán es **"legislar el acceso ilícito a sistemas y equipos de informática transgrediendo medidas de seguridad"**.

De lo cual se puede decir que cometerá el delito aquella persona que sin autorización acceda o conozca información protegida por algún mecanismo de seguridad.

Como sujeto activo se tendrá a aquella persona que acceda o conozca la información protegida por algún mecanismo de seguridad, contenida en un equipo o sistema de informática, sin el consentimiento del propietario.

Agravando esta figura el hecho de que la persona que cuente con conocimientos profesionales en la materia considerándose como experto en ella. constituyendo con ellos una agravante al delito.

El sujeto pasivo será aquella persona física, a la cual se le haya violentado su derecho a la privacidad.

La penalidad que yo propongo es que se le impongan de 3 meses a un año de prisión y multa de cincuenta a ciento cincuenta días, siempre que el sujeto activo no tengan conocimientos profesionales en la materia.

Sin considerar que estos puedan ser cometido de manera imprudencial, ya que es una conducta que se realiza con plena voluntad de realizarla; ya que debe de llegarse a transgredir esos mecanismos de seguridad y para ellos descifrar determinadas contraseñas.

La manera de presentar la denuncia tendrá que ser por querella de parte ofendida ya que México no cuenta con los medio para realizar la identificación de estos sujetos por otro medio.

BIBLIOGRAFÍA

CARRANCÁ y TRUJILLO, Raúl (1995)

"Derecho Penal Mexicano"

Editorial Porrúa

México, D.F.

GONZÁLEZ QUINTANILLA, José Arturo (1993)

"Derecho Penal Mexicano"

Editorial Porrúa, S.A.

México 1993

GONZÁLEZ DE LA VEGA, Francisco (1996)

"Derecho Penal Mexicano"

Editorial Porrúa. S.A.

México.

JIMÉNEZ DE ASUA, Luis (1995)

"Lecciones De Derecho Penal"

Editorial Episa

México, D.F.

JIMÉNEZ ASÚA, Luis (1986)

"La Ley y el Delito"

Editorial Hermes

México, D.F.

OROZCO FLORES, Jorge (1998)

"Anuario de ABZ, 1997"

Editorial ABZ

México, D.F

SOLER, Sebastián (1992)

"Derecho Penal Argentino"

Editorial TEA

Buenos Aires, Argentina.

TÉLLEZ VALDES,Julio (1996)

"Derecho Informático"

Editorial Mc Graw Hill

México, Segunda Edición

VILLALOBOS, Ignacio (1975)

"Derecho Penal Mexicano"

Editorial Porrúa, S.A.

México, 1975

CÓDIGO PENAL DEL ESTADO DE MICHOACÁN

Cuadernos Michoacanos de Derecho

Editorial ABZ

México, D.F. del año de 1998

CÓDIGO DE PROCEDIMIENTOS PENALES DEL ESTADO DE MICHOACÁN

Cuadernos Michoacanos de Derecho

Editorial ABZ

México, D.F. del año 1998

CÓDIGO PENAL FEDERAL

Cuadernos Michoacanos de Derecho

Editorial ABZ

México, D.F. del año de 2000

CÓDIGO PENAL PARA EL ESTADO DE SINALOA

www.ordenjuridico.gob

DICCIONARIO DE INFORMÁTICA

Pws.prserv.net/esinet.migcc/diccionarios/

WWW.edata.es/Enciclop.htm/

WWW.Delitosinformaticos.com

WWW.tribunalmmm.gob.mx