"Victimas del delito a través del internet"

Autor: Ma. Soledad Zaragoza Yácuta

Tesis presentada para obtener el título de:

Lic. en Derecho

Nombre del asesor:

Lic. Mónica Adriana Figueroa Bejar

UNIVERSIDAD VASCO DE QUIROGA

FACULTAD DE DERECHO

“VÌCTIMAS DEL DELITO, A TRAVÈS DEL INTERNET”

TESIS

Que para obtener el título de
LICENCIADO EN DERECHO

Presenta
MA. SOLEDAD ZARAGOZA YÁCUTA

Asesor
LIC. MÓNICA ADRIANA FIGUEROA BÉJAR

REVOE NUMERO 990803 **CLAVE 16PSU0044K**

DEDICATORIA

Con profundo amor y agradecimiento a Dios, que con amor me ha conducido y me ha guiado por el camino de la vida y durante mis años de estudios me abrió el camino poniendo a mi alcance todos los medios para lograr mi meta, así como a tantas personas con las cuales me di cuenta que él se hacia presente.

Con agradecimiento y amor a mis padres Salvador Zaragoza Vázquez y Ma. del Carmen Yacuta Paredes, quienes antepusieron a su propio bienestar para dotar de felicidad a sus hijos, dándonos lo necesario a base de sacrificios, con el bendito propósito de vernos realizados.

Con cariño, respeto y agradecimiento a mis hermanos quienes me incitaron a no desistir y de igual forma a la Magistrada Licenciada Ma. de los Ángeles Rusiles Gracián, a quien debo la determinación de realizar este trabajo.

Con cariño y gratitud a los presbíteros Javier Cortez y Eduardo Corral quienes me ayudaron en momentos difíciles para poder continuar.

Al señor Jesús Gracián a quien le agradezco profundamente su preocupación y apoyo para hacer fructífera mi carrera.

A mis valiosas amistades que oraron por mi y me apoyaron.

Mi reconocimiento y afecto para la licenciada Mónica Adriana Figueroa Béjar, la cual me incito en este trabajo, con sus conocimientos y experiencias.

A la Universidad Vasco de Quiroga, así como al Ingeniero Leonardo González Tafolla, directivos y maestros, quienes con sus conocimientos y dedicación nos aconsejaron e instruyeron a lo largo de mi carrera.

A mis queridos compañeros con quienes compartíamos agradables experiencias a lo largo de esta maravillosa experiencia que significo haber concluido mis estudios profesionales.

A todos….¡¡ Mil gracias !!

I N D I C E

CAPÍTULO VI

"LA NO REGULACIÓN SOBRE EL USO DE INTERNET EN MÉXICO"

CAPITULO VII

"EL DERECHO PENAL EN MICHOACÁN FRENTE AL USO DEL INTERNET COMO INSTRUMENTO DEL DELITO"

CAPITULO I

PARTE GENERAL DEL DERECHO PENAL

1.1. DEL DERECHO EN GENERAL

El derecho tiene como finalidad encauzar la conducta humana para hacer posible la vida gregaria; definamos pues como "un conjunto de normas que rigen la conducta externa de los hombres en sociedad, las cuales pueden imponerse a sus destinatarios mediante el empleo de la fuerza de que dispone el estado".[1]

Así pues entiéndase que el derecho no es sino la sistematización del ejercicio del poder coactivo del estado, mas indudablemente tal sistematización inspirase en ideas del mas alto valor ético y cultural para realizar su fin primordial, de carácter mediato: la paz y seguridad social.

1.2. NECESIDAD DEL DERECHO PENAL

Todos los intereses que el derecho intenta proteger son de importancia incalculable; sin embargo, de entre ellos hay algunos cuya tutela debe de ser asegurada a toda costa, por ser fundamentales en determinado tiempo y lugar para garantizar la supervivencia misma del orden social. Para lograr tal fin, el estado esta naturalmente, facultado y obligado a la vez, a valerse de los adecuados, originándose así la necesidad y justificación del Derecho Penal que, por su naturaleza esencialmente punitiva, es capaz de crear y conservar el orden social.

[1] FERNANDO CASTELLANOS; Lineamientos elementales de derecho penal Página 17.

1.3. EL DERECHO PENAL, EVOLUCION HISTORICA

Desde que la sociedad existe -desde las primeras agrupaciones humanas-, el hombre ha conocido el fenómeno de la criminalidad. Esta se manifiesta en todas las sociedades.

Constituye uno de los aspectos constantes de la vida social, hasta el punto que hoy no se considera la criminalidad como un fenómeno anormal del grupo social, sino como algo connatural a toda sociedad organizada, siendo sólo lo anormal los bruscos crecimientos o decrecimientos de las tasas de delito. Con base a ello, se han señalado como características del fenómeno criminal su permanencia y su actualidad.

El manejo que en forma común han transmitido los juristas de la historia del Derecho Penal es la siguiente: Venganza Privada; Venganza Divina; Venganza Pública; Defensa del Poder Absoluto; Período Humanitario y Etapa Científica[2].

1.3.1. VENGANZA PRIVADA.- En esta etapa fue el impulso de la defensa o la venganza *ratio essendi* (razón de ser) de todas las actividades provocadas por un ataque injusto. Durante esta época, la función punitiva la ejercían los particulares; pues cada particular, cada familia y cada grupo se protege y se hace justicia por sí mismo, sin embargo, debido a los excesos cometidos por los ofendidos al realizar su "venganza", surgió lo que se conoce como la Ley del Talión, que no fue otra cosa, sino una medida moderadora, pues sólo se le reconocía al ofendido el derecho de causar un mal de igual intensidad al sufrido.

Fue poco después que nació la compensación, mediante la cual se autorizaba para que ofendido y ofensor, nombrasen representantes que moderaran los reclamos recíprocos y acordaran la cantidad del castigo.

[2] Idem. Pág.31.

1.3.2. VENGANZA DIVINA. Al lado del período conocido como venganza privada, se gestó dentro de organizaciones sociales más cultas, el principio teocrático y éste vino a convertirse en fundamento del derecho penal, pues no se castigaba al culpable para satisfacer al ofendido, sino para que aquél expiase la ofensa causada a Dios con su delito. En general, esta época fue manejada por la clase sacerdotal.

1.3.3. VENGANZA PÚBLICA. Durante esta etapa, se empieza a hacer distinción entre delitos privados y públicos, según el hecho lesione de manera directa los intereses de los particulares o el orden público.

Es entonces cuando aparece la etapa llamada "venganza pública" o "concepción política"; los tribunales juzgan en nombre de la colectividad. Este fue una inmensa época, de propósitos retributivos y a lo sumo intimidantes, con fines de prevención general, en que se aspiraba a utilizar al delincuente en provecho del Estado (minas, galeras).

1.3.4. DEFENSA DEL PODER ABSOLUTO. En este período, el motivo para prohibir o para castigar no fue ni la ofensa al individuo, ni la ofensa a la divinidad; fue la ofensa a la majestad soberana, y la voluntad soberana, que imponía el castigo, al tornarse autócrata, encontró su razón en sí misma, mediante un círculo vicioso. Las penas no tuvieron otra medida que el capricho o el temor de los gobernantes, o la necesidad de consolidar con sangre un cetro empleado como azote de la nación.

1.3.5. PERIODO HUMANITARIO. Nació como reacción a la excesiva crueldad imperante en la aplicación de penas. Dentro de esta corriente, se pugna por la exclusión de suplicios y crueldades innecesarios, se propone la certeza contra las atrocidades de las penas, se preconiza la peligrosidad del delincuente como punto de mira para la determinación de las sanciones aplicables y se urge por una legalidad de los delitos y de las penas.

1.3.6. ETAPA CIENTIFICA. En esta etapa, el delincuente es el objeto de la máxima preocupación científica de la justicia. El delito es una manifestación de la personalidad del delincuente y hay que readaptar a éste a la sociedad corrigiendo sus inclinaciones viciosas. Tal corrección es el pivote sobre el cual gira este nuevo período.

La pena como sufrimiento carece de sentido; lo que importa es su eficacia, dado aquel fin. Las ciencias criminológicas vinieron a iluminar el problema hasta su fondo y a caracterizar el nuevo período en el que la personalidad compleja del sujeto es lo que se destaca en el primer término del panorama penal.

1.4. DEFINICION DERECHO PENAL

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

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

Así y de acuerdo a lo estimado por Ignacio Villalobos, en su obra "Derecho Penal Mexicano", define al Derecho Penal como "aquella rama del Derecho Público Interno, cuyas disposiciones tienden a mantener el orden político-social de una comunidad, combatiendo por medio de penas y otras medidas adecuadas aquellas conductas que le dañan o ponen en peligro”.

El Derecho Penal en sentido subjetivo, es el atributo de la soberanía por el cual a todo Estado corresponde reprimir los delitos por medio de las penas; en tanto que objetivamente se forma por el conjunto de normas y de disposiciones que reglamentan el ejercicio de ese atributo:

El Estado, como organización política de la Sociedad, tiene como fines primordiales la creación y el mantenimiento del orden jurídico; por tanto, su esencia misma supone el uso de los medios adecuados para tal fin.

Define al Derecho Penal José Arturo González Quintanilla, en su obra intitulada "Derecho Penal Mexicano", de la siguiente forma: " El Derecho Penal es el poder punitivo del Estado, constituyendo, desde luego, la expresión más enérgica del poder. Mediante este fenómeno se establecen los delitos y las penas como su legítima consecuencia"[3].

Los representantes y órganos correspondientes del Estado captan los valores medios que se requieren para la convivencia en común de la colectividad; así también, llevan a cabo la imposición de los valores propios que aseguran la subsistencia y desarrollo del Estado como tal, incorporando los de mayor envergadura en el Código o Leyes Penales.

Entre las diversas concepciones del Derecho Penal, Jiménez de Asúa citando a varios autores, nos menciona: "Hay definiciones subjetivas en que se alude al fundamento del derecho de castigar, considerándolo como "la ciencia que funda y determina el ejercicio del poder punitivo del Estado". En su sentido objetivo lo define como: " conjunto de normas que regulan el Derecho Punitivo"[4],.El Derecho Penal, es el complejo de las normas del derecho positivo destinadas a la definición de los delitos y fijación de las sanciones; así como a las instituciones para aplicarlo y regularlo (Tribunales, Agencias del Ministerio Público, Penitenciarías, etc)

[3] José Arturo González Quintanilla; Derecho Penal Mexicano; pag.67.
[4] Jiménez Asúa; Derecho Penal Mexicano; pag.178.

1.5. CONCEPCION MODERNA DEL DERECHO PENAL.

En la evolución de lo que hoy conocemos como Derecho Penal, tuvo que pasar a través de diferentes etapas, las cuales se hicieron referencia en párrafos precedentes; de dicho desarrollo se formaron las "Escuelas Penales", las cuales como lo menciona "González Quintanilla" en su obra "Derecho Penal Mexicano", “son el cuerpo orgánico de las concepciones contrapuestas sobre la legitimidad del derecho penal, sobre la naturaleza el delito y sobre el fin de las sanciones"[5].Así, antes del siglo XVIII, sólo existían opiniones o elucubraciones sobre el delito, la pena, su fundamento y su fin, y no fue sino hasta 1764, al margen de las meras especulaciones filosóficas, con fines políticos, funcionales y pragmáticos, que surge a la luz del libro de "Beccaria", lo que en el contenido primordialmente implicaba una "ardiente acusación contra la barbarie del Derecho Penal del antiguo régimen".

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

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

2.- El método es deductivo y especulativo.

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

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

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

[5] Ibidem. Pag. 102

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

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

Posteriormente, le cedió el paso a la Escuela Positiva, la cual de manera preponderante, en esta rama del pensamiento, se toma en cuenta la personalidad del reo como criterio determinante en las disposiciones y las finalidades del Derecho Penal.

Las directrices conceptual-básicas de la Escuela Positiva se pueden resumir de la siguiente manera:

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

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

3.- El método es el inductivo, experimental.

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

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

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

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

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

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

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

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

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

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

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

- Teoría del Funcionalismo Político Criminal.- Después de las consecuencias de la Segunda Guerra Mundial, se pronunció el interés de incorporar el respeto a los Derechos Humanos dentro de la legislación mundial.

A la vez, esta situación se reflejó en el campo de la ley penal, en una tendencia que frecuentemente, apuntada como orientación político criminal, significó la necesidad de entender el contenido de la propia ley penal en relación con la realidad social.

Es decir, de entender que el Derecho tiene un contenido social y que esa realidad social, no solamente tiene que ser regulada, sino entendida y atendida por el Derecho, como consecuencia de los fines de la seguridad jurídica para la

convivencia, sobre la base de protección a los bienes jurídicos de los miembros de la comunidad.

Uno de los principales sostenedores de éste teoría, Claus Roxin, señala, que el análisis del Derecho Penal exige tomar en cuenta sus fines; son los fines de política criminal del derecho los que deben dar la luz para explicar y para determinar la existencia del delito; la responsabilidad del autor y tercero para determinar la aplicación de la pena en base, precisamente a sus fines de política criminal. En México, después de tener bastante tiempo adoptada la teoría causalista en el Derecho Penal, se tomó la doctrina finalista, la cual se encuentra plasmada en la mayoría de nuestras legislaciones penales de las entidades que conforman la República Mexicana, así como en nuestra propia Constitución. De acuerdo a lo anterior, el Código Penal del Estado de Michoacán sufrió un retroceso en el avance del derecho penal, ya que mencionaba *el cuerpo del delito* en el artículo 16 Constitucional, y retomaba nuevamente la teoría causalista, para tener por demostrado el cuerpo del delito (esto antes de la reforma al Código Penal del Estado de 6 de marzo del 2008); ahora el texto jurídico referido cita lo siguiente: “el interés es que se sancione con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participo en su comisión”, circunstancia que impide desarrollar la legislación penal en sus ámbitos, toda vez que el finalismo proclama el resultado y el fin buscado por el sujeto, para tener por demostrado si éste actúo dolosa o culposamente; o bien, no es responsable del resultado de la acción; al avance que se tenía en el ámbito del Derecho Penal se destacaba, al tener el creador de la norma y del Derecho Penal, dudas respecto al finalismo, no obstante que éste, haya sido adoptado por la mayoría de las legislaciones de habla hispana y del Derecho Escrito.

CAPITULO II

“EL DELITO”

El delito en el derecho penal, “*es la acción u omisión ilícita y culpable expresamente descrita por la ley bajo la amenaza de una pena o sanción criminal*”.[6]

2.1 EL DELITO: DEFINICION LEGAL Y DOCTRINARIA

La anterior definición del concepto de delito como ente jurídico, derivado de los extremos exigidos por la ley para tener una acción u omisión por criminalmente punible, difiere por supuesto, del concepto de delito que puedan eventualmente utilizar las ciencias de la conducta o la sociología. Así, es distinto, p.e., del implicado al hablarse de la lucha contra el delito, en que se alude manifiestamente el fenómeno social de la delincuencia o criminalidad.

Nada tiene que ver tampoco este concepto jurídico con el delito natural, elaborado por los positivistas en el intento de fijar el contenido material del delito en todas las sociedades y todos los tiempos. Los juristas han seguido tratando, sin embargo, de precisar las características sustanciales que una determinada legislación ha tenido en cuenta para incluir una acción u omisión en el elenco de los hechos punibles, esfuerzo que difícilmente puede arrojar resultados claros, debido a que esa selección proviene de un juicio valorativo basado, en la naturaleza y entidad del bien jurídico protegido, ora en el carácter irreparable de la lesión inferida a él, en las características especialmente odiosas de la forma de conducta incriminada, y , las demás veces, en la concurrencia de más de uno de los factores señalados o de todos ellos.Definición legal del Delito: de acuerdo con el artículo 7° del Código Penal del Estado de Michoacàn, "el Delito es el acto u omisión que sancionan las leyes penales".

[6] Diccionario Jurídico de la UNAM, tomo D-H, pag. 1305

La palabra "delito", deriva del supino *delictum* del verbo *delinquiere*, a su vez compuesto de linquere, dejar y el prefijo de, en la connotación peyorativa, se toma como *linquere viam* o *rectam viam*: dejar o abandonar el buen camino"[7].

Para González Quintanilla el Delito "es un comportamiento típico, antijurídico y culpable"[8],.

Segùn el autor Ignacio Villalobos el Delito "es un acto humano típicamente antijurídico y culpable"[9],.

De acuerdo a Rafael de Pina Vara el Delito "es un acto u omisión constitutivo de una infracción de la ley penal" [10].

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

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

b) un dato de orden subjetivo, el que expresado en sentido llano se reduce a la normalidad mental, normalidad que comprende la capacidad de querer y comprender "el significado de la acción".

[7] Tena Ramírez, Diccionario de Derecho, pag.87.
[8] González Quintanilla; Derecho Penal. Pag. 65.

[9] Idem. Ignacio Villalobos; pag. 78.

[10] Pina Vara Rafael; Derecho Penal Mexicano;

2.2 ELEMENTOS DEL DELITO

El Delito tiene diversos elementos que conforman un todo. Para Maurach el delito es una acción típicamente antijurídica, atribuible; para Berling es la acción típica, antijurídica, culpable, sometida a una adecuada sanción penal y que llena las condiciones objetivas de penalidad; Max Ernesto Mayer define al delito como acontecimiento típico, antijurídico e imputable; Eduardo Mezger afirma que el delito es una acción típicamente antijurídica y culpable; para Jiménez de Asúa es un acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad imputable a un hombre y sometido a una sanción penal[11].

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

POSITIVOS	*NEGATIVOS*
Conducta	Ausencia de conducta
Antijuricidad	**Causas de justificación**
Imputabilidad	**inimputabilidad**
Culpabilidad	**inculpabilidad**
Condicionalidad objetiva	**Falta de condiciones objetivas**
Punibilidad	**Excusas absolutorias**

De acuerdo a nuestro Derecho Positivo Mexicano, el Código Penal para el Estado de Michoacán, en su artículo 7º, define al delito como el "acto u omisión que sancionan las leyes penales", así la conducta o hecho que se obtiene de este artículo y del núcleo respectivo de cada tipo o descripción legal.

[11] Comentarios que se encuentran en el Diccionario Jurídico de la UNAM, en el Tomo D-H.

La tipicidad se presentará cuando exista una adecuación de dicha conducta a alguno de los tipos descritos en el Código Penal de estado de Michoacán; la antijuridicidad, esta existe cuando el sujeto no esté protegido por una causa de licitud descrita en el artículo 16 del Código Penal. La imputabilidad se presenta cuando concurre la capacidad de obrar en el Derecho Penal, es decir, que no se presente la causa de inimputabilidad descrita en el mismo ordenamiento legal. Habrá culpabilidad de acuerdo a los artículos 7 de nuestra ley penal. La punibilidad existe en el artículo 17 del Código Penal de nuestro Estado y se dará cuando no se presentan las excusas absolutorias descritas por nuestro Derecho Positivo (federal). Las condiciones objetivas de punibilidad se presentan cuando al definir la infracción punible se establecen requisitos constantes, pero aparecen variables de acuerdo a cada tipo penal; pueden o no presentarse.

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

Ahora, entraremos al estudio de cada uno de los elementos que componen al delito:

2.2.1. LA CONDUCTA

La conducta es el primer elemento básico del delito, y se define como el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito.

“Lo que significa que sólo los seres humanos pueden cometer conductas positivas o negativas, ya sea una actividad o inactividad respectivamente”[12].

[12] Ibidem. Castellanos Tena. Pag. 126-156.

Es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito porque tiene una finalidad al realizarse la acción u omisión. La conducta puede ser de acción o de omisión, y esta última se subdivide en omisión simple y comisión por omisión.

La conducta tiene tres elementos:

1) un acto positivo o negativo (acción u omisión).

2) un resultado.

3) una relación de causalidad entre el acto y el resultado.

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

Positivo será una acción, que consiste en una actividad, en un hacer; mientras la omisión es una inactividad, es cuando la ley espera una conducta de un individuo y éste deja de hacerla. Delito de Acción. La acción se define como aquella actividad que realiza el sujeto, produciendo consecuencias en el mundo jurídico, en dicha acción debe de darse un movimiento por parte del sujeto, de esta manera, la conducta de acción tiene tres elementos:

a) movimiento;

b) resultado;

c) relación de causalidad.

La acción en sentido estricto, es la actividad voluntaria realizada por el sujeto, consta de un elemento físico y de un elemento psíquico, el primero es el movimiento y el segundo la voluntad del sujeto, esta actividad voluntaria produce un resultado y existe un nexo causal entre la conducta y el resultado.

Dicho resultado de la acción debe ser sancionado por la ley penal, es decir, deberá configurar un delito descrito y penado en la ley, será intrascendente que lesione intereses jurídicos protegidos por la ley o sólo los ponga en peligro según el tipo penal.

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

Así pues, la omisión, dice Cuello Calón, es "la inactividad voluntaria cuando existe el deber jurídico de obrar"[13].

La omisión tiene cuatro elementos:

a) Manifestación de la voluntad.

b) Una conducta pasiva.

c) Deber jurídico de obrar.

d) Resultado típico jurídico.

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

En los delitos de simple omisión, se viola una norma preceptiva penal, mientras en los de comisión por omisión se viola una norma preceptiva penal o de otra rama del derecho y una norma prohibitiva penal.

[13] Ibidem. Cuello Calón. Pag. 76.

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

En los delitos de omisión simple, se sanciona la omisión y en los de comisión por omisión, no se sanciona la omisión en sí, sino el resultado producido.

Ahora bien, el aspecto negativo de la conducta es la ausencia de conducta, la cual abarca la ausencia de acción o de omisión de la misma, en la realización de un ilícito. Nuestro Derecho Positivo Mexicano, en el artículo 15 del Código Penal Federal, en su fracción primera, determina como causa de exclusión del delito: "el hecho se realice sin intervención de la voluntad del agente", esto es la afirmación de que no puede constituir una conducta delictiva cuando no se presenta la voluntad del agente. El artículo 12 del Código Penal del Estado, menciona como causas excluyentes de incriminación, en su facción I. "el violar la ley penal por fuerza física irresistible o cuando haya ausencia de voluntad del agente…".

2.2.2 LA TIPICIDAD

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

Se debe tener cuidado de no confundir la tipicidad con tipo, la primera se refiere a la conducta, y el segundo pertenece a la ley, a la descripción o hipótesis plasmada por el legislador sobre un hecho ilícito, es la fórmula legal a la que se debe adecuar la conducta para la existencia de un delito.

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

El aspecto negativo de la tipicidad es la atipicidad. La atipicidad es la falta de adecuación de la conducta al tipo penal. Es importante diferenciar la atipicidad de la falta de tipo, siendo que en el segundo caso, no existe descripción de la conducta o hecho, en la norma penal[14].

2.2.3. LA ANTIJURICIDAD

La antijuricidad la podemos considerar como un elemento positivo del delito, es decir, cuando una conducta es antijurídica, es considerada como delito. Para que la conducta de un ser humano sea delictiva, debe contravenir las normas penales, es decir, ha de ser antijurídica.

La antijuricidad es lo contrario a Derecho, por lo tanto, no basta que la conducta encuadre en el tipo penal, se necesita que esta conducta sea antijurídica, considerando como tal, a toda aquella definida por la ley, no protegida por causas de justificación, establecidas de manera expresa en la misma. La causa de justificación, es cuando un hecho presumiblemente delictuoso falta la antijuricidad, podemos decir: no hay delito, por la existencia de una causa de justificación, es decir, el individuo ha actuado en determinada forma sin el ánimo de transgredir las normas penales.

"Así, si un hombre ha matado a otro, en defensa de su vida injustamente atacada, estará en una causa de justificación, excluyéndose la antijuricidad en la conducta del homicida"[15].

[14] Ididem. Castellanos Tena. Pág. 125-134.
[15] Ibidem. Castellanos. Pág. 176-189.

2.2.4. LA CULPABILIDAD

El concepto de la culpabilidad, dependerá de la teoría que se adopte, pues no será igual el de un psicologista, el de un normativista o el de un finalista.

Así, el primero diría, la culpabilidad consiste en el nexo psicológico que une al sujeto con la conducta o el resultado material, y el segundo, en el nexo psicológico entre el sujeto y la conducta o el resultado material, reprochable, y el tercero, afirmaría, que la culpabilidad es la reprochabilidad de la conducta, sin considerar el dolo como elemento de la culpabilidad, sino de la conducta. La culpabilidad en la tesis finalista se reduce a la reprochabilidad y a diferencia de la teoría normativa el dolo y la culpa no son elementos de la culpabilidad porque son contenido del tipo.

La culpabilidad es por lo tanto, responsabilidad, apartándose consecuentemente de los normativistas mantienen el dolo y la culpa en la culpabilidad, constituyendo como se afirma por un sector un mixtum compositum, de cosas no pueden mezclarse.

“El concepto de culpabilidad como tercer aspecto del delito y de acuerdo a la definición anterior, nos señala cuatro importantes elementos que la conforman y son: una ley, una acción, un contraste entre esta acción y esta ley, y el conocimiento de esta situación, según lo manifestó Maggiore"[16].

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

2.2.5. LA PUNIBILIDAD

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

[16] Ibidem. Pág. 245-255.

Cuello Calón considera que “la punibilidad no es más que un elemento de la tipicidad, pues el hecho de estar la acción conminada con una pena, constituye un elemento del tipo delictivo”[17],.

Guillermo Saucer dice que la punibilidad "es el conjunto de los presupuestos normativos de la pena, para la ley y la sentencia, de acuerdo con las exigencias de la Idea del Derecho"[18].

Por su parte Ignacio Villalobos, tampoco considera a la punibilidad como elemento del delito, ya que el concepto de éste no concuerda con el de la norma jurídica: " una acción o una abstención humana son penadas cuando se les califica de delictuosas, pero no adquieren este carácter porque se les sancione penalmente” [19].

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

El aspecto negativo de la punibilidad se llama excusa absolutoria. Jiménez de Asúa dice “que son excusas absolutorias las causas que hacen que a un acto típico, antijurídico, imputable a un autor y culpable, no se asocie pena alguna por razones de utilidad pública"[20].

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

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

[17] Idem. Pag. 92.
[18] Comentarios que realiza Cuello Cálon, en las mismas paginas referidas en el pie de pagina anterior.
[19] Referencia anterior.
[20] Idem. Pag. 109.

2.2.6. LA IMPUTABILIDAD.

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

El aspecto negativo de la imputabilidad es la inimputabilidad, consistente en la incapacidad de querer y entender en el mundo del Derecho. Son aquellas causas en las que si bien el hecho es típico y antijurídico, no se encuentra el agente en condiciones de que se le pueda atribuir el acto que perpetró. Por lo tanto, ésta implica la capacidad de ser sujeto activo del delito, o sea, no es un comportamiento propio del delito. La imputabilidad no es mencionada, por tratarse de una referencia al delincuente, no al delito.

En el Código Penal del Estado, se encuentra contemplada la imputabilidad en el artículo 15, así como también en el artículo 16 menciona las causas de inimputabilidad.

2.3 FORMAS DE COMISION DE LOS DELITOS

Como se ha venido mencionando en los capítulos anteriores, el artículo 7° del Código Penal del Estado de Michoacán, aduce: "Delito es el acto u omisión que sancionan las leyes penales.

Los delitos pueden ser:

I. Dolosos;
II. II. Culposo.

El delito es doloso cuando el agente quiere o acepta el resultado, o cuando éste es consecuencia necesaria de la conducta realizada. El delito es culposo cuando habiéndose previsto el resultado, se confió en que no se produciría; cuando se causó por impericia o ineptitud".

El dolo y la culpa, son especies o formas de culpabilidad de acuerdo al psicologismo. El dolo para Cuello Calón es: "la voluntad consciente dirigida a la ejecución de un hecho que es delictuoso".

Eduardo López Betancourt, menciona al dolo: " consistente en el conocimiento de la realización de circunstancias que pertenecen al tipo, y voluntad o aceptación de realización del mismo"[21].

La culpa, es la segunda forma de culpabilidad, con base en el psicologismo. Cuello Calón, expresa: "existe culpa cuando obrando sin intención y sin la diligencia debida se causa un resultado dañoso, previsible y penado por la ley"[22]. Carrara, por su parte, expuso que la culpa es una voluntaria omisión de diligencia, donde se calculan las consecuencias posibles y previsibles del mismo hecho"[23].

De lo anterior se concluye que de las definiciones formales ofrecidas surgen tanto el núcleo de la infracción como sus caracteres:

El mero pensamiento no es susceptible de castigo (*cogitationis nemo patitur*). Para que haya delito es, pues, necesario, en primer término, que la voluntad humana se manifieste extremadamente en una acción o en la omisión de una acción. Es frecuente abrazar la acción y la omisión bajo el común concepto de una conducta, base y centro del delito, sin la cual este es inconcebible.

Aunque esa conducta no puede por si misma, ser extinguida, aparece en cuanto conducta delictiva, es decir, en cuanto delito, dotada de ciertos caracteres que, para los efectos del análisis, se estudian por separado. Estos caracteres son la tipicidad, la ilicitud o antijuricidad y la culpabilidad.

La acción y omisión deben de deben de ser típicas, ello es, conformarse a una descripción de la conducta delictiva hecha previamente por la ley (tipicidad).

[21] LOPEZ BETANCOURT, Eduardo; Derecho Penal Mexicano; pág. 98.
[22] Ibidem. Pag.107.
[23] Ibidem. Pag. 107.

Esta descripción es el tipo, medio de que el derecho se vale, en la parte especial de los códigos penales o de las leyes penales independientes, para individualizar las conductas punibles.

La tipicidad de la acción pues, no se da con la acción u omisión no se da cuando el hecho acontecido falta alguno de los elementos objetivos de tipo o todos ellos, cuando por error irreversible de tipo desaparece el dolo sin dejar un remanente culposo y cuando está ausente alguno de los demás elementos subjetivos requeridos por el tipo, en su caso.

Las acciones u omisiones típicas deben, en seguida, para constituir delito, ser antijurídicas, esto es, hallarse en contradicción con el derecho.

Tal ocurre cuando no existen en el ordenamiento jurídico, tomado en conjunto, preceptos que autoricen o permitan la conducta de que se trata, autorizaciones o permisos que reciben el nombre de causas de justificación.

2.4. LUGAR Y TIEMPO DE LA COMISIÓN DEL DELITO

Dice Castellanos Tena[24], que casi en la mayoría de los casos, la actividad o la omisión se realizan en el mismo lugar en donde se produce el resultado; el tiempo que media entre el hacer o no hacer humanos y su resultado es insignificante y por ello pueden considerarse concominantes.

En ocasiones, sin embargo, la conducta y el resultado no coinciden respecto al lugar y al tiempo y es entonces cuando se esta en presencia de los llamados DELITOS A DISTANCIA, que dan lugar no solo a la aplicación de la ley Penal en función de dos o mas países soberanos, sino también, dentro del derecho interno, a cuestiones sobre determinación de la legislación aplicable, dentro del sistema federal mexicano; así por ejemplo, la carta calumniosa escrita en Michoacán cuyo destinatario, que radica en Chihuahua, la recibe tres o cuatro días después de confeccionada. ¿se cometió el delito en Michoacán y, en consecuencia, deberá aplicarse el código penal de esta entidad, o bien en

[24] Ibidem. Pag. 289.

Chihuahua, en cuyo caso será aplicable el ordenamiento respectivo?; ¿se delinquió cuando fue escrita la carta o cuando se leyó?.Para solucionar estos problemas se han elaborado diversas teorías.

Para Cuello Calón señala tres, a saber: a) Teoría de la actividad, según la cual el delito se da en el lugar y al tiempo de acción o de la omisión; b) Teoría del resultado, de acuerdo con ella la conducta se realiza en el lugar y al tiempo de producción del resultado; y c) Teoría del conjunto o de la obicuidad, para la cual la actividad se produce en el lugar y al tiempo de su realización de la conducta, como en donde y cuando se produce el resultado.

Para Edmundo Mezger, "lugar del hecho es todo lugar en el que ha sido realizada alguna parte integrante del hecho tratándose de la actividad corporal del autor o del resultado posterior"[25]. El penalista alemán se adhiere a la teoría del conjunto o de la ubicuidad, en cuanto al lugar se refiere; con relación al tiempo; para cuestiones, sobre prescripción, se afilia a la teoría del resultado a la de la actividad, tratándose de determinan la imputabilidad del sujeto.

Además de los criterios anteriores, se han elaborado algunos otros, como el de la intención, según el cual el delito debe tenerse por realizado en el tiempo y lugar en donde subjetivamente el agente lo ubica, y el de la actividad preponderante, que ve en el acto de mayor trascendencia, dentro de la actividad, el medio de determinar el lugar y tiempo de ejecución del delito.

[25] MEZGER, Edmundo; Derecho Penal, pag. 289.

CAPITULO III

3.1. CONCEPTOS DE DELITOS INFORMATICOS Y SUS GENERALIDADES.

Muchos estudiosos del derecho penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a ésta.

Según el ilustre penalista CUELLO CALON[26], los elementos integrantes del delito son:

a. El delito es un acto humano, es una acción (acción u omisión)
b. Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.
c. Debe corresponder a un tipo legal (figura de delito), definido por La Ley, ha de ser un acto típico.
d. El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona
e. La ejecución u omisión del acto debe estar sancionada por una pena.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

Entonces se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por La Ley, que se realiza en el entorno informático y está sancionado con una pena.

[26] Ibídem. Pag.145.

De esta manera, el autor mexicano Julio TELLEZ VALDEZ[27] señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)". Por su parte, el tratadista penal italiano Carlos SARZANA sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".[28],

3.2. FUENTES DE INTERNET Y DE LOS DELITOS INFORMATICOS

Pese a las infinitas posibilidades que ofrece Internet como infraestructura económica y cultural para facilitar muchas de las actividades humanas y contribuir a una mejor satisfacción de nuestras necesidades y a nuestro desarrollo personal, el uso de Internet también conlleva **riesgos, especialmente para los niños, los adolescentes y las personas que tienen determinados problemas**: tendencia al aislamiento social, parados de larga duración...

En el caso de los niños, la falta de una adecuada atención por parte de los padres (que muchas veces están trabajando fuera de casa todo el día) les deja aún más vía libre para acceder sin control a la TV e Internet, si está disponible en el hogar, cuando vuelven de la escuela.

Si el ordenador familiar no dispone de filtros que limiten el acceso a las páginas inadecuadas, de forma accidental o buscando nuevos amigos y estímulos se irán encontrando allí con toda clase de contenidos, servicios y personas, no siempre fiables ni convenientes para todas las edades.

Y lo que empieza por curiosidad puede acabar en una adicción ya que los niños y los adolescentes son fácilmente deducibles.

[27] Julio Téllez, Derecho Informático. Pagina 75.
[28] Definición a la que hace referencia Julio Téllez en su texto Derecho Informático.

Por desgracia hay muchos padres que no son conscientes de estos peligros, que ya se daban en parte con la televisión y los videojuegos y que ahora se multiplican en Internet, cada vez más omnipresente y accesible a todos en las casas, escuelas, cibercafés...

Todas las funcionalidades de Internet (navegación por las páginas web, publicación de deblas y webs, correo electrónico, mensajería instantánea, foros, chats, gestiones y comercio electrónico, entornos para el ocio...) pueden comportar algún riesgo, al igual como ocurre en las actividades que realizamos en el "mundo físico". En el caso de Internet, destacamos los siguientes **riesgos**[29]:

- Riesgos relacionados con la información. Las personas frecuentemente necesitamos información para realizar nuestras actividades, y muchas veces la podemos obtener en Internet de manera más rápida, cómoda y económica que en el "mundo físico".

No obstante hemos de considerar posibles riesgos:

[29] Pagina Web. www.riezgosenred.net

- Acceso a información poco fiable y falsa. Existe mucha información errónea y poco actualizada en Internet, ya que cualquiera puede poner información en la red. Su utilización puede dar lugar a múltiples problemas: desde realizar mal un trabajo académico hasta arruinar una actuación empresarial.

- Dispersión, pérdida de tiempo. A veces se pierde mucho tiempo para localizar la información que se necesita. Es fácil perderse navegando por el inmenso mar informativo de Internet lleno de atractivos "cantos de sirena". Al final el trabajo principal puede quedar sin hacer.

- Acceso de los niños a información inapropiada y nociva. Existen webs que pese a contener información científica, pueden resultar inapropiadas y hasta nocivas (pueden afectar a su desarrollo cognitivo y afectivo) para niños y menores por el modo en el que se abordan los temas o la crudeza de las imágenes (sexo, violencia, drogas, determinados relatos históricos y obras literarias...). La multimedialidad de Internet puede hacer estos contenidos aún más explícitos e impactantes.

- Acceso a información peligrosa, inmoral, ilícita. Existe información poco recomendable (pornografía infantil, violencia, todo tipo de sectas...) y hasta con contenidos considerados delictivos que incitan a la violencia, el racismo, la xenofobia, el terrorismo, la pedofilia, el consumo de drogas, participar en ritos satánicos y en sectas ilegales, realizar actos delictivos... La globalidad de Internet y las diferentes culturas y legislaciones de los países hacen posible la existencia (por lo menos temporal, ya que grupos especiales de la policía dedicados a *delitos informáticos* realiza actuaciones a nivel internacional) de estas páginas web en el ciberespacio

Los primeros riesgos se pueden paliar aprendiendo buenas técnicas para buscar la información y valorarla con juicio crítico, así como adquiriendo hábitos de trabajo en Internet que limiten la tendencia a la dispersión al buscar contenidos.

En cuanto a los segundos, que afectan sobre todo a los más jóvenes, exigen una adecuada respuesta por parte de padres y educadores mediante la instalación de programas de protección en los ordenadores que limiten el acceso a determinadas páginas web y alertando a los niños y jóvenes sobre estos riesgos, explicándoles de manera adecuada a su edad las razones. Entendemos que los medios de comunicación social también deberían alertar a los ciudadanos en general sobre las páginas web con contenidos ilegales y sobre la conveniencia de denunciarlas.

- Riesgos relacionados con la comunicación interpersonal. Las personas muchas veces necesitamos comunicarnos con personas lejanas o establecer nuevos contactos sociales. Internet nos ofrece infinidad de canales y oportunidades (e-mail, chats, weblogs...), aunque conllevan algunos riesgos:

- Bloqueo del buzón de correo*.* Hay personas que ignorando las normas de ***"netiquette"*** (pautas de comportamiento que facilitan la convivencia entre los usuarios y el buen funcionamiento de la red) adjuntan grandes archivos a los correos sin pedir previamente autorización al receptor del mensaje, con lo que acaban bloqueando temporalmente su buzón de correo.

- Recepción de "mensajes basura". Ante la carencia de una legislación adecuada, por e-mail se reciben muchos mensajes de propaganda no deseada (spam) que envían indiscriminadamente empresas de todo el mundo. En ocasiones su contenido es de naturaleza sexual o proponen oscuros negocios. Otras veces pueden contener archivos con virus.

- Recepción de mensajes personales ofensivos. Al comunicarse en los foros virtuales, como los mensajes escritos (a menudo mal redactados y siempre privados del contacto visual y la interaccción inmediata con el emisor) se prestan más a malentendidos que pueden resultar ofensivos para algunos de sus receptores, a veces se generan fuertes discusiones que incluyen insultos e incluso amenazas.

Por otra parte, en ocasiones hay personas que son acosadas a través del e-mail con mensajes que atentan contra su intimidad.

- Pérdida de intimidad. En ocasiones, hasta de manera inconsciente al participar en los foros, se puede proporcionar información personal, familiar o de terceras personas a gente desconocida. Y esto siempre supone un peligro. También es frecuente hacerlo a través de los formularios de algunas páginas web que proporcionan determinados servicios gratuitos (buzones de e-mail, alojamiento de páginas web, música y otros recursos digitales...)

- Acciones ilegales. Proporcionar datos de terceras personas, difundir determinadas opiniones o contenidos, plagiar información, insultar, difamar o amenazar a través de los canales comunicativos de Internet... puede acarrear responsabilidades judiciales (como también ocurre en el "mundo físico").

- Malas compañías. Especialmente en los chats, MUDs.., se puede entrar en contacto con personas que utilizan identidades falsas con oscuras intenciones, en ocasiones psicópatas que buscan víctimas para actos violentos o delictivos a las que prometen estímulos, experiencias y amistad. Para paliar estos riesgos es conveniente informar sobre las normas de "netiquette" y educar a los usuarios en el uso correcto de los canales comunicativos de Internet, alertándoles del riesgo de difundir sus datos más personales y de las repercusiones legales que pueden tener sus mensajes y los archivos que se intercambian. Nuevamente esta sensibilización resulta especialmente necesaria en el caso de los menores, que resultan mucho más vulnerables ante las personas que quieran aprovecharse de ellos..

- Riesgos relacionados con actividades con repercusión económica (compras y gestiones, envío y recepción de archivos...). El ciberespacio que sustenta Internet es un mundo paralelo en el que se pueden realizar prácticamente todas las actividades que realizamos en el "mundo físico". Y las actividades con repercusión económica siempre suponen riesgos. En el caso de Internet destacamos los siguientes:

- Estafas. En las compras y demás transacciones económicas (tiendas virtuales, bancos, servicios formativos...) que se realizan por Internet, especialmente si las empresas no son de solvencia reconocida, la virtualidad muchas veces enmascara sutiles engaños y estafas a los compradores.

- Compras inducidas por una publicidad abusiva. Aprovechando la escasa regulación de las actividades en Internet, las empresas utilizan sofisticados sistemas de marketing para seducir a los internautas e incitarles a la adquisición de sus productos, incluyendo publicidad subliminal. Sus anuncios de reclamo ("banners"...) aparecen en todo tipo de webs, y a veces resulta difícil separar los contenidos propios de la web de la publicidad. De manera que a veces se acaba haciendo compras innecesarias.

- Compras por menores sin autorización paterna. Niños y jóvenes pueden realizar compras sin control familiar a través de Internet, en ocasiones incluso utilizando las tarjetas de crédito de familiares o conocidos.

- Robos. Al facilitar información personal y los códigos secretos de las tarjetas de crédito por Internet, a veces son interceptados por ciberladrones y los utilizan para suplantar la personalidad de sus propietarios y realizar compras a su cargo. Con todo, se van desarrollando sistemas de seguridad (firmas electrónicas, certificados digitales...) que cada vez aseguran mas la confidencialidad al enviar los datos personales necesarios para realizar las transacciones económicas. Hay empresas que delinquen vendiendo los datos personales de sus clientes a otras empresas y estafadores.

- Actuaciones delictivas por violación de la propiedad intelectual. Muchas personas, a veces incluso sin ser conscientes de ello o de la gravedad de su acción, realizan actos delictivos violando la propiedad intelectual a través de Internet: búsqueda y recepción de programas o música con copyright (piratería musical) o software para desactivar sistemas de protección de los productos digitales, difusión de estos materiales a personas conocidas...

- Realización de negocios ilegales a través de Internet: compra-ventas, subastas, préstamos, apuestas...

- Gastos telefónicos desorbitados. Si no se dispone de una conexión adecuada con tarifa plana que fije el coste mensual por uso de Internet, o el internauta entra de manera inconsciente en páginas (generalmente de contenido sexual) en las que al solicitar un servicio aparentemente gratuito le conectan a líneas telefónicas de alta tarifación, las facturas telefónicas pueden proporcionar serios disgustos.

Ante la gravedad de estos riesgos y la relativa novedad que supone Internet en nuestra sociedad para la mayor parte de los ciudadanos, entendemos que deberían hacerse campañas informativas a nivel nacional a través de todos los medios de comunicación, con una especial incidencia en los centros docentes. Al mismo tiempo deben seguir desarrollándose la legislación que regule el uso de Internet y las medidas policiales dirigidas a la captura de los delincuentes del ciberespacio.

- Riesgos relacionados con el funcionamiento de la red Internet. A veces por limitaciones tecnológicas, a veces por actos de sabotaje y piratería y que aún resultan incontrolables, la red Internet no siempre funciona como quisiéramos:

- Lentitud de accesos. A veces debido al tipo de conexión (modem...), otras veces debido a la saturación de algunos servidores en horas punta.

- Imposibilidad de conexión a una web o a un servicio de Internet, que puede ser debida a problemas del servidor que da el servicio. Si esta circunstancia nos impide la realización de un trabajo importante, puede traernos muy malas consecuencias.

- Problemas de virus, que actualmente se propagan con libertad por la red y pueden bloquear el funcionamiento del ordenador y destruir la información que almacena. Para navegar por Internet resulta imprescindible disponer de un sistema antivirus actualizado en el ordenador.

- Espionaje. A través de mecanismos como las "cookies" o de virus, se puede conocer todo lo que se hace desde un ordenador y copiar todos los archivos que tiene almacenados. Con estos sistemas algunos espías se dedican a detectar las circunstancias y preferencias de las personas con el fin de elaborar listas de posibles clientes que luego venden a las empresas comerciales.

- ***Publicidad subliminal, spam***...

En siglos anteriores las vías de comunicación entre las ciudades resultaban también lentas e inseguras (mal firme, guerras, bandidos...). Seguro que dentro de unos pocos años todos estos problemas de Internet también se habrán solucionado. De momento hay que conocerlos y tenerlos en cuenta: no podemos confiar que todo Internet esté siempre operativo a nuestra disposición y debemos proteger nuestro ordenador con un sistema antivirus/espionaje adecuado.

- Riesgos relacionados con las adicciones (IAD, Internet Addiction Disorder). En toda adicción siempre confluyen tres elementos: una persona, unas circunstancias personales determinadas y una sustancia o situación que produzca placer (Internet puede proporcionar múltiples sensaciones placenteras).

Aunque la conexión compulsiva a Internet constituye un indicador significativo en los casos de IAD, no es posible establecer una correspondencia entre determinadas horas de conexión a Internet y adicción, pues el uso de Internet depende de las circunstancias personales de cada uno (algunos trabajadores y estudiantes deben estar conectados casi siempre a Internet).

Incluso considerando solamente el tiempo de ocio que se emplea en Internet, resulta difícil establecer la frontera de la adicción basada en el número de horas diarias o semanales de conexión; como mundo alternativo al "mundo físico", Internet ofrece infinidad de ofertas de ocio: lecturas, música, películas, juegos, reuniones ("virtuales", esto si, pero a veces incluso con sistemas de videochat)... y cada persona puede tener sus preferencias.

Con todo, podemos considerar que una persona tiene **adicción a Internet** cuando de manera habitual es **incapaz de controlar el tiempo que está conectado a Internet**, relegando las obligaciones familiares, sociales y académicas/profesionales. Más que una adicción genérica a Internet, podemos considerar adicciones o usos compulsivos a determinados contenidos o servicios:

- Adicción a buscar información de todo tipo: noticias, webs temáticas, webs personales, servicios ofrecidos por empresas... Muchas veces incluye pornografía, imágenes o escenas que incluyen violencia... Se buscan sensaciones más que información.

- Adicción a frecuentar los entornos sociales: chats, MUDs... Los usuarios no dependientes tienen más tendencia a comunicarse con las personas conocidas. Los adictos buscan más conocer gente nueva y buscar el apoyo en los grupos de la red; a veces se crean varias personalidades virtuales.

- Juego compulsivo. Internet está lleno de webs con todo tipo de juegos, algunos de ellos tipo casino con apuestas en dinero; otros muy competitivos o violentos..., que pueden fomentar ludopatías en determinadas personas.

- Compras compulsivas: comercio electrónico, subastas...

Para superar estas adicciones que distorsionan la vida normal de los individuos, muchas veces será necesaria la ayuda de las personas próximas y hasta de médicos especialistas.

En el caso de los menores, es importante que los padres estén atentos al uso que hacen sus hijos de Internet y vean de detectar estos problemas lo antes posible.

A partir de los datos que proporciona un estudio realizado en noviembre de 2002 por las organizaciones de protección de la infancia ACPI <http://www.asociacion-acpi.org> y PROTEGELES http://www.protegeles.com> sobre "Seguridad Infantil y Costumbres de los Menores en Internet", se consideran las siguientes características que alertan sobre una posible adicción a Internet: necesidad de conectarse con frecuencia y a diario o casi a diario, navegar más de 10 horas semanales, buscar sensaciones y visitar tanto páginas de pornografía como de violencia, entrar en los chats creando personalidades distintas y con frecuencia de sexo opuesto.

A pesar de que los riesgos a los que estamos expuestos en Internet son básicamente los mismos que encontramos en el "mundo físico" (no olvidemos que al acceder a Internet accedemos a un mundo paralelo o ciberespacio que en gran medida lo imita), la naturaleza "virtual" de Internet y su creciente ubicuidad en nuestra sociedad, la novedad que representan sus servicios y nuestra poca experiencia en su uso (aún estamos en fase de descubrir muchas de sus posibilidades), introducen nuevos **factores que aumentan estos riesgos**:

- Fácil acceso a la información. En el mundo físico suele resultar difícil, y muchas veces costoso económicamente, encontrar muchas de las informaciones peligrosas que en Internet se encuentran con facilidad, gratis, y hasta a veces aparecen de manera ocasional: por ejemplo al teclear erróneamente una palabra en una búsqueda.

Por contra, en el "mundo físico" las restricciones legales a la distribución de contenidos pornográficos y violentos suelen alejarlos de los entornos infantiles, y la necesidad de dinero para adquirir determinados materiales y hasta la entidad física de los mismos (que hay que guardar en algún lugar) contribuye a facilitar un cierto control parental.

- Fácil comunicación interpersonal. En el mundo físico los contactos personales nos aportan más datos sobre las personas con las que nos relacionamos que pueden alertarnos ante conductas extrañas de algunos individuos que se nos acerquen. Además, las personas y grupos se mueven en determinados espacios físicos, que muchas veces suponen un inconveniente para coincidir con ellos. En Internet no hay distancias, todo está a nuestro alcance, y la virtualidad permite moverse por el ciberespacio con personalidades ficticias.

- Accesibilidad permanente. Internet, cada vez más, está siempre a nuestro alcance, de manera que facilita la inmediata realimentación de las adicciones: violencia, ludopatía...

- Anonimato. En Internet pueden realizarse muchas acciones de manera anónima, con un ***escaso control social***, lo que permite a algunas personas realizar actos en el "mundo virtual" que no se atreverían a hacer en el "mundo físico": comportamientos poco respetuosos en chats, visitar casinos, proveerse de pornografía.

3.3. CONSIDERACIONES SOBRE LOS DELITOS INFORMATICOS.

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

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

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

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

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

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

Este es el panorama de este nuevo fenómeno científico tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la Informática es hoy una forma de Poder Social.

Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

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

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a París en mayo de 1983, el término delitos relacionados con las computadoras se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.

La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminólogos, económicos, preventivos o legales.

En la actualidad la informatización se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como "criminalidad informática".

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables.

La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos.

A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

3.4. CARACTERISTICAS DE LOS DELITOS INFORMATICOS

Según el mexicano Julio Téllez Valdez, los delitos informáticos presentan las siguientes características principales:

a. Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
b. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
c. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
e. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
f. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
g. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
h. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
i. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

3.5 CLASIFICACION DE LOS DELITOS INFORMATICOS

Para la comisión de dicha conducta antisocial, encontraremos a uno o varios sujetos activos como también pasivos, los cuales tienen características propias:

3.5.1. ***El Sujeto Activo***, posee ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos, es decir, el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional, pues son personas listas, decididas y motivadas, dispuestas a aceptar un reto tecnológico.

3.5.2. ***El Sujeto Pasivo o víctima del delito*** es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones creditícias, gobiernos, etcétera, que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito es sumamente importante, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables" y si a esto se suma la

falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otras más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta o cifra negra".

En forma general, las principales características que revisten los Delitos informáticos son:

a) Conductas criminógenas de cuello blanco.

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

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

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

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

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

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

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

i) En su mayoría son imprudenciales y no necesariamente se cometen con intención.

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

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

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

Por lo anterior, se puede apreciar que los que cometen este tipo de ilícitos, son personas con conocimientos sobre la informática y cibernética, los cuales, se encuentran en lugares estratégicos o con facilidad para poder acceder a información de carácter delicado, como puede ser a instituciones creditícias o del gobierno, empresas o personas en lo particular, dañando en la mayoría de los casos el patrimonio de la víctima, la cual, por la falta de una ley aplicable al caso concreto, no es denunciada quedando impune estos tipos de conductas antisociales; siendo esto alarmante, pues como se mencionó en líneas precedentes este tipo de acciones tienden a proliferar y ser más comunes, por lo que se pretende en la presente investigación, es crear una conciencia sobre la necesidad urgente de regular estas conductas, ya que debe ser legislado de una manera seria y honesta, recurriendo a las diferentes personalidades del conocimiento, tanto técnico en materia de computación, como en lo legal, ya que si no se conoce de la materia, difícilmente se podrán aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular. Después de ubicar las características que tienen el tipo de delitos informáticos así como sus sujetos y víctimas, se entrará al estudio de su Clasificación:

La mayoría de los estudiosos en la materia clasifican a este tipo de acciones de dos formas, como instrumento o medio y como fin u objeto.

Aún así autores como Sarzana mencionan que estos ilícitos pueden clasificarse en atención a que producen un provecho para el autor y provocan un daño contra la computadora como entidad física y que procuren un daño a un individuo o grupos, en su integridad física, honor o patrimonio.

Julio Téllez Valdes[30], clasifica a los delitos informáticos:

1. **Como Instrumento o medio**, dichas conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito; por ejemplo, la falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera), la variación de los activos y pasivos en la situación contable de las empresas, la planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera), el "robo" de tiempo de computadora, la lectura, sustracción o copiado de información confidencial, el aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas, la alteración en el funcionamiento de los sistemas (virus informáticos) y el acceso a áreas informatizadas en forma no autorizadas entre muchas más, y;
2. **Como Fin y Objeto**. En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física, los cuales pueden ser la programación de instrucciones que producen un bloqueo total al sistema, la destrucción de programas por cualquier método, el daño a la memoria, o el atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).

Para María de la Luz Lima[31], en su trabajo sobre "Delitos Electrónicos" los clasifica en tres categorías, a saber:

1.- Los que utilizan la tecnología electrónica como método;

[30] Idem. Pág.260
[31] María de La Luz Lima, Delitos Electrónicos, Pág. 275

2.- Los que utilizan la tecnología electrónica como medio y;

3.- Los que utilizan la tecnología electrónica como fin.

Como método, los individuos utilizan métodos electrónicos para llegar a un resultado ilícito. Como medio, son aquellas conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo. Y Como fin, son las dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

3.6. SISTEMAS Y EMPRESAS CON MAYOR RIEZGO

Evidentemente el artículo que resulta más atractivo robarse el dinero o algo de valor. Por lo tanto, los sistemas que pueden estar más expuestos a fraude son los que tratan pagos, como los de nómina, ventas, o compras. En ellos es donde es más fácil convertir transacciones fraudulentas en dinero y sacarlo de la empresa.

Por razones similares, las empresas constructoras, bancos y compañías de seguros, están más expuestas a fraudes que las demás.

Los sistemas mecanizados son susceptibles de pérdidas o fraudes debido a que:

- Tratan grandes volúmenes de datos e interviene poco personal, lo que impide verificar todas las partidas.
- Se sobrecargan los registros magnéticos, perdiéndose la evidencia auditable o la secuencia de acontecimientos.
- A veces los registros magnéticos son transitorios y a menos que se realicen pruebas dentro de un período de tiempo corto, podrían perderse los detalles de lo que sucedió, quedando sólo los efectos.
- Los sistemas son impersonales, aparecen en un formato ilegible y están controlados parcialmente por personas cuya principal preocupación son los aspectos técnicos del equipo y del sistema y que no comprenden, o no les afecta, el significado de los datos que manipulan.

- En el diseño de un sistema importante es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que se hayan hecho queden huecos sin cubrir.
- Los sistemas tienden a ser algo rígidos y no siempre se diseñan o modifican al ritmo con que se producen los acontecimientos; esto puede llegar a ser otra fuente de "agujeros".
- Sólo parte del personal de proceso de datos conoce todas las implicaciones del sistema y el centro de cálculo puede llegar a ser un centro de información. Al mismo tiempo, el centro de cálculo procesará muchos aspectos similares de las transacciones.
- En el centro de cálculo hay un personal muy inteligente, que trabaja por iniciativa propia la mayoría del tiempo y podría resultar difícil implantar unos niveles normales de control y supervisión.
- El error y el fraude son difíciles de equiparar. A menudo, los errores no son iguales al fraude. Cuando surgen discrepancias, no se imagina que se ha producido un fraude, y la investigación puede abandonarse antes de llegar a esa conclusión. Se tiende a empezar buscando errores de programación y del sistema. Si falla esta operación, se buscan fallos técnicos y operativos. Sólo cuando todas estas averiguaciones han dado resultados negativos, acaba pensándose en que la causa podría ser un fraude.

3.7. DELITOS EN PERSPECTIVA

Los delitos pueden ser examinados desde dos puntos de vista diferentes:

- Los delitos que causan mayor impacto a las organizaciones.
- Los delitos más difíciles de detectar.

Aunque depende en gran medida del tipo de organización, se puede mencionar que los Fraudes y sabotajes son los delitos de mayor incidencia en las organizaciones.

Además, aquellos que no están claramente definidos y publicados dentro de la organización como un delito (piratería, mala utilización de la información, omisión deliberada de controles, uso no autorizado de activos y/o servicios computacionales; y que en algún momento pueden generar un impacto a largo plazo).

Pero si se examina la otra perspectiva, referente a los delitos de difícil detección, se deben situar a aquellos producidos por las personas que trabajan internamente en una organización y que conocen perfectamente la configuración interna de las plataformas; especialmente cuando existe una cooperación entre empleados, cooperación entre empleados y terceros, o incluso el involucramiento de la administración misma.

3.8. TIPIFICACIÓN DE LOS DELITOS

3.8.1. Clasificación Según la Actividad Informática

- Sabotaje informático

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema.

Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

Básicamente, se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

Conductas dirigidas a causar daños físicos

El primer grupo comprende todo tipo de conductas destinadas a la destrucción «física» del hardware y el software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc.

En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

Conductas dirigidas a causar daños lógicos

El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos «lógicos», o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático.

Este tipo de daño a un sistema se puede alcanzar de diversas formas. Desde la más simple que podemos imaginar, como desenchufar el ordenador de la electricidad mientras se esta trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

Estos programas destructivos, utilizan distintas técnicas de sabotaje, muchas veces, en forma combinada. Sin pretender realizar una clasificación rigurosa de estos métodos de destrucción lógica, podemos distinguir:

1. Bombas lógicas (time bombs): En esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (por ejemplo a los dos meses o en una fecha o a una hora determinada), o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar.
2. La jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa.

3. Otra modalidad que actúa sobre los programas de aplicación es el llamado «cáncer de rutinas» («cancer routine»).

   En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos.

   Una variante perfeccionada de la anterior modalidad es el «virus informático» que es un programa capaz de multiplicarse por sí mismo y contaminar los otros programas que se hallan en el mismo disco rígido donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión.

Fraude a través de computadoras

Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.

Los distintos métodos para realizar estas conductas se deducen, fácilmente, de la forma de trabajo de un sistema informático: en primer lugar, es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos, en un ordenador. Esta forma de realización se conoce como manipulación del input.

Ulrich Sieber, cita como ejemplo de esta modalidad el siguiente caso tomado de la jurisprudencia alemana:

Una empleada de un banco del sur de Alemania transfirió, en febrero de 1983, un millón trescientos mil marcos alemanes a la cuenta de una amiga - cómplice en la maniobra - mediante el simple mecanismo de imputar el crédito en una terminal de computadora del banco. La operación fue realizada a primera hora de la mañana y su falsedad podría haber sido detectada por el sistema de seguridad del banco al mediodía.

Sin embargo, la rápida transmisión del crédito a través de sistemas informáticos conectados en línea (on line), hizo posible que la amiga de la empleada retirara, en otra sucursal del banco, un millón doscientos ochenta mil marcos unos minutos después de realizada la operación informática.

En segundo lugar, es posible interferir en el correcto procesamiento de la información, alterando el programa o secuencia lógica con el que trabaja el ordenador. Esta modalidad puede ser cometida tanto al modificar los programas originales, como al adicionar al sistema programas especiales que introduce el autor.

A diferencia de las manipulaciones del input que, incluso, pueden ser realizadas por personas sin conocimientos especiales de informática, esta modalidad es más específicamente informática y requiere conocimientos técnicos especiales.

Sieber cita como ejemplo el siguiente caso, tomado de la jurisprudencia alemana:

El autor, empleado de una importante empresa, ingresó al sistema informático un programa que le permitió incluir en los archivos de pagos de salarios de la compañía a «personas ficticias» e imputar los pagos correspondientes a sus sueldos a una cuenta personal del autor.

Esta maniobra hubiera sido descubierta fácilmente por los mecanismos de seguridad del banco (listas de control, sumarios de cuentas, etc.) que eran revisados y evaluados periódicamente por la compañía. Por este motivo, para evitar ser descubierto, el autor produjo cambios en el programa de pago de salarios para que los «empleados ficticios» y los pagos realizados, no aparecieran en los listados de control.

Por último, es posible falsear el resultado, inicialmente correcto, obtenido por un ordenador: a esta modalidad se la conoce como manipulación del output.

Una característica general de este tipo de fraudes, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo.

Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. Incluso, en los casos de "manipulación del programa", la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y cada vez que el programa se active.

En el ejemplo jurisprudencial citado al hacer referencia a las manipulaciones en el programa, el autor podría irse de vacaciones, ser despedido de la empresa o incluso morir y el sistema seguiría imputando el pago de sueldos a los empleados ficticios en su cuenta personal.

Una problemática especial plantea la posibilidad de realizar estas conductas a través de los sistemas de teleproceso. Si el sistema informático está conectado a una red de comunicación entre ordenadores, a través de las líneas telefónicas o de cualquiera de los medios de comunicación remota de amplio desarrollo en los últimos años, el autor podría realizar estas conductas sin ni siquiera tener que ingresar a las oficinas donde funciona el sistema, incluso desde su propia casa y con una computadora personal.

Aún más, los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otro.

Respecto a los objetos sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles (ej.: depósitos monetarios, créditos, etc.), en otros casos, los datos que son objeto del fraude, representan objetos corporales (mercadería, dinero en efectivo, etc.) que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles.

En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser «creado» por el autor.

Ejemplos

El autor, empleado del Citibank, tenía acceso a las terminales de computación de la institución bancaria. Aprovechando esta circunstancia utilizó, en varias oportunidades, las terminales de los cajeros, cuando ellos se retiraban, para transferir, a través del sistema informático, fondos de distintas cuentas a su cuenta personal.

Posteriormente, retiró el dinero en otra de las sucursales del banco.

En primera instancia el Juez calificó los hechos como constitutivos del delito de hurto en forma reiterada. La Fiscalía de Cámara solicitó el cambio de calificación, considerando que los hechos constituían el delito de estafa.

La Cámara del crimen resolvió:

«... y contestando a la teoría fiscal, entiendo que le asiste razón al Dr. Galli en cuanto sostiene que estamos en presencia del tipo penal de hurto y no de estafa. Ello es así porque el apoderamiento lo hace el procesado y no le entrega el banco por medio de un error, requisito indispensable para poder hablar de estafa. El apoderamiento lo hace el procesado directamente, manejando el sistema de computación.

De manera que no hay diferencia con la maniobra normal del cajero, que en un descuido se apodera del dinero que maneja en caja y la maniobra en estudio en donde el apoderamiento del dinero se hace mediante el manejo de la computadora...»

Como el lector advertirá, la resolución adolece de los problemas de adecuación típica a que hacíamos referencias más arriba.

En realidad, el cajero no realizó la conducta de apoderamiento que exige el tipo penal del hurto ya que recibió el dinero de manos del cajero. En el caso de que se considere que el apoderamiento se produjo en el momento en el que el autor transfirió los fondos a su cuenta, el escollo de adecuación típica insalvable deriva de la falta de la «cosa mueble» como objeto del apoderamiento exigido por el tipo penal.

Los fraudes que se cometen a través de las computadoras

1.- Estafas electrónicas: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra.

No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

2.- "Pesca" u "olfateo" de claves secretas: Los delincuentes suelen engañar a los usuarios nuevos e incautos de la Internet para que revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio.

Los "sabuesos" utilizan programas para identificar claves de usuarios, que más tarde se pueden usar para esconder su verdadera identidad y cometer otras fechorías, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

3.- Estratagemas: Los estafadores utilizan diversas técnicas para ocultar computadoras que se "parecen" electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos.

El famoso pirata Kevin Mitnick se valió de estratagemas en 1996 para introducirse en la computadora de la casa de Tsutomo Shimamura, experto en seguridad, y distribuir en la Internet valiosos útiles secretos de seguridad.

4.- Juegos de azar: El juego electrónico de azar se ha incrementado a medida que el comercio brinda facilidades de crédito y transferencia de fondos en la

Red. Los problemas ocurren en países donde ese juego es un delito o las autoridades nacionales exigen licencias.

Además, no se puede garantizar un juego limpio, dadas las inconveniencias técnicas y jurisdiccionales que entraña su supervisión.

5.- Fraude: Ya se han hecho ofertas fraudulentas al consumidor tales como la cotización de acciones, bonos y valores o la venta de equipos de computadora en regiones donde existe el comercio electrónico.

6.- Blanqueo de dinero: Se espera que el comercio electrónico sea el nuevo lugar de transferencia electrónica de mercancías o dinero para lavar las ganancias que deja el delito, sobre todo si se pueden ocultar transacciones.

7.- Copia ilegal de software y espionaje informático.

Se engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información.

Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apoderamiento es el mismo programa de computación (software) que suele tener un importante valor económico.

8.- Infracción de los derechos de autor: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.

9.- Infracción del Copyright de bases de datos: No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.

10.- Uso ilegítimo de sistemas informáticos ajenos. Esta modalidad consiste en la utilización sin autorización de los ordenadores y los programas de un sistema informático ajeno.

Este tipo de conductas es comúnmente cometida por empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias a su trabajo.

En estos supuestos, sólo se produce un perjuicio económico importante para las empresas en los casos de abuso en el ámbito del teleproceso o en los casos en que las empresas deben pagar alquiler por el tiempo de uso del sistema.

11.- Acceso no autorizado: La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

12.- Delitos informáticos contra la privacidad.

Grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos

Esta tipificación se refiere a quién, 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 cualquier otro tipo de archivo o registro público o privado.

Existen circunstancias agravantes de la divulgación de ficheros, los cuales se dan en función de:

A) El carácter de los datos: ideología, religión, creencias, salud, origen racial y vida sexual.

B) Las circunstancias de la víctima: menor de edad o incapaz.

También se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, se piensa que entre lo anterior se encuentra el pinchado de redes informáticas.

13.- Interceptación de e-mail: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

- Pornografía infantil

La distribución de pornografía infantil por todo el mundo a través de la Internet está en aumento. Durante los pasados cinco años, el número de condenas por transmisión o posesión de pornografía infantil ha aumentado de 100 a 400 al año en un país norteamericano. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material "ofensivo" que se transmita o archive.

3.8.2. Clasificación Según el Instrumento, Medio o Fin u Objetivo

Asimismo, TELLEZ VALDEZ clasifica a estos delitos, de acuerdo a dos criterios:

Como instrumento o medio.

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

1. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)

2. Variación de los activos y pasivos en la situación contable de las empresas.
3. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
4. Lectura, sustracción o copiado de información confidencial.
5. Modificación de datos tanto en la entrada como en la salida.
6. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
7. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
8. Uso no autorizado de programas de cómputo.
9. Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
10. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
11. Obtención de información residual impresa en papel luego de la ejecución de trabajos.
12. Acceso a áreas informatizadas en forma no autorizada.
13. Intervención en las líneas de comunicación de datos o teleproceso[32].

- Como fin u objetivo.

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

a. Programación de instrucciones que producen un bloqueo total al sistema.
b. Destrucción de programas por cualquier método.
c. Daño a la memoria.
d. Atentado físico contra la máquina o sus accesorios.
e. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

[32] Idem. Pág. 100.

f. Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

3.8.3. Clasificación según sus actividades

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

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

La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

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

Tanto el FBI como el Fiscal General de los Estados Unidos han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles.

3 Espionaje: Se ha dado casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto de los Estados Unidos, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera.

Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles.

Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

4 Espionaje industrial: También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y know how estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

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

1. Infracciones que no Constituyen Delitos Informáticos.

Usos comerciales no éticos: Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mailings electrónicos" al colectivo de usuarios de un gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

Actos parasitarios: Algunos usuarios incapaces de integrarse en grupos de discusión o foros de debate online, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc.

También se deben tomar en cuenta las obscenidades que se realizan a través de la Internet.

3.9 USO DEL INTERNET Y LA RELACIÓN PARA LA COMISIÓN DE LOS DELITOS

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

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

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

a) Elementos de entrada, representado por la forma de alimentación de información a la computadora, por medio de datos e instrucciones realizados por elementos periféricos tales como pantallas, lectoras de soportes magnéticos, discos, diskettes etc;

b) el Procesador Central, siendo el dispositivo en que se ejecutan las operaciones lógico-matemáticas, conocido más comúnmente como unidad Central del proceso, es decir, el CPU (siglas en inglés);

d) Dispositivo de almacenamiento, el cual contiene o almacena la información que se ha de procesar; e)

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

a) Hardware, constituido por las partes mecánicas, electromecánicas y electrónicas, como estructura física de las computadoras y encargadas de la captación, almacenamiento y procesamiento de información, así como la obtención de resultados; y

b) Software, que constituye la estructura lógica que permite a la computadora la ejecución del trabajo que se ha de realizar.

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

La cibernética es la ciencia de la comunicación y el control. Los aspectos aplicados de ésta ciencia, están relacionados con cualquier campo de estudio. Sus aspectos formales estudian una teoría general del control, destratada de los campos de aplicación y adecuada para todos ellos.

La noción de "INFORMATICA", es un 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.

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

Se le da el término a TELEMÁTICA, a todo lo que abarca la revolución tecnológica acelerada, en los campos afines de telecomunicaciones, computadoras, microinformática y bancos de datos. Es el término en boga en los países europeos.

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

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

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

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

Se calcula que Internet enlaza hoy día a 60 millones de computadoras personales en un extenso tejido electrónico mundial, lo cual hace necesario

entenderla como un fenómeno social, dado el crecimiento exponencial que ha mostrado.

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

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

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

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

Esta red, permitió primero a los investigadores de Estados Unidos acceder y usar directamente super computadoras localizadas en algunas universidades y laboratorios clave; después, compartir archivos y enviar correspondencia electrónica. A finales de 1970 se crearon redes cooperativas descentralizadas, como UUCP, una red de comunicación mundial basada en UNIX y USENET (red de usuarios), la cual daba servicio a la comunidad universitaria y más adelante a algunas organizaciones comerciales. En 1980, las redes más coordinadas, como CSNET (red de ciencias de cómputo), y BITNET,

empezaron a proporcionar redes de alcance nacional, a las comunidades académicas y de investigación, las cuales hicieron conexiones especiales que permitieron intercambiar información entre las diferentes comunidades.

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

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

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

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

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

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

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

Se intenta que Internet, sea, un medio interactivo viable para la libre expresión, la educación y el comercio.

No existe institución académica, comercial, social o gubernamental que pueda administrarla. Son cientos de miles de operadores y redes de cómputo, que de manera independiente, deciden usar los protocolos de transferencia y recepción de datos para intercambiar comunicaciones, información. No existe un lugar que concentre o centralice la información de Internet. Sería técnicamente imposible.

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

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

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

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

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

a) CORREO ELECTRONICO, siendo el servicio de mayor uso, de mayor tráfico y, por lo tanto, de mayor importancia para el surgimiento, en la actualidad, de diversas relaciones contractuales.

Permite escribir y enviar mensajes a una persona o grupo de personas conectadas a la red;

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

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

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

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

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

Un ejemplo de conducta activa sería remitir una recopilación de imágenes pornográficas scaneadas a los mailbox de un país en que dicho tráfico estuviese prohibido.

3.10. DELITOS TRADICIONALMENTE DENOMINADOS INFORMATICOS

A pesar de que el concepto de delito informático engloba tanto los delitos cometidos contra el sistema como los delitos cometidos mediante el uso de sistemas informáticos, cuando hablamos del ciberespacio como un mundo virtual distinto a la "vida real", me refiero al delito informático como aquél que está íntimamente ligado a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información, etc..

Incluyo también dentro de este apartado los actos que sólo constituirían una infracción administrativa o la vulneración de un derecho no tutelado por la jurisdicción penal, pero que en algunos países pueden llegar a ser delito.

Dentro de este tipo de delitos o infracciones podríamos destacar:

Acceso no autorizado: La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático no disponen en algunos países de preceptos que permitan su persecución.

Infracción de los derechos de autor: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.

No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line o de un sysop respecto a las copias ilegales introducidas en el sistema. Mientras un tribunal condenó a un sysop porque en su BBS había imágenes scaneadas de la revista Playboy, en el caso La Macchia, el administrador del sistema fue hallado no responsable de las copias de programas que albergaba su BBS.

El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a un "upload" de un programa o fichero que infrinja los derechos de autor de terceros.

Infracción del copyright de bases de datos: No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contratual: el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.

Interceptación de e-mail: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

Estafas electrónicas: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que

además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra.

No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

Transferencias de fondos: Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático. A pesar de que en algunas legislaciones y en sentencias aisladas se ha asimilado el uso de passwords y tarjetas electrónicas falsificadas al empleo de llaves falsas, calificando dicha conducta como robo, existe todavía una falta de uniformidad en la materia.

CAPITULO IV

"OTRAS LEGISLACIONES QUE SI CONTEMPLAN LOS DELITOS COMETIDOS A TRAVEZ DEL INTERNET"

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

4.1. TIPOS DE DELITOS RECONOCIDOS POR LA ORGANIZACIÓN DE NACIONES UNIDAS (O.N.U.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.2 LEGISLACION EN OTROS PAISES

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

1. Espionaje de datos. 2. Estafa Informática. 3. Falsificación de datos probatorios. 4. Alteración de Datos. 5. Sabotaje Informático. 6. Utilización abusiva de cheques o tarjetas de crédito.

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

Alemania también cuenta con una Ley de Protección de Datos, promulgada el 27 de enero de 1977, en la cual, en su numeral primero menciona que "el cometido de la protección de datos es evitar el detrimento de los intereses dignos de protección de los afectados, mediante la protección de los datos personales contra el abuso producido con ocasión del almacenamiento, comunicación, modificación y cancelación (proceso) de tales datos.

La presente ley protege los datos personales que fueren almacenados en registros informatizados, modificados, cancelados o comunidades a partir de registros informatizados".

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos.

De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos.

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

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

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

4.2.3. CHILE. Cuenta con una ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993, la cual en sus cuatro numerales menciona: Artículo 1° "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo". Artículo 2° " El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio". Artículo 3° "

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

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

Artículo 4° " El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

4.2.4. ESTADOS UNIDOS. Cabe mencionar, la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030). Que modificó al Acta de Fraude y Abuso Computacional de 1986.

Dicha acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año de prisión.

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

Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple que se debe entender como acto delictivo. Es interesante también señalar que el Estado de California, en 1992 adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta ley de 1994.

4.2.5. FRANCIA. Las disposiciones penales están contempladas en sus numerales del 41 al 44, los cuales contemplan lo siguiente:

Artículo 41" El que hubiere procedido o mandado proceder a la realización de tratamientos automatizados de información nominativa sin que hubieran sido publicados los actos reglamentarios previstos en el artículo 15 o formuladas las denuncias previstas en el artículo 16, supra, será castigado con pena de privación de libertad de seis meses a tres años y con pena de multa de 2 000 a 200 000 francos, o con una sola de estas dos penas. Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos, en las condiciones que determinare y a expensas del condenado".

Artículo 42 " El que hubiere registrado o mandado registrar, conservando o mandando conservar informaciones nominativas con infracción de las disposiciones de los artículos 25, 26 y 28, será castigado con pena de privación de libertad de uno a cinco años y con pena de multa de 20 000 a 2 000 000 francos, o con una de estas dos penas. Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos en las condiciones que determine, y a expensas del condenado.

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

castigado con pena de privación de libertad de dos a seis meses y con pena de multa de 2 000 a 20 000 francos, o con una de las dos penas. El que por imprudencia o negligencia, hubiere divulgado o permitido divulgar informaciones de la índole de las que se mencionan en le párrafo anterior, será castigado con pena de multa de 2 000 a 20 000 francos.

Artículo 44 "El que, disponiendo de informaciones nominativas con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento las hubiere desviado de su finalidad, según la misma hubiera sido definida, bien en el acto reglamentario previsto en el artículo 15, supra, o en las denuncias formuladas en aplicación de los artículos 16 y 17, bien en una disposición legal, será castigado con pena de privación de libertad de uno a cinco años y con multa de 20 000 a 2000 000 francos".

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

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

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

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

4.2.6.4. Fraude Informático. Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un injusto beneficio, ocasionando daño a otro. También se entiende como tal la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en ellos contenidos o pertenecientes a ellos, cuando se procure una ventaja injusta, causando daño a otro. La punibilidad de este tipo de delito es de meses a tres años de prisión, más una multa considerable.

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

4.2.6.6. Falsificación informática. Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. En este caso, se presupone la existencia de un documento escrito (aunque se debate doctrinariamente si los documentos electrónicos o virtuales pueden considerarse documentos escritos).

En este caso, la doctrina italiana tiene muy clara la noción de "documento informático", al cual define como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.

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

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

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

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

4.2.7. **República Portuguesa**, hace mención sobre la utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976, y la cual menciona:

Artículo 35: " Utilización de la Informática.

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

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

3. Queda prohibida la atribución de un número nacional único a los ciudadanos.

De lo anterior, se advierte que en diferentes países se han preocupado por el mal uso que pueda tener los grandes avances tecnológicos, el cual sin una reglamentación adecuada pueden desbordarse y salir de un control, así pues, la apremiante necesidad de que en nuestro Código Penal del Estado, se contemplen de una forma u otra.

La legislación y regulación sobre los delitos informáticos en otros países, constituye un gran avance para países como en el nuestro que no tienen una legislación al respecto, por lo anterior, no se va ha realizar una crítica a las anteriores disposiciones legales, ya que cada país contempló dichas normas de acuerdo a sus necesidades propias, como se puede observar en líneas precedentes, (ya que algunos países se enfocaron propiamente a proteger el derecho a la privacidad, y a la propiedad intelectual, o como el que disponga de informaciones nominativas y haga un mal uso de ello; otros tantos a proteger al patrimonio de las personas afectadas como en los fraudes informáticos etcétera).

Mas sin embargo como se mencionó con anterioridad, nos ayudan y nos dan la pauta para que nuestros legisladores contemplen las figuras delictivas de "delitos informáticos", de acuerdo a nuestra realidad.

4.3 LEGISLACION NACIONAL DEL DELITO INFORMATICO

En México, Internet no se ha regulado de manera expresa, como tampoco en el resto de los países latinoamericanos.

Su uso gira en torno a cierto Código Ético y la tendencia Institucional es que será un fenómeno "autor regulable. A pesar de los índices de crecimiento del uso de la computadora y de Internet, México enfrenta un problema social consistente en lo que denominamos "analfabetismo informático", del cual el Poder Legislativo no está exento, por lo que muchos congresistas no entienden el concepto y la estructura de Internet.

Asimismo, nos atrevemos a afirmar que tanto los jueces como los magistrados que forman parte del Poder Judicial tienen hoy día la misma carencia. Es difícil prever el pronunciamiento de los tribunales federales o de la Suprema Corte de Justicia Mexicanos en un caso cuya resolución se base esencialmente en un conflicto por el uso de Internet, por lo cual no se tiene conocimiento de la existencia de tesis ni jurisprudencia algunas que se refieran a los medios electrónicos en general y a Internet en especial.

Como se mencionó es un Código Ético el que puede regular la conducta de los usuarios, mas sin embargo, existe en nuestro país una regulación administrativa sobre las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos, en este sentido, se considera pertinente recurrir a aquellos tratados internaciones de los que el Gobierno de México es parte en virtud de que el artículo 133 Constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

4.4. CODIGO PENAL DEL ESTADO DE SINALOA

El único estado de la República que contempla en su legislación los delitos informáticos es el Estado de Sinaloa. Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos informáticos, se considera pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo. "Delitos contra el Patrimonio"

Capítulo V. Delito Informático.

Artículo 217.- Comete delito informático, la persona que dolosamente y sin derecho:

"1.- Use o entre a una base de datos, sistemas de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o´II.- Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistemas o red.

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

En el caso particular al que se refiere, cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

Se considera que se ubicó el delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícito, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad.

Por lo anterior, es necesario que en nuestro Estado, también exista una conciencia sobre la necesidad de legislar en este aspecto, creando el tipo penal adecuado a estas conductas antisociales, lo cual sería, un freno eficaz para su comisión.

Tal vez porque aún no se han visto en gran escala los estragos que pueden ocasionar estos tipos de conductas, y porque mucha gente aún no se ha incorporado al mundo de la telecomunicación, nuestros legisladores se han quedado al margen en cuanto a este aspecto.

4.5. LEY FEDERAL DE DERECHOS DE AUTOR Y CODIGO PENAL PARA EL DISTRITO FEDERAL EN MATERIA DEL FUERO COMUN Y PARA TODA LA REPUBLICA EN MATERIA DEL FUERO FEDERAL

Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997.

Esta ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos.

Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.

En este sentido, se considera importante detenernos en los artículo 102 y 231, el primero de ellos, regula la protección de los programas de computación y señala además que los programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos.

El segundo en su fracción V sanciona el comercio de programas de dispositivos o sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo.

Aún cuando la infracción se circunscribe al área del comercio, permite la regulación administrativa de este tipo de conductas ilícitas, como una posibilidad de agotar la vía administrativa antes de acudir a la penal.

Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, artículo 424, fracción IV del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal del que se infiere la sanción al uso de programas de virus.

Si bien pudiera pensarse que la inclusión de las sanciones a la fabricación de programas de virus en el Código Penal lleva implícito el reconocimiento de un delito informático debe tenerse presente que los delitos a regular en este título son en materia de derechos de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los delitos informáticos el bien jurídico serían por ejemplo el de la intimidad, patrimonio, etcétera.

CAPITULO V

“PRACTICAS DELICTIVAS A TRAVES DEL INTERNET”

En los albores del nuevo milenio, puede decirse que el siglo XXI ya ha comenzado con la llamada "revolución digital", la cual ha tomado forma mediante un complejo y laberíntico entramado de cables, satélites, redes, computadoras, televisores e impulsos electrónicos que constituyen la infraestructura del cyberespacio. Esta revolución, que encuentra en Internet su máxima expresión, es posible gracias al fenómeno de la convergencia, es decir, en el uso combinado de las computadoras y las redes de comunicación.

Los efectos de semejante transformación ya se están haciendo sentir en la ciencia, economía, la política, la sociedad, la cultura, la educación y entretenimiento. La forma en que nos interrelacionamos con los demás está siendo socavada por nuevas prácticas (compras on-line, chats, e-mail, educación a distancia, foros de discusión, etcétera) y ya nadie puede ser capaz de predecir exactamente cuán profundos serán los cambios. Los que sí parece ser notorio es que el cambio debe ocurrir simultáneamente en todos los ámbitos a fin de lograr un proceso de transición armónico. En esta era digital o de la informática, infinidad de instituciones, normas, leyes, costumbres, formas de pensar y de relacionarse resultan inadecuadas e inapropiadas y necesitan ser revisadas y actualizadas en forma urgente.

Además de todos los beneficios que la revolución digital conlleva, el cyberespacio puede ser también concebido como un ámbito propicio para la realización de conductas disvaliosas. A partir de la existencia de nuevas formas de operar con la tecnología delitos que no son nuevos, y ya existían desde mucho antes de la aparición de la informática, han planteado serios interrogantes que nuestro derecho positivo parece no saber cómo resolver.

Cualquiera de nosotros puede ser víctima de delitos, tanto en el mundo "real", por llamarlo de alguna manera, como del "virtual". Sin embargo, parecería que las conductas disvaliosas realizadas en éste último ámbito gozan de cierta impunidad.

Ciertas conductas como la destrucción de base de datos personales, el hurto o el fraude informático pueden resultar impunes en virtud de la falta de adecuación de la normativa vigente a las nuevas situaciones.

El principio de legalidad expresado en la máxima "nullum crimen nulla poena sine lege" el que establece que no hay delito ni pena sin ley penal anterior. En el orden penal la ley debe contener la descripción precisa de las acciones delictuosas, únicas conductas susceptibles de ser penadas.

Caso contrario, se estaría sancionando como delitos hechos no descriptos en la ley, con motivo de una extensión extralegal del ilícito penal y violando garantías constitucionales, como la que prescribe la analogía en materia penal, entendida ésta como la aplicación de la ley a un caso similar al legislado pero no comprendido en su texto.

Así pues, la proliferación de conductas disvaliosas que no encuentran un castigo adecuado demanda una mayor y más rápida actividad por parte de los legisladores. Esta es la mejor solución si queremos contar con un sistema jurídico seguro, que no de lugar a soluciones injustas y castigos no previstos expresamente por la ley. Son precisos y urgentes acuerdos internacionales a fin de armonizar criterios y evitar incompatibilidades entre distintos sistemas legales. El anquilosado ordenamiento jurídico se nos presenta como un aparato demasiado "pesado", lento y obsoleto, como para seguir el desenfrenado e imparable ritmo impuesto por el desarrollo de las tecnologías y hacer frente a los desafíos planteados por la revolución digital.

5.1 CONDUCTAS ILEGITIMAS MAS COMUNES:

A) HACKER: Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas. El término de hacker en castellano significa "cortador". Las incursiones de los piratas son muy diferentes y responden a motivaciones dispares, desde el lucro económico a la simple diversión.

Los "Hackers", son fanáticos de la informática, generalmente jóvenes, que tan sólo con un ordenador personal, un modem, gran paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, saltándose todas las medidas de seguridad, y leer información, copiarla, modificarla, preparando las condiciones idóneas para realizar un fraude, o bien destruirla. Se pueden considerar que hay dos tipos; 1) los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad; 2) los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables.

B) CRACKER: Para las acciones nocivas existe la más contundente expresión, "Cracker" o "rompedor", sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender; es decir, presenta dos vertientes, el que se cuela en un sistema informático y roba información o produce destrozos en el mismo, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anti-copia.

C) PHREAKER: Es el que hace una actividad parecida a la anterior, aunque ésta se realiza mediante líneas telefónicas y con y/o sin el auxilio de un equipo de cómputo. Es el especialista en telefonía, empleando sus conocimientos para poder utilizar las telecomunicaciones gratuitamente.

D) VIRUCKER: Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o inutilizar la información contenida. Existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

E) PIRATA INFORMATICO: Es quien reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor.

5.2 CONDUCTAS QUE SE COMETEN A TRAVES DE LA COMPUTADORA Y DEL INTERNET, TRADICIONALMENTE DENOMINADOS "DELITOS INFORMATICOS"

A pesar de que el concepto de delito informático engloba tanto los delitos cometidos contra el sistema como los delitos cometidos mediante el uso de sistemas informáticos, en este apartado se hablará del delito informático como aquél que está íntimamente ligado a la informática, es decir, las conductas realizadas a través del mundo virtual del ciberespacio.

A) FRAUDE INFORMATICO.- El fraude informático solo está limitado por la imaginación del autor, su capacidad técnica y las medidas de seguridad de la instalación. Se pueden clasificar en cuatro grupos: 1.- Intervención en los datos de entrada al sistema; 2.- Incorporación de modificaciones no autorizadas en los programas; 3.- Modificación fraudulenta de la información almacenada en el sistema. 4.- Intervención en las líneas de transmisión de datos.

B) ACCESO NO AUTORIZADO.- El uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

C) DESTRUCCION DE DATOS.- Son daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático.

D) INFRACCION DE LOS DERECHOS DE AUTOR.- Es la interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red.

E) INFRACCION DEL COPYRIGHT DE BASES DE DATOS.- Aún no existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet.

F) INTERCEPCION DE E-MAIL.- Constituye una violación de correspondencia, y la intercepción de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

G) ESTAFAS ELECTRONICAS.- La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra.

H) TRANSFERENCIA DE FONDOS.- Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático.- Como se puede observar, muchas de estas conductas no son irreales, es decir, las encontramos de una manera palpable, y cualquier persona que tenga conocimientos básicos de informática puede llegar a cometerlos.

5.3 DELITOS CONVENCIONALES QUE PUEDEN TRASLADARSE AL CIBERESPACIO

Al hablar de delitos convencionales, nos referimos a aquellos que tradicionalmente se han venido dando en la "vida real", sin el empleo de medios informáticos y que con la irrupción de las autopistas de la información se ha producido también en el ciberespacio.

Por mencionar algunos delitos, pueden ser el robo, el espionaje a través de un acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, o el espionaje industrial, el terrorismo mediante la existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo, siendo aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional, el propio narcotráfico ya que se ha utilizado a la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el bloqueo de dinero y para la coordinación de entregas y recogidas; así como más delitos como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

5.4. ESTADISTICA SOBRE DELITOS INFORMATICOS

Desde hace cinco años, en los Estados Unidos existe una institución que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos a través de las computadoras.

Esta entidad es El Instituto de Seguridad de Computadoras (CSI), quien anunció recientemente los resultados de su quinto estudio anual denominado "Estudio de Seguridad y Delitos Informáticos" realizado a un total de 273 Instituciones principalmente grandes Corporaciones y Agencias del Gobierno.

Este Estudio de Seguridad y Delitos Informáticos es dirigido por CSI con la participación Agencia Federal de Investigación (FBI) de San Francisco, División de delitos informáticos.

El objetivo de este esfuerzo es levantar el nivel de conocimiento de seguridad, así como ayudar a determinar el alcance de los Delitos Informáticos en los Estados Unidos de Norteamérica.

Entre lo más destacable del Estudio de Seguridad y Delitos Informáticos 2000 se puede incluir lo siguiente:

Violaciones a la seguridad informática.

Respuestas	PORCENTAJE (%)
No reportaron Violaciones de Seguridad	10%
 Reportaron Violaciones de Seguridad	90%

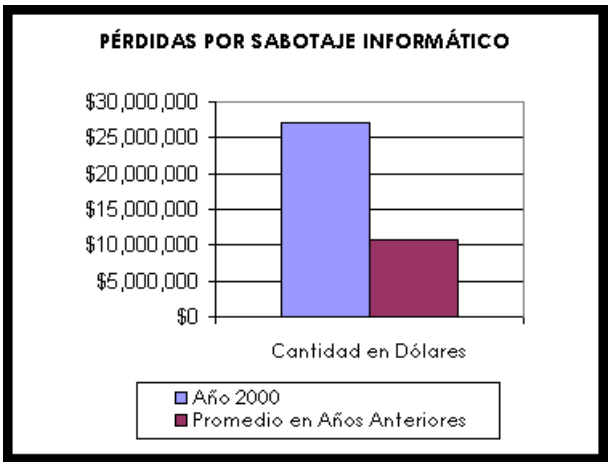
90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.

- 70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados -- por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

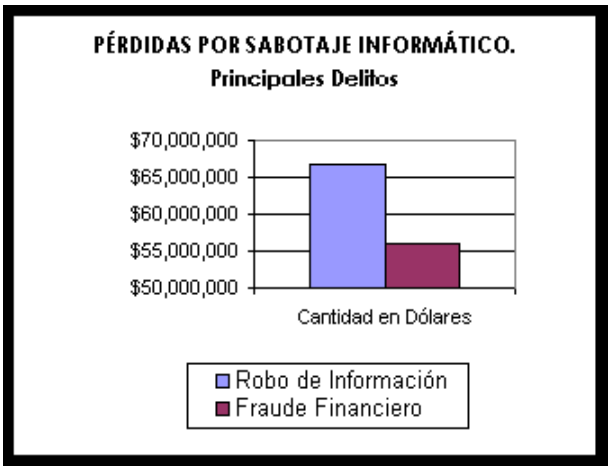
Pérdidas Financieras.

74% reconocieron pérdidas financieras debido a las violaciones de las computadoras.

- Las pérdidas financieras ascendieron a $265,589,940 (el promedio total anual durante los últimos tres años era $120,240,180).



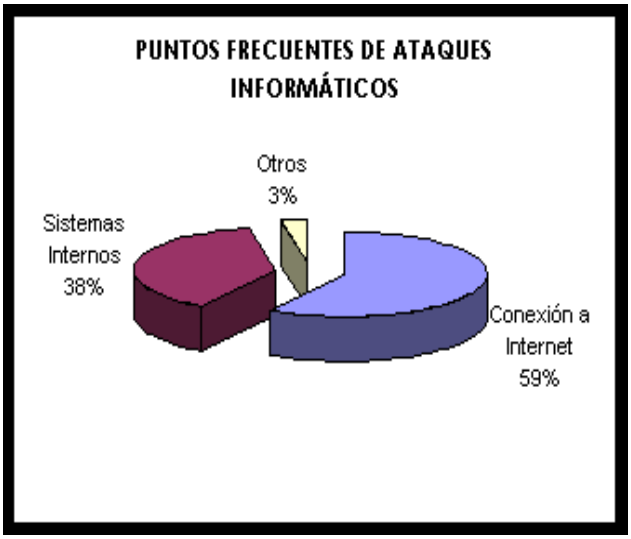
6I encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27,148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10,848,850.



Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) y el fraude financiero (53 encuestados informaron $55,996,000).

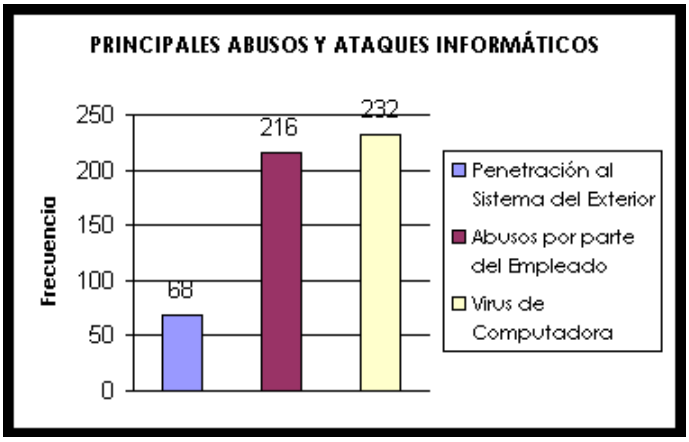
Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

Accesos no autorizados.



71% de los encuestados descubrieron acceso desautorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuestados (59%) mencionó su conexión de Internet como un punto frecuente de ataque, los que citaron sus sistemas interiores como un punto frecuente de ataque fue un 38%.

Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del "Estudio de Seguridad y Delitos Informáticos 2000" confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo.



Los encuestados detectaron una amplia gama a de ataques y abusos. Aquí están algunos otros ejemplos:

- 25% de encuestados descubrieron penetración al sistema del exterior.
- 79% descubrieron el abuso del empleado por acceso de Internet (por ejemplo, transmitiendo pornografía o pirateó de software, o uso inapropiado de sistemas de correo electrónico).
- 85% descubrieron virus de computadoras.
- Comercio electrónico.

Por segundo año, se realizaron una serie de preguntas acerca del comercio electrónico por Internet. Aquí están algunos de los resultados:

1. 93% de encuestados tienen sitios de WWW.
2. 43% maneja el comercio electrónico en sus sitios (en 1999, sólo era un 30%).
3. 19% experimentaron accesos no autorizados o inapropiados en los últimos doce meses.
4. 32% dijeron que ellos no sabían si hubo o no, acceso no autorizado o inapropiado.
5. 35% reconocieron haber tenido ataques, reportando de dos a cinco incidentes.
6. 19% reportaron diez o más incidentes.
7. 64% reconocieron ataques reportados por vandalismo de la Web.

8. 8% reportaron robo de información a través de transacciones.
9. 3% reportaron fraude financiero.

Conclusión sobre el estudio csi:

Las tendencias que el estudio de CSI/FBI ha resaltado por años son alarmantes. Los "Cyber crímenes" y otros delitos de seguridad de información se han extendido y diversificado. El 90% de los encuestados reportaron ataques. Además, tales incidentes pueden producir serios daños.

Las 273 organizaciones que pudieron cuantificar sus pérdidas, informaron un total de $265,589,940. Claramente, la mayoría fueron en condiciones que se apegan a prácticas legítimas, con un despliegue de tecnologías sofisticadas, y lo más importante, por personal adecuado y entrenando, practicantes de seguridad de información en el sector privado y en el gobierno.

Otras estadísticas:

- La "línea caliente" de la Internet Watch Foundation (IWF), abierta en diciembre de 1996, ha recibido, principalmente a través del correo electrónico, 781 informes sobre unos 4.300 materiales de Internet considerados ilegales por usuarios de la Red. La mayor parte de los informes enviados a la "línea caliente" (un 85%) se refirieron a pornografía infantil. Otros aludían a fraudes financieros, racismo, mensajes maliciosos y pornografía de adultos.
- Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.

- Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson[33] "Asecho cibernético: delito, represión y responsabilidad personal en el mundo online", publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.
- En Singapur El número de delitos cibernéticos detectados en el primer semestre del 2000, en el que se han recibido 127 denuncias, alcanza ya un 68 por ciento del total del año pasado, la policía de Singapur prevé un aumento este año en los delitos por Internet de un 38% con respecto a 1999.
- En relación con Internet y la informática, la policía de Singapur estableció en diciembre de 1999 una oficina para investigar las violaciones de los derechos de propiedad y ya ha confiscado copias piratas por valor de 9,4 millones de dólares.
- En El Salvador, existe más de un 75% de computadoras que no cuentan con licencias que amparen los programas (software) que utilizan. Esta proporción tan alta ha ocasionado que organismos Internacionales reacciones ante este tipo de delitos tal es el caso de BSA (Bussines Software Alliance).

Como se señaló, es indispensable el uso de la computadora y del manejo del Internet, para la comisión de conductas delictivas denominadas "Delitos Informáticos", sin embargo, aún en la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe una concepto propio de los llamados delitos informáticos.

Aún cuando no existe dicha definición con carácter universal, se han formulado conceptos funcionales atendiendo a las realidades concretas de cada país.

[33] www.asechocibernetico.com

Por lo que se refiere a nuestro país, cabe destacar lo mencionado por Julio Téllez Valdes, al decir que hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, requiere que la expresión "delitos informáticos" esté consignada en los Códigos Penales, lo cual en México, al igual que en otros muchos no ha sido objeto de tipificación aún.

Mencionando algunas de las diferentes definiciones que nos aportan estudiosos en la materia, sobre los Delitos Informáticos, diremos que para:

María de la Luz Lima[34], 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 cual en el concepto típico de Delitos Informáticos nos dice que "son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin". En el concepto atípico menciona que "son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin"[35].

El Departamento de Investigación de la Universidad de México, señala como delitos informáticos a "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático"Así pues, y realizando una definición personal sobre los delitos informáticos, diremos que: "son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal y que en su realización se valen de las computadoras como medio o fin para su comisión".

[34] Ibidem. Pág.74.
[35] Ibidem. Pág. 264.

CAPITULO VI

“LA NO REGULACIONSOBRE EL USO DEL INTERNET EN MEXICO”

6.1. ARGUMENTOS CONTRA LA REGULACIÓN

Frente a la corriente reguladora se levantan los partidarios de que ciertas áreas queden libres del intervencionismo o proteccionismo estatal. Entre los argumentos más utilizados figuran el derecho a la intimidad y la libertad de expresión.

6.1.1 DERECHO A LA INTIMIDAD

Uno de los derechos más defendidos en los países en los que ha habido una gran implantación de los sistemas informáticos en la gestión de los datos de los ciudadanos por parte de la Administración, ha sido el derecho de la persona a que su intimidad no sea vulnerada por un abuso de estos medios. La protección de este derecho ha generado preceptos de rango constitucional en muchos países. En España, el artículo 18 CE garantiza el secreto de las comunicaciones y abre la posibilidad de que la Ley limite el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Del desarrollo de este precepto ha surgido hasta ahora la LORTAD como instrumento destinado a evitar que mediante el tratamiento automatizado de los datos se llegue a obtener el perfil de una persona, sus aficiones y sus hábitos. Con ello se reconoce que el uso de las tecnologías de la información permite una rapidez en la manipulación de datos que era impensable con el empleo de medios manuales o analógicos. En la discusión de la LORTAD se llegó a establecer la comparación de que los sistemas manuales equivalían a pescar con caña y los informáticos a pescar con red.

La misma frase se ha repetido al hablar sobre el poder del Estado al investigar las transmisiones efectuadas en la infraestructura de la información, y concretamente al interceptar y leer el e-mail.

En la declaración de Phill Zimmermann ante el Subcomité de Política Económica, Comercio y Medio Ambiente de la Cámara de Representantes de los EEUU, puede leerse:

"En el pasado, si el Gobierno quería violar la intimidad de los ciudadanos corrientes, tenía que gastar sus recursos en interceptar, abrir al vapor y leer el correo y escuchar, grabar y transcribir las conversaciones telefónicas. Eso era como pescar con caña, de uno en uno. Por el contrario, los mensajes de e-mail son más fáciles de interceptar y se pueden scanear a gran escala, buscando palabras interesantes. Esto es como pescar con red, existiendo una diferencia orwelliana cuantitativa y cualitativa para la salud de la democracia"[36].

Con argumentos similares se está defendiendo la idea de que si los avances tecnológicos han creado un ciberespacio en el que cualquiera puede expresarse y comunicarse sin temor a ser oído por otros, el poder del Estado no debería ampliarse hasta poder controlar este nuevo mundo.

Por de pronto, el servicio secreto norteamericano ya ha sido condenado por introducirse sin mandamiento judicial en la BBS Esteve Jackson Gámez y leer el e-mail en ella depositado. El servicio secreto ha tenido que pagar una indemnización de 50.000 dólares al propietario de la BBS y 1.000 dólares a cada usuario de la misma, por haber vulnerado su intimidad.

6.1.2. LIBERTAD DE EXPRESIÓN

Pocas propuestas de ley han generado tanta discusión en Internet como la Communications Decency Act. Los detractores de este proyecto sostienen que no sólo prohibiría conversaciones públicas de contenido "obsceno, lascivo, sucio o indecente"[37] sino incluso las de ámbito privado entre dos personas, con la posibilidad de sancionar al proveedor del servicio on-line. Los usuarios de Internet americanos se niegan a tener que hablar constantemente como si estuviesen en un entierro.

[36] http://www.phantom.com
[37] Idem. Pág. Web anterior.

La aplicación de esta ley, además de ser un importante obstáculo para la libertad de expresión, exigiría una enorme inversión en la monitorización y vigilancia del sistema y generaría constantes intromisiones en la intimidad de los ciudadanos.

Durante el mes de abril y mayo de 1995, ha habido un importante movimiento para conseguir firmas de oposición a este proyecto.

La dirección donde debían enviarse los mensajes era s314-petition[arroba]netcom.com

6.1.3. LIBERTAD DE ACCESO A LA INFORMACIÓN

Una corriente de usuarios de la red considera que el derecho a la información está por encima de otros derechos como la propiedad intelectual, la propiedad de los datos el secreto que se da al know how. Los partidarios de esta idea consideran que cualquier tipo de obra introducida en la red debería pertenecer al dominio público, y solicitan la inaplicabilidad de los derechos de autor y la supresión de fronteras en el ciberespacio para permitir el libre flujo de la información en todo el planeta.

6.1.4. AUTO REGULACIÓN: CÓDIGOS DE CONDUCTA Y CIBERPOLICIAS

Códigos de conducta: Por el momento, y a falta de una legislación específica, en Internet existen unos códigos de ética cuyo incumplimiento está castigado con la censura popular, lo cual acaba siendo, en algunos casos, más eficaz que una norma de derecho positivo.

Es posible que un usuario se marque unas pautas de conducta de acuerdo con unas leyes, pero la distancia o la ausencia de control de los órganos de vigilancia pueden hacer que esas pautas se relajen.

No obstante, si sabemos que podemos ser juzgados por nuestros compañeros de la red y somos conscientes de que de nuestro comportamiento en los debates on-line y en la emisión y recepción de mensajes dependerá la opinión que tengan de nosotros y la calificación de novato, informal o persona non grata que podamos recibir, actualizaremos nuestras pautas de conducta día a día.

Ello hace que la tónica normal en Internet sea de respeto entre los usuarios de la red, siendo los demás casos la excepción.

Sistemas de seguridad informática: Las propios sistemas de control de cada host garantizan un umbral de seguridad aceptable, aunque no impiden que los archivos que circulan por la red puedan contener algún virus.

Y en muchos casos pueden ser neutralizados por un programa generador de passwords. Ciberpolicías: Tanto NSA, FIRST Forum of Incident Response and Security Teams y CERT Computer Emergency Response Team tienen equipos de especialistas dedicados a la localización de hackers, defensa frente a sabotajes e intervención en caso de siniestros informáticos. Por otra parte, algunas policías como el FBI y Scotland Yard disponen de unidades especiales para investigar la comisión de delitos a través de la red.

6.1.5. SITUACIÓN ACTUAL Y PROPUESTAS LEGISLATIVAS

El Código Penal de 1995 contiene muchas referencias a los delitos informáticos y a los derivados del uso de las telecomunicaciones, entre las que podemos destacar las siguientes:

- Delitos contra la intimidad y el secreto de las comunicaciones

- Estafas electrónicas.

- Infracción de los derechos de propiedad intelectual

- Delito de daños

- Revelación de secretos contenidos en documentos o soportes informáticos.

- Falsedad en documento electrónico

- Fabricación o tenencia de útiles e instrumentos específicamente destinados a la comisión de delitos.

- Sustracción, destrucción, inutilización u ocultación de documentos electrónicos por parte de un funcionario público cuya custodia le esté encomendada por razón de su cargo.

Por otra parte, algunas leyes como por ejemplo la LORTAD, incluyen en su articulado referencias a la seguridad informática de las bases de datos.

Pero en general, los españoles estamos algo desprotegidos frente a la nueva categoría de delitos que hemos comentado en este artículo.

Proyectos de ley de EEUU: Después del atentado de Oklahoma, el gobierno norteamericano ha empezado a estudiar formas de investigación y prevención antiterrorista. Ante la sospecha de que en la organización del atentado se utilizara la red Internet para el envío de mensajes encriptados, la propuesta de ley antiterrorista de los senadores Dole y Hatch incluyen la ampliación de las facultades del FBI en materia de vigilancia electrónica y rastreo de la red.

Otro proyecto de la Casa Blanca modifica las leyes que regulan la intimidad y la intervención de las telecomunicaciones (Privacy Act y Wiretap Act) para poder interceptar y desencriptar mensajes electrónicos enviados o recibidos por sospechosos o presuntos terroristas, con plena eficacia procesal como prueba documental incluso cuando dichas evidencias hayan sido obtenidas sin el correspondiente mandamiento judicial.

Este proyecto también prevé la asignación de una partida presupuestaria para que el Fiscal General pueda solicitar a compañías telefónicas, electrónicas y de seguridad informática el diseño de tecnologías de intervención de las telecomunicaciones.

Todo ello va acompañado de un intenso debate sobre las posibilidades de desencriptación y la posible vulneración del derecho a la intimidad, al que antes he hecho referencia.

GATT - Ronda de Uruguay: En los últimos acuerdos del GATT se hacen referencias al nuevo entorno económico y tecnológico y a la necesidad de acuerdos globales en materia de Propiedad Industrial e Intelectual, pero no se analizan a fondo ni se resuelven los problemas que se han mencionado en este artículo.

Reuniones del G7 respecto a la Global Infraestructure Información: Las conclusiones del G7 en sus últimas reuniones han supuesto un enorme esfuerzo de síntesis para resumir en unos puntos básicos las actuales necesidades en materia normativa, frente al reto de la sociedad de la información. A continuación se enumeran algunas de las conclusiones más significativas:

a) La necesidad de analizar el alcance del derecho de información frente a la seguridad de la información.

c) La conveniencia o no de seguir limitando la cobertura del copyright a la expresión, en un contexto en el que la expresión es a veces menos importante que la propia información.

d) La necesidad de modificar los conceptos tradicionales del derecho de autor.

e) La necesidad de proteger las herramientas de navegación en el nuevo contexto digital.

f) La necesidad de analizar el impacto en el derecho de autor de nuevos conceptos como "almacenamiento temporal", "browsing" y "cita digital".

g) La necesidad de que el uso de las tecnologías de la información también es importante para los países en vías de desarrollo.

Proyecto de Libro Verde: La Comisión Europea ha editado un Libro Verde sobre los derechos de autor y los derechos conexos en la sociedad de la información. Entre las propuestas que contiene este texto cabe destacar:

a) La existencia de ventanillas únicas para contratar telemáticamente los derechos necesarios para crear obras multimedia, facilitando así la localización de los titulares y el pago de los royalties correspondientes a las imágenes, textos, sonidos y videos utilizados.

b) La determinación del derecho aplicable en los casos de infracciones transfronterizas a través de la infraestructura de la información.

c) La armonización del derecho de los estados miembro para proteger de manera uniforme los derechos de las obras multimedia y de las bases de datos que se hallen en la infraestructura de la información.

d) La necesidad de redefinir del concepto de reproducción por medios digitales, planteando la cuestión de si la digitalización de una obra y la copia privada deberán ser objeto de autorización por parte del titular o no.

e) La necesidad de definir el concepto de transmisión digital de una obra en el seno de la infraestructura de la información con el fin de determinar si constituye un nuevo acto que precisa autorización del autor o si, por el contrario, está integrado en otros derechos como el de cesión, distribución o comunicación pública.

f) La conveniencia o no de regular las medidas de protección, seguridad informática, passwords y encriptación.

6.2. DERECHO A LA INTIMIDAD, A LA LIBERTAD DE EXPRESION Y AL LIBRE ACCESO A LA INFORMACION

Frente a la corriente reguladora se levantan los partidarios de que ciertas áreas queden libres del intervencionismo o proteccionismo estatal. Entre los argumentos más utilizados figuran el derecho a la intimidad y la libertad de expresión. Uno de los derechos más defendidos en los países en los que ha habido una gran implantación de los sistemas informáticos en la gestión de los datos de los ciudadanos por parte de la administración, ha sido el derecho a la persona a que su intimidad no sea vulnerada por un abuso de estos medios.

La protección de éste derecho ha generado preceptos de rango constitucional en muchos países.

Otra figura es el Derecho a la Libertad de Expresión, la cual en nuestro país se encuentra contempla en sus artículos 6 y 7 de nuestra Carta Maga, los cuales a la letra dicen:

Artículo 6. " La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho a la información será garantizado por el Estado".

Artículo 7. " Es inviolable la libertad de escribir y publicar escritos sobre cualquier materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública. En ningún caso podrá secuestrarse la imprenta como instrumento del delito.

Las leyes orgánicas dictarán cuantas disposiciones sean necesarias para evitar que so pretexto de las denuncias por delitos de prensa, sean encarcelados los expendedores, "papeleros", operarios y demás empleados del establecimiento de donde haya salido el escrito denunciado, a menos que se demuestre previamente la responsabilidad de aquellos".

Ahora bien, la Constitución Política del Estado de Michoacán, menciona en su artículo 1, lo siguiente: " En el Estado de Michoacán de Ocampo todo individuo gozará de las garantías que otorga la Constitución Política de los Estados Unidos Mexicanos, así como de los demás derechos establecidos en esta Constitución y en las leyes que de ambas emanen".

Lo más característico del hombre, lo que lo distingue de los demás seres de la naturaleza, es la facultad de concebir ideas y poderlas transmitir a sus semejantes. Por eso la libertad de expresión es el derecho más propiamente humano, el más antiguo y el origen y base de otros muchos. Nuestra Constitución, fiel a su estructura democrática y a la tradición liberal que recoge, garantiza el derecho a la libertad de expresión en su artículo 6°, en forma general y en el 7° que establece la libertad de escribir y publicar obras sobre cualquier materia.

Así pues, es el derecho que tenemos a manifestarnos libremente, siempre y cuando no sean atacados derechos de terceros, a la moral, se provoque algún delito o perturbe el orden público.

Garantizándose también el derecho a la información. Teniendo que ser aplicable dicho precepto Constitucional, al comunicarse, manifestar sus ideas y obtener información a través del ciberespacio.

La libertad de acceso a la información (como se observó en líneas recedentes, consagrada en nuestra Carta Magna), es otro tema importante a tocar, una corriente amplia de usuarios de la red considera que el derecho a la información está por encima de otros derechos como la propiedad intelectual. Los partidarios de esta idea consideran que cualquier tipo de obra introducida en la red debería pertenecer al dominio público.

De todo lo anteriormente dicho, es creíble que en la libertad de expresión y en el derecho a la información deben estar garantizados, independientemente de cualquier medio de manifestación. Por lo tanto, el Internet no debe quedar al margen, siendo ésta la red de redes más importante y con mayor tráfico de información a nivel mundial. La libertad de información en Internet es un fenómeno muy interesante. Esa red permite la difusión y el acceso a gran número de documentos, obras multimedia, conciertos, música, base de datos, archivos, información económicas, tecnológica, películas; incluso permite la telefonía a costos de llamadas locales.

El acceso a toda esta información debe facilitarse a todos los interesados a un precio razonable, sin perder de vista los derechos de propiedad intelectual, en particular las leyes internacionales y locales de derechos de autor. El debate sobre los límites de la regulación de Internet es global, pero las tendencias en Estados Unidos y en los países europeos tendrán, sin duda, una influencia directa tanto en la regulación mexicana como en la de otras naciones.

Podemos señalar, por poner un caso, que la reciente sentencia de la Corte Suprema de Estados Unidos sobre la Libertad de expresión y el Derecho a la Información en Internet, en defensa de las normas constitucionales, tendrá una vasta influencia ene l mundo.

Así pues, en México, la libertad de expresión se fundamenta en los artículos 6° y 7° Constitucionales, así como en la Ley Federal de Imprenta, la Ley de Radio, y Televisión y Cinematografía, así como en la reciente Ley Federal de Derechos de Autor. Estos marcos jurídicos definen los límites de la libertad de expresión mediante el concepto de difamación.

Asimismo, el Código Penal Federal y los Códigos Penales estatales limitan la libertad de expresión mediante el concepto de difamación. (contemplado y sancionado en los artículos 250 y 251 del Código Penal del Estado de Michoacán).

Por lo tanto, se considera que la libertad de expresión y el Derecho a la información se deben de dar en todos los ámbitos incluyendo a la red de redes (internet), sin perder de vista, los derechos del hombre, ya que para ser respetados, deben ser respetables. La libertad de expresión ya no lo es si ataca la vida privada, es decir cuando se cause odio, desprecio o demérito hacia una persona, o con tal actitud se le perjudica en sus intereses, a la moral cuando se defiendan o aconsejen vicios, faltas o delitos, o se ofenda al pudor, decencia o buenas costumbres, y a la paz pública, cuando se desprestigien, ridiculicen o destruyan las instituciones fundamentales del país, se injurie a México, se lastime su buen crédito, o se incite al motín a la rebelión o a la anarquía.

CAPITULO VII

"EL DERECHO PENAL EN MICHOACAN FRENTE AL USO DEL INTERNET COMO INSTRUMENTO DE DELITO"

7.1. EL CODIGO PENAL MICHOACANO Y SU NECESIDAD DE ADAPTACIÓN AL SIGLO XXI

En México, no se contemplan los delitos informáticos en ninguna legislación penal, propiamente en el estado de Michoacán con excepción del estado de Sinaloa, por ello es importante adicionar estas conductas antijurídicas a nuestra legislación estatal, para evitar, daños graves a los usuarios del internet, como medio de trabajo y desarrollo de sus actividades cotidianas. protegiendo su integridad y patrimonio.

Como se expuso con anterioridad en los países más desarrollados ya se ha legislado al respecto, por el contrario en el estado de Michoacán quizás el legislador considera que no es un asunto de relevancia para introducirse en esta área y crear las normas jurídicas adecuadas para frenar con estos actos jurídicos provocados por el mal uso de la red, por lo tanto, es de gran relevancia que se regule adecuadamente el uso de la red como medio de protección al usuario, ya que por la facilidad de acceso al internet cualquier persona con intensiones delictivas puede realizar conductas que impliquen responsabilidad penal, sin embargo, y en vista de que en nuestro estado no existe nada al respecto, permite que éstas queden impunes o bien se tipifiquen en otro delito que no es aplicable muchas veces al caso concreto.

En consecuencia, es importante adicionar en nuestro Código Penal del estado de Michoacán, un capitulo en donde se contemple el uso del internet como instrumento para cometer delitos que contempla el código penal para el estado de Michoacán.

Consistente en el derecho que tiene una persona de no ser molestada o sufrir invasión a su persona o a su información personal, así como a sus relaciones y comunicaciones privadas, entre las que cuenta las comunicaciones electrónicas en este caso el Internet.

El Derecho Mexicano no ha reglamentado esta garantía individual que se deduce de las libertades de la persona en el aspecto espiritual, o sea la libertad de intimidad, no obstante que existen varios artículos como lo son el 16, 24, 25 y 26 Constitucionales, que se refieren a la inviolabilidad de correspondencia, libertad de intimidad e inviolabilidad del domicilio, con el propósito de garantizar jurídicamente el derecho a la privacidad, toda persona requiere de mandamiento judicial escrito, fundado y motivado para hacer molestado en su persona, familia, domicilio, papeles o posesiones. Es decir, no puede violarse la intimidad de ningún individuo sin un mandamiento judicial escrito, conforme a derecho y con fundamento a la ley. Desafortunadamente, la realidad es otra en cuanto a este derecho, por falta de regulación; es uno de los menos respetados, tanto por violaciones del orden común como de la misma autoridad.

El concepto de vida privada, en relación con la informática y telemática, tiene un doble significado.

Por un lado la protección de la vida privada, estricto sensu, se refiere al problema de la información sensible, definida aquella como relativa al origen racial, a las opiniones públicas, religiosas y membresías sindicales, información que no puede ser recopilada ni procesada electrónicamente salvo que exista autorización expresa del autor; por el otro lado, el manejo y registro de otro tipo de información puede también causar atentados a la vida privada estricto sensu, pero en relación con el ámbito social al que pertenece. En México, es necesario reconocer la importancia del Internet como un medio de comunicación de tecnología avanzada además de fomentarse la defensa del derecho de autodeterminación informática.

Por lo que el Capítulo I del Título Décimo Tercero del Código Penal del Estado de Michoacán, se pudiese adicionar el final del mismo, como Delito contra la Libertad y Seguridad de las Personas una cuestión referente a la informática, tomando como base lo siguiente: Será considerado como Delito contra la Libertad de las Personas: "Cuando un individuo almacene, comunique, modifique o cancele un proceso de una base de datos a partir de registros informatizados personales, sin la autorización de su autor o de mandato judicial, deberá sancionársele con la penalidad de 1 uno a 6 seis años de prisión y multa de cien a quinientos días de salario al momento en que se haya cometido el delito".

A manera de explicación, consideré necesario señalar esta hipótesis por principio, en este Título Décimo Tercero de los Delitos contra la Libertad y Seguridad de las Personas, en virtud, de que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, pues debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el Derecho a la intimidad o privacidad de las personas.

En lo que concierne al contenido de dicha hipótesis es debido a que en la actualidad por medio de las computadoras y del Internet, las personas físicas cuentan en sus bases de datos con información confidencial, la cual hace referencia a muchas cuestiones personales, sin embargo, existen sujetos que son capaces de introducirse a dicha información electrónica evadiendo las contraseñas e introduciéndose a nuestro sistema informático sin la autorización de su creador o de mandamiento judicial, lo que implica un gran riesgo personal a la privacidad, sin estar legislado penalmente en nuestra entidad.

Referente a la penalidad que pretendo se imponga por este tipo de conductas, creo que es la adecuada, ya que como mencioné en líneas precedentes, es importante que se proteja la base de datos que pudiera tener una persona, ya que ésta es confidencial, lo cual atacaría el bien jurídico tutelado de la privacidad, y por las características de dicha conducta, además pueden provocar pérdidas económicas, con o sin un beneficio para los que la cometen; pudiendo ser cometidos imprudencialmente, pero en la mayoría de los casos, es una conducta que se realiza con la intención de transformar o difundir una información contenida en una base de datos; siendo importante señalar que son muchos los casos en que se produce este tipo de conductas, por lo cual considero adecuada la penalidad que pretendo en dicha hipótesis.

Al respecto, de no imponer una sanción menor es porque se ha visto en la práctica desafortunadamente que la imposición de sanciones menores no desalienta la comisión de estos delitos, es por ello que sancionar con una pena más elevada implica que el sujeto, en caso de que realice su conducta e intente hacerlo de nuevo es sabedor de que será una pena elevada que le causará más perjuicio, que el beneficio que haya obtenido de su conducta.

Ahora bien, dichas conductas pueden causar en la mayoría de los casos un beneficio económico para quien las cometen y por consiguiente un detrimento patrimonial de sus víctimas, por eso, menciono las siguientes hipótesis referentes a los Delitos Informáticos, las cuales se encontrarían en el Título Décimo Octavo, de los Delitos contra el Patrimonio en el Código Sustantivo del Estado:

I. "Cuando una persona se introduzca o use un sistema o red de computadoras sin tener derecho a ello, con el objeto de obtener un lucro indebido, o información delicada. Igualmente al que altere el funcionamiento de sistemas informáticos o telemáticos procurando una ventaja injusta, causando daño a otro.

II. Al que de forma dolosa causen perjuicio a un soporte lógico, sistema de red de computación o los datos contenidos en la misma, o introduzca virus que causen daños al sistema ya sea bloqueando, modificando o destruyendo datos o dañando el hardware. Al responsable de estos delitos se le impondrá una sanción de 3 tres a 8 ocho años de prisión y multa de cien a quinientos días de salario mínimo vigentes en el momento de la comisión del delito".

Hemos visto en la actualidad, que estos supuestos se realizan con mayor frecuencia, pues con los avances tecnológicos estas conductas son fáciles de cometer y difíciles de descubrir. Muchos de los fraudes o robos que se realizan son cometidos mediante manipulación de computadoras; en muchas ocasiones se realizan cuando el sujeto se encuentra en horas de trabajo, siendo acciones de oportunidad y ocasionando en éstos casos en particular, serias pérdidas económicas pero a la vez traduciéndose en beneficios para los que las comenten. Son conductas que en milésimas de segundos y sin una necesaria presencia física pueden llegar a consumarse; en la mayoría de los casos son muy sofisticados, lo cual implica grandes dificultades para su comprobación y, desafortunadamente, hasta el momento siguen siendo ilícitos impunes. Ya que éstas conductas no se encuentran contempladas en nuestra legislación penal, y que la mayoría de las veces al no existir un tipo penal adecuado al caso, el sujeto que las comete no se le sanciona; lo que ha permitido, con el desarrollo de la tecnología, que cada día se cometan con mayor frecuencia, por lo que considero que esta adición, sería un freno eficaz contra esas acciones. Al imponerle una penalidad mínima de tres años, es por tratarse de un delito patrimonial, y ver como afecta en forma cuantiosa al daño que cause con su accionar el sujeto que comete el delito, también lo es, que por tratarse de una situación demasiado actual, es obligado a que se ponga un alto en este tipo de delito, no obstante que a criterio de muchos juristas, la elevación de las penas, no es el medio adecuado para acabar con la delincuencia, sin embargo, en nuestro país, es el más útil y que en la práctica a dado resultado.

Consecuentemente, lo que se pretende con el planteamiento de las anteriores hipótesis y propuestas, es que conductas que se están realizando puedan castigarse y no quedan impunes, es decir, que se establezca en nuestra legislación penal estatal, los "Delitos Informáticos", con lo cual nuestros juzgadores tengan un tipo penal adecuado a este tipo de conductas.

CONCLUSIONES

Al inicio de la vida en sociedad el hombre, se vio en la necesidad de cuantificar sus pertenencias y por ello, ha tenido que procesar datos, limitándose en un principio al número de sus dedos, después a cuentas de granos y objetos similares, posteriormente, inventó sistemas numéricos que le permitieron realizar sus operaciones con mayor confiabilidad y rapidez, inventando al paso de los siglos el ábaco, las tablas de logaritmos (1614), la regla de cálculo (1630), las tarjetas perforadoras (1804) hasta la creación de la computadora en 1937 conocida como "MARK", la cual en pocos años ha sufrido una transformación tan rápida, convirtiéndose en la herramienta más importante en la sociedad actual.

A través de la tecnología y de la computadora se ha tenido en diferentes campos innumerables avances, como lo es en el científico, en la educación, la medicina, el entretenimiento, y en cualquier área donde el hombre se desempeña laboralmente. No se podría imaginar ahora en el siglo XXI al hombre sin la ayuda de las computadoras.

El origen del Internet en el año de 1969, creado exclusivamente a proyectos de Investigación Avanzada en Estados Unidos (ARPA), se desarrolló tan rápidamente creando lo que ahora conocemos como Internet en 1991, la cual es una red diseñada por uniones de redes de computo, con la capacidad de transmitir comunicaciones rápidamente sin el control de persona o empresa determinada y con la habilidad automática de renrutar datos.

Son diversos los servicios que nos brinda el Internet, desde la transferencia de archivos, pasando por las páginas word wide web (www) hasta una comunicación en tiempo real con una persona que se encuentre en cualquier parte del mundo.

Es sumamente sencillo el acceso a la red de Internet, encontrándose tanto en universidades, bibliotecas, oficinas gubernamentales y hasta las "cibercafeterias"; el espíritu de la información que se maneja en Internet es que sea pública, libre y accesible, así pues, hoy en día esta red de redes entrelaza a 60 millones de computadoras personales, las cuales se rigen en la mayoría de los casos por un Código ético entre sus usuarios, nos tendremos que enfrentar indudablemente en un futuro próximo a una avalancha de conductas ilícitas a través de este medio.

PROPUESTAS

Al respecto propongo:

I) Al respecto considero y propongo que sí debe de legislarse, claro, siempre y cuando el legislador tenga presente los preceptos constitucionales 6° y 7°, donde exista una libertad de expresión y el derecho a la información; teniendo presente que la libertad de expresión ya no lo es, si ataca la vida privada, a la moral, y a la paz pública.

Al estudiar todo lo referente a los Delitos Informáticos, me di cuenta de la importancia que están cobrando y que es verdaderamente apremiante que nuestros legisladores locales empiecen a trabajar al respecto. Es por ello que menciono algunas hipótesis que se pudieran dar al cometer actos por medio del uso de las computadoras.

La primera de ellas, que a continuación menciono, propongo se incluya en el Capítulo I del Título Décimo Tercero del Código Penal del Estado de Michoacán, en los Delitos contra la libertad y Seguridad de las Personas:

I.- Cuando un individuo almacene, comunique, modifique o cancele un proceso de una base de datos a partir de registros informatizados personales, sin la autorización de su autor o de mandato judicial, deberá sancionársele con la penalidad de 1 uno a 6 seis años de prisión y multa de cien a quinientos días de salario al momento en que se haya cometido el delito.

En el Título Décimo Octavo de los Delitos contra el Patrimonio en el Código Penal del Estado propongo se adicione:

I.- Cuando una persona se introduzca o use un sistema o red de computadoras sin tener derecho a ello, con el objeto de obtener un lucro indebido, o información delicada. Igualmente al que altere el funcionamiento de sistemas informáticos o telemáticos procurando una ventaja injusta, causando daño a otro.

II.- Al que de forma dolosa causen perjuicio a un soporte lógico, sistema de red de computación o los datos contenidos en la misma, o introduzca virus que causen daños al sistema ya sea bloqueando, modificando o destruyendo datos o dañando el hardware.-

Al responsable de estos delitos se le impondrá una sanción de 3 tres a 8 ocho años de prisión y multa de cien a quinientos días de salario mínimo vigentes en el momento de la comisión del delito.

Las anteriores propuestas de los Delitos Informáticos la baso en lo siguiente:

I.- Primordialmente, en la imperante necesidad de que nuestros legisladores locales tomen conciencia sobre la importancia que revisten este tipo de conductas obviamente antijurídicas y se empiece a legislar al respecto, ya que hay muchas conductas que implican responsabilidad para aquellos que las cometen, sin embargo, y en vista de que en nuestro Estado no existe nada al respecto, permite que éstas queden impunes o bien se tipifiquen en otro delito que no es aplicable muchas veces al caso concreto.-

II.- En que este tipo de conductas afecta no solamente como bien jurídico tutelado al patrimonio, sino también a la libertad de privacidad e intimidad de las personas, contempladas en los artículos Constitucionales 16, 24, 25 y 26.

III.- En el Derecho que tiene una persona de no ser molestada o sufrir invasión a su persona o a su información personal, así como a sus relaciones y comunicaciones privadas, sin perder de vista que se esta hablando sobre las comunicaciones electrónicas, el Internet o un soporte de datos. Por lo cual, la primera de las hipótesis la contemplo en el Capítulo I del Título Décimo Tercero del Código Penal del Estado de Michoacán, de los Delitos contra la libertad y Seguridad de las Personas.

Por lo que toca a la penalidad que menciono en la primera de las propuestas de 1 un año a 6 seis años de prisión y multa de cien a quinientos días de salario, al momento en que se haya cometido el delito; es porque este tipo de conductas pueden afectar gravemente a sus víctimas, al introducirse a una información electrónica sin la autorización de su creador y obtener de dicha información un beneficio que pudiera ser o no económico. Hay que tener en cuenta, que los sujetos activos de éstos delitos son personas con un status socioeconómico elevado, que generalmente los cometen para obtener un lucro indebido a sabiendas de que es difícil que se descubran.

IV.- Como se ha mencionado, los Delitos Informáticos afectan principalmente el patrimonio de sus víctimas, es por ello, que propongo su adición en el Título Décimo Octavo de los Delitos contra el Patrimonio en el Código Sustantivo del Estado. Ya que si lo que se pretende es sancionar a aquellas personas que se introduzca a un sistema o red de computadoras sin tener derecho a ello, y con el objetivo de obtener un beneficio, cualquiera que sea; así como también al que en forma dolosa cause perjuicio a un soporte lógico o sistema de red de computación ya sea en forma manual o por la introducción de cualquier tipo de virus de los que ya se han mencionado y explicado anteriormente.

Lo que se pretende es que, como estas conductas se realizan con mayor frecuencia, a través de la manipulación de computadoras, realizando fraudes informáticos o transferencia de fondos, las sanciones que se contemplen sean elevadas.

Como se observa en la primera de las hipótesis se contempla una penalidad de 1 un año a 6 años de prisión y una multa de cien a quinientos días de salario al momento de la comisión del delito y en las dos restantes una penalidad de 3 tres a 8 ocho años de prisión, con la misma multa que la primera, esto es debido al daño que se causa a sus víctimas, y la forma en que se cometen dichas conductas, no obstante que a criterio de muchos juristas, la elevación de las penas no es el medio adecuado para acabar con la delincuencia.

FUENTES DE INFORMACIÓN

1. BIBLIGRAFICAS

.
MALO CAMACHO, Gustavo; “DERECHO PENAL MEXICANO”
Editorial Porrúa. S.A.
México. 1998.

.
GONZALEZ DE LA VEGA, Francisco; “DERECHO PENAL MEXICANO”
Editorial Porrúa. S.A.
México 1996.
pp. 473.

Betancourt López, Eduardo; “TEORIA DEL DELITO”.
Editorial Porrúa. S.A.
México 1994.
pp. 304.

TRATADO DE LOS DELITOS Y DE LAS PENAS.
BECCARIA.
Editorial Porrúa, S.A.
México 1995.
Pp. 408.

.
González Quintanilla, José Arturo;” DERECHO PENAL MEXICANO. (PARTE GENERAL)”
Editorial Porrúa, S.A.
México 1993.
pp. 504.

Villalobos, Ignacio. “DERECHO PENAL MEXICANO”
Editorial Porrúa, S.A.
México 1975.
pp. 650.

Barrios Garrido Gabriela, Muñoz de Alba M Marcia, Pérez Bustillos Camilo.
"INTERNET Y DERECHO EN MEXICO".
Edt. Mc Graw Hill.
México 1998.
pp.180.

Téllez Valdes Julio. "DERECHO INFORMATICO".
Edt. Mc Graw Hill.
México, Segunda Edición 1996.
pp.283.

Barragán, Julia. "INFORMATICA Y DECISION JURIDICA"
Distribuciones Fontamara S.A.
Primera Edición 1994, México.
pp 184.

DICCIONARIO DE LA MICROCOMPUTACION T. II.
pp. 632.

.
MOLINA ENZO MORA José Luis,. "INTRODUCCION A LA INFORMATICA"
1974.

"INTRODUCCION A LA TEORIA DE COMUNICACIÓN DE MASAS".
Mc Quail.
Paidos Comunicación,
Barcelona 1983.

CASTELLANOS TENA; Fernando; "LINIEMIENTOS ELEMENTALES DEL DERECHO PENAL"Editorial. Porrúa Edición. Cuarta.

2. LEGISLACIÓN

CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS.
Cuadernos Michoacanos de Derecho.
Edt. ABZ
MEXICO: ESTA ES TU CONSTITUCION.
Rabasa, O Emilio, Caballero Gloria.
Cámara de Diputados. Legislatura LI.
Cuarta Edición 1982.
pp. 264.

CONSTITUCION POLITICA DEL ESTADO DE MICHOACAN.
Cuadernos Michoacanos de Derecho.
Edt. ABZ.

CODIGO PENAL DEL ESTADO DE MICHOACAN.
Cuadernos Michoacanos de Derecho.
Edt. ABZ.
CODIGO PENAL DEL ESTADO DE SINALOA.

3. INTERNET:

1. Reducing the risks of Internet connection and use: FIPS, CSL, FIRST y CERT

FIPS: gopher://csrc.ncsl.nist.gov:71/11/nistpubs/fips46-2.txt

CSL: gopher://csrc.ncsl.nist.gov:71/00/nistbul/csl7-93.txt

FIRST: http://csrc.ncsl.nist.gov/

CERT: ftp://ftp.cert.org/

2. Communications Decency Act:

http://www.eff,org/pub/EFF/Legislation/Bills_new/s314.bill

http://www.phantom.com/(slowdog/

http://www.panix.com/vtw/exon/exon.html

3. Derecho a la intimidad y seguridad de la información:

SERVICOM:

Derecho a la intimidad:

Profesionales/Librería Legislación B+/eff0803.txt

Informática/Internet/alt.privacy

Fraudes informáticos:

Informática/Forum/Legislación

Otros temas:

Profesionales/Internet/alt.comp.acad-freedom.t/Protecting Kids from porn on WEB

Servidor de la Universidad Autónoma de Sinaloa.
Spapalazu@themis.derecho.unam.max
Ultima Actualización, mayo 1997.