UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

“LA NECESIDAD DE LEGISLAR EL DELITO DE FRAUDE ELECTRÓNICO DERIVADO DE LA PRÁCTICA DEL COMERCIO POR INTERNET”

T E S I S

P A R A O B T E N E R E L T Í T U L O D E

L I C E N C I A D A E N D E R E C H O

P R E S E N T A :

M I R N A H E I D Y C R U Z C R U Z

ASESOR: LIC. MTRA. MARÍA GRACIELA LEÓN LÓPEZ.

MÉXICO 2008

AGRADECIMIENTOS

A mis padres Clara Cruz Clemente y Francisco Cruz Ojeda, con un profundo respeto les agradezco de todo corazón su cariño, comprensión, apoyo y sobre todo la confianza que siempre me han brindado. Gracias por ser el pilar de mi vida, todo se los debo a ustedes, los quiero mucho.

Agradezco a mis hermanos Nadia, Sandra, Wendy, Erika, Verónica, Xóchitl y Ernesto, el cariño, compañía y apoyo que me brindan, ya que han sido la fortaleza para lograr mis objetivos, sé que cuento con ustedes siempre.

Gracias a ti Nay, porque eres nuestro ejemplo a seguir y nuestro orgullo, gracias por enseñarme que no hay límites, que lo que me proponga lo puedo lograr y que sólo depende de mí, gracias por tu ayuda, consejos, comprensión y cariño, te quiero mucho hermana.

Agradezco a Dios por permitirme llegar hasta este momento tan importante de mi vida y lograr otra meta más en mi carrera, gracias por llenar mi vida de dichas y bendiciones.

Agradezco a mi asesora la Lic. Mtra. María Graciela León López, por su disposición y ayuda brindadas en este trabajo, ya que sin ella no hubiera sido posible. Gracias por sus consejos, paciencia y opiniones.

Gracias a cada uno de los maestros que participaron en mi desarrollo profesional durante mi carrera, sin su ayuda y conocimientos no estaría en donde me encuentro ahora. Gracias a la Universidad Nacional Autónoma de México y a la Facultad de Estudios Superiores Aragón por darme la oportunidad de ser un miembro de su grandiosa familia.

LA NECESIDAD DE LEGISLAR EL DELITO DE FRAUDE ELECTRÓNICO DERIVADO DE LA PRÁCTICA DEL COMERCIO POR INTERNET.

ÍNDICE

INTRODUCCIÓN

El presente trabajo de investigación se crea debido a la problemática de la sociedad moderna mediante la cual la evolución tecnológica ha generado un importante número de conductas nocivas que, aprovechando el poder de la información, buscan lucros ilegítimos y causan daños.

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general. Los llamados delitos informáticos, no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquélla.

Debido a que la computadora se ha convertido en una herramienta indispensable para el desarrollo humano, gracias a toda esta tecnología computacional podemos hacer uso de estos servicios libremente con el sólo hecho de conectarnos a el Internet, por medio de una línea telefónica y un módem; lamentablemente la tecnología no se ha ocupado solamente para el beneficio del hombre, sino que algunos individuos han traspasado los límites, de la seguridad y realizado actos ilícitos, lo que ha generado una gran preocupación por parte de los usuarios de este medio informático.

Creo que ésta es una visión demasiado limitada de la realidad; esto puede ser así si pensamos tan sólo en delitos del tipo de un apunte informático falso en un banco o del robo de una cantidad de dinero gracias a la utilización ilícita de una tarjeta de crédito. Pero existen muchos otros delitos que difícilmente podemos tipificar con las leyes actuales, y que éstas rápidamente se tendrán que adaptar o redactar acorde a los nuevos tiempos que impone el uso de las tecnologías de la información ¿Cómo no se va a hablar constantemente de lagunas o de falta de regulación si las leyes no cambian?.

La insuficiencia de los instrumentos penales del presente para evitar y castigar las distintas formas de delitos informáticos supone un reto tanto a los estudiosos del derecho como a nuestros legisladores. Tampoco podemos estar ajenos los que estudiamos la abogacía.

La dificultad de tipificar penalmente situaciones sometidas a un constante cambio tecnológico, la manifiesta insuficiencia de las sanciones en relación con la gravedad y el daño de los delitos informáticos y la propia inadecuación de los medios penales tradicionales, para remediar esta situación, ha venido favoreciendo a que dichas conductas se realicen más usualmente sin ser castigadas.

En el primer capítulo hablaremos acerca del delito, su definición legal y doctrinal, haciendo un análisis de diferentes definiciones dadas por estudiosos del derecho, hasta llegar a una personal. Asimismo, analizaremos sus elementos tanto positivos como negativos.

El segundo capítulo podrá adentrarnos al estudio de los llamados delitos electrónicos, se hará una breve reseña acerca de la estructura de la computadora, así como también haremos referencia a conceptos, antecedentes y desarrollo del internet. Asimismo veremos como el internet a través del tiempo ha ido generando diversas funciones para los cibernautas creando hasta el día de hoy no sólo beneficios sino fines ilícitos a través de las computadoras. También se hace referencia acerca de las personas que pueden ser sujetos del delito de fraude electrónico; así como las características que deben reunir los delitos electrónicos.

El tercer capítulo trata la problemática jurídica en que se encuentra nuestro país al no regular principalmente este delito de fraude electrónico por internet, ya que es sólo uno de los delitos que no están contemplados en el Código Penal y requieren análisis urgente ya que constituyen una gran laguna en nuestras leyes. Por lo que en este capítulo analizaremos las legislaciones de algunos países en

los que ya contemplan dichas figuras delictivas, mencionando en forma especial, al Estado de Sinaloa ya que es el único en la República Mexicana que contempla dichos delitos.

En el cuarto capítulo se estudiará la utilización de la computadora y del Internet para la comisión de conductas ilícitas, aquí analizaremos cada uno de los conceptos de esas conductas ilegítimas así como su clasificación. Asimismo se hará referencia a 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. Por lo anterior también se busca una solución del problema que se puede generar en caso de uso fraudulento de los servicios del internet.

En el capítulo quinto se verá la otra cara de la moneda, la que apoya la no regulación de la práctica y uso del internet, ya que argumentan el derecho a la intimidad, a la libertad de expresión y al libre acceso a la información, existiendo partidarios de que ciertas áreas queden libres de intervencionismo o proteccionismo estatal. Asimismo se analizarán los argumentos que existen para que no se regule la práctica y uso del Internet y, de forma particular, porque considero que se deben de incorporar los Delitos Informáticos en el Código Penal para el Distrito Federal, con la finalidad de proteger jurídicamente a la sociedad como sujeto pasivo en sentido amplio, para evitar la impunidad ante este tipo de conductas delictivas.

CAPÍTULO I. EL DELITO.

1.1. El Delito, definición legal y doctrinal.

La noción legal la encontramos en el artículo 7° de l Código Penal Federal, "Delito es el acto u omisión que sancionan las leyes penales".

La palabra delito, proviene del latín *delicto* o *delictum*, supino del verbo *delinqui*, *delinquere*, que significa desviarse, resbalar, abandonar. [1]

"El delito es un hecho del hombre que vulnera las condiciones de existencia, de conservación, de desarrollo de una sociedad en un momento determinado y por el cual se prevé para el sujeto agente como consecuencia, una pena de naturaleza aflictiva en cuanto comporta privación o disminución del disfrute de determinados bienes jurídicos (vida, libertad personal, patrimonio, etcétera)".[2]

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".

---

[1] Rafael Márquez Piñero, *Derecho Penal. Parte general*, 4ª. ed., Trillas, México, 1999, pág.133.

[2] José Arturo González Quintanilla, *Derecho Penal Mexicano. Parte general,* Porrúa, México, 1993, pág. 170.

Para González Quintanilla, el Delito "es una acción típica, antijurídica y culpable".

Para Ignacio Villalobos, el Delito "es un acto humano típicamente antijurídico y culpable".

Para Rafael de Pina Vara, el Delito "es un acto u omisión constitutivo de una infracción de la ley penal".

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

1.2. Elementos del delito.

Los elementos del delito son cada una de las partes que lo integran; dicho de otra manera, el delito existe en razón de la existencia de los elementos: conducta, tipicidad, antijuricidad, culpabilidad, imputabilidad, punibilidad y condicionalidad objetiva.[3] Los elementos del delito son los aspectos positivos, a cada uno de los cuales corresponde uno negativo, que constituye la negación de aquél; significa que anula o deja sin existencia al positivo y, por tanto, al delito.

Elementos integrantes del delito:

a. El delito es un acto humano, es un actuar (acción u omisión). Un mal o un daño, aun siendo muy grave, tanto en el orden individual como en el colectivo, no es delito si no tiene su origen en un comportamiento humano. Los hechos de los animales, los sucesos fortuitos, como extraños a la actividad humana, no constituyen delito.

[3] Griselda Amuchategui Requena, *Derecho Penal,* 3ª. ed., Oxford, México, 2007.

b. El acto humano ha de ser antijurídico, ha de estar en contradicción en oposición, a una norma jurídica; debe lesionar o poner en peligro un interés jurídicamente protegido.

c. Además de esa contraposición con la norma jurídica, es necesario que el hecho esté previsto en la ley como delito, que se corresponda con un tipo legal; es decir, ha de ser un acto típico. No toda acción antijurídica constituye delito, sino que ha de tratarse de una antijuricidad tipificada.

d. El acto humano (acción u omisión) debe estar sancionado con pena, pues de ahí deriva la consecuencia punible. Si no hay conminación de penalidad, no existiría delito.[4]

Si concurren todos estos elementos, habrá delito.

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, los siguientes:

Positivos	**Negativos**
Conducta	Ausencia de conducta
Tipicidad	Ausencia de tipo o atipicidad.
Antijuricidad	Causas de justificación.
Imputabilidad	Inimputabilidad.
Culpabilidad	Inculpabilidad.
Condicionalidad objetiva	Falta de condiciones objetivas.
Punibilidad	Excusas absolutorias.

1.3. Conducta o hecho.

[4] Rafael Márquez Piñero, *op.cit*., pág.135.

La conducta es el primer elemento básico del delito, y se define como el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito. Lo que significa que sólo los seres humanos pueden cometer conductas positivas o negativas, ya sea una actividad o inactividad respectivamente. Es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito porque tiene una finalidad al realizarse la acción u omisión.

La conducta puede ser de acción (movimiento corporal consciente que provoca un cambio peligroso) o de omisión (ausencia del movimiento corporal esperado por la ley o que no evita la producción del resultado material) y ésta última se subdivide en omisión simple (inactividad ante el deber de obrar legalmente establecido, que actualiza la hipótesis preceptiva y es sancionado conforme a ésta) y comisión por omisión (no evitación de la producción de un resultado material delictivo, cuando se tiene la obligación de evitarlo).

Elementos de la conducta:

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.

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.

Elementos de la acción:

a) Voluntad. Es el querer, por parte del sujeto activo, cometer el delito. Es propiamente la intención.

b) Actividad. Consiste en el "hacer" o actuar. Es el hecho positivo o movimiento corporal humano encaminado a producir ilícito.

c) Resultado. Es la consecuencia de la conducta; el fin deseado por el agente y previsto en la ley penal;

d) Nexo de causalidad.- Es el ligamen o nexo que une a la conducta con el resultado, el cual debe ser material. Dicho nexo es el que une la causa con el efecto, sin el cual este último no puede atribuirse a la causa.

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

La omisión tiene cuatro elementos:

a) Manifestación de la voluntad. Consiste en la realización o en la omisión voluntaria de un movimiento del cuerpo.

b) Una conducta pasiva. (inactividad).

c) Deber jurídico de obrar.

d) Resultado típico jurídico. Es la consecuencia de la conducta

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

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

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

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.

El fraude es un delito de acción respecto al elemento engaño, a virtud de que el agente requiere realizar un acto positivo, consistente en un movimiento corporal, para que se produzca el resultado.

La conducta en el delito de que se trata consiste en efectuar una manipulación informática, emplear datos sin estar autorizado legítimamente para ello, o ejecutar un artificio semejante.

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. Ausencia de acción es la realización de la acción sin la voluntad del agente (Código Penal Federal, art. 15 fracción I).

1.4. Típico.

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".

En cuanto a la ausencia del tipo, ésta se produce cuando el legislador, por defecto técnico o deliberadamente, no describe una conducta que, según el sentir general, debía haber sido definida y fijada en los preceptos penales, dejando sin protección punitiva a los intereses violados. [5]

Castellanos Tena señala que hay ausencia de tipo cuando el legislador no describe la conducta y hay ausencia de tipicidad cuando hay tipo legal pero la conducta no se amolda a él.

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

[5] Rafael Márquez Piñero, *op. cit.*, pág.232.

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 (Código Penal Federal, art. 15 fr. II). 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.

Nadie puede ser sancionado penalmente si la conducta no se encuentra prevista como delictiva en un ordenamiento vigente con anterioridad al hecho.

1.5. Antijurídico.

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.

Clases de antijuricidad:

Material. Es propiamente lo contrario a derecho, por cuanto hace a la afectación genérica hacia la colectividad.

Formal. Es la violación de una norma emanada del Estado.

El aspecto negativo de la antijuricidad es la causa de justificación o licitud, que son las razones o circunstancias que el legislador consideró para anular la antijuricidad de la conducta típica realizada, al estimarla lícita, jurídica o justificativa.

De manera genérica el Código Penal Federal las maneja como causas de exclusión del delito, como se observa en el artículo 15 que mezcla distintas circunstancias entre ellas las de justificación.

1.6. Culpabilidad.

De acuerdo con Castellanos Tena "existe culpa cuando se realiza la conducta sin encaminar la voluntad a la producción de un resultado típico, pero éste surge a pesar de ser previsible y evitable, por no ponerse en juego, por negligencia o imprudencia, las cautelas o precauciones legalmente exigidas".[6]

Los requisitos que se requieren para que exista culpa:

- por ser necesaria la conducta humana para la existencia del delito, ella constituiría el primer elemento; es decir, un actuar voluntario (positivo o negativo);
- en segundo término que esa conducta voluntaria se realice sin las cautelas o precauciones exigidas por el Estado;
- tercero: los resultados del acto han de ser previsibles y evitables y tipificarse penalmente; por último, precisa una relación de causalidad entre el hacer o no hacer iniciales y el resultado no querido.

[6] Fernando Castellanos Tena, *Lineamientos elementales de Derecho Penal, 40ª. ed., Porrúa, México, 1999, pág.*246.

La culpabilidad es la relación directa que existe entre la voluntad y el conocimiento del hecho con la conducta realizada.

Existe culpa cuando no se provee el cuidado posible y adecuado para no producir, o en su caso evitar, la lesión típica, previsible y provisible, se haya o no previsto.

Para Vela Treviño, la culpabilidad es el elemento subjetivo del delito y el eslabón que asocia lo material del acontecimiento típico y antijurídico con la subjetividad del autor de la conducta.

Podemos definir la culpa como aquél resultado típico y antijurídico, no querido ni aceptado, previsto o previsible, derivado de una acción o una omisión voluntarias, y evitables si se hubieran observado los deberes impuestos por el ordenamiento jurídico y aconsejable por los usos y costumbres.

El aspecto negativo es la inculpabilidad que es la ausencia de culpabilidad, significa la falta de reprochabilidad ante el derecho penal, por faltar la voluntad o el conocimiento del hecho. Esto tiene una relación estrecha con la imputabilidad; así no puede ser culpable de un delito quien no es imputable, (por error, inculpable ignorancia (Código Penal Federal, art. 15 fracción VIII), obediencia jerárquica, eximentes putativas, violencia moral y miedo, estados de necesidad en que colisionan bienes de igual jerarquía y no exigibilidad de otra conducta (Código Penal Federal, art. 15 fracción I).

1.7. 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.

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”.

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".

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

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”.

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

Es decir, 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.

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.

Es imputable quien goza de salud mental, no se encuentra afectado por sustancias que alteren su comprensión y tiene la edad que la ley señala para considerar a las personas con capacidad mental para ser responsables del delito; en la mayoría de los estados de la República es a partir de los 18 años.

El aspecto negativo de la imputabilidad es la inimputabilidad, consistente en la ausencia para querer y entender en el ámbito del derecho penal. 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, (Código Penal Federal, art. 15 fracción VII).

La imputabilidad no es mencionada, por tratarse de una referencia al delincuente, no al delito.

1.8. Forma de comisión de los delitos.

El Código Penal para el Distrito Federal, establece en su artículo 18:

> "Artículo 18. (Dolo y culpa). Las acciones u omisiones delictivas solamente pueden realizarse dolosa o culposamente.
>
> Obra dolosamente el que, conociendo los elementos objetivos del hecho típico de que se trate, o previendo como posible el resultado típico, quiere o acepta su realización.

> Obra culposamente el que produce el resultado típico, que no previó siendo previsible o previó confiando en que no se produciría, en virtud de la violación de un deber de cuidado que objetivamente era necesario".

El dolo consiste en causar intencionalmente el resultado típico, con conocimiento y conciencia de la antijuricidad de hecho. También se le conoce como delito intencional o doloso.[7]

Elementos. Los elementos del dolo son dos: **ético**, que consiste en saber que se infringe la norma, y **volitivo**, que es la voluntad de realizar la conducta antijurídica.

Clases de dolo:

- *Directo*. El sujeto activo tiene intención de causar un daño determinado y lo hace, de manera que existe identidad entre la intención y el resultado típico; por ejemplo, el agente desea violar y lo hace.
- *Indirecto o eventual.* El sujeto desea un resultado típico, a sabiendas de que hay posibilidades de que surjan otros diferentes; por ejemplo, alguien quiere lesionar a un comensal determinado, para lo cual coloca una sustancia venenosa en la sal de mesa, sabiendo que podrán resultar lesionados otros sujetos.
- *Genérico.* Es la intención de causar un daño o afectación, o sea, la voluntad consciente encaminada a producir el delito.
- *Específico*. Es la intención de causar un daño con una especial voluntad que la propia norma exige en cada caso, de modo que deberá ser objeto de prueba.

[7] Griselda Amuchategui Requena, *op. cit.,* pág. 19.

- *Indeterminado*. Consiste en la intención de delinquir de manera imprecisa, sin que el agente desee causar un delito determinado; por ejemplo, colocar una bomba para protestar por alguna situación de índole política: el sujeto sabe que causará uno o más daños, pero tiene intención de infligir alguno en particular.

La culpa es el segundo grado de culpabilidad y ocurre cuando se causa un resultado típico sin intención de producirlo, pero se ocasiona por imprudencia o falta de cuidado o de precaución, cuando pudo ser previsible y evitable. La doctrina le llama delito culposo, imprudencial o no intencional.[8]

Los elementos de la culpa son:

- Conducta (acción u omisión).
- Carencia de cuidado, cautela o precaución que exigen las leyes.
- Resultado previsible y evitable.
- Tipificación del resultado.
- Nexo o relación de causalidad.

Cada elemento de la culpa se explica por sí mismo, de modo que no se detallarán por ser entendibles.

Las clases de culpa son:

- *Consciente*. También llamada con revisión o con representación, existe cuando el activo prevé como posible el resultado típico, pero no lo quiere y tiene la esperanza de que no se producirá.
- *Inconsciente.* Conocida como culpa sin previsión o sin representación, existe cuando el agente no prevé el resultado típico; así, realiza la conducta

[8] Griselda Amuchategui Requena, *op. cit.*, pág. 20.

sin pensar que puede ocurrir el resultado típico y sin prever lo previsible y evitable.

Dicha culpa puede ser lata, leve y levísima:

a) Lata. En esta culpa hay mayor posibilidad de prever el daño

b) Leve. Existe menor posibilidad que en la anterior.

c) Levísima. La posibilidad de prever el daño es considerablemente menor que en las dos anteriores.

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".[9]

Por lo anterior, se concluye que el dolo es intencional, ya que el sujeto conoce o prevé el resultado típico y asimismo quiere y acepta su realización; y, por el contrario la culpa genera un resultado típico sin intención de producirlo, pero se ocasiona por imprudencia o falta de cuidado o de precaución, cuando pudo ser previsible y evitable.

[9] Rafael Márquez Piñero, *op. cit.*, pág.293.

CAPÍTULO II. CONCEPTOS Y ANTECEDENTES DEL INTERNET Y DE LOS DELITOS INFORMÁTICOS, SU CLASIFICACIÓN Y CARACTERÍSTICAS.

2. I. Conceptos y Antecedentes del Internet.

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, etcétera, entraremos al conocimiento y manejo de lo que es la computadora en nivel operacional y estructural, (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, disquetes entre otros.

b) **Procesador Central**: dispositivo en que se ejecutan las operaciones lógico-matemáticas, conocido más comúnmente como unidad central del proceso, (CPU, por sus siglas en inglés).

c) Dispositivo de almacenamiento: contiene o almacena la información a procesar.

d) Elementos de Salida: son 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:

1) Hardware: está constituido por las partes mecánicas, electromecánicas y electrónicas, como estructura física de las computadoras, encargadas de la captación, almacenamiento y procesamiento de información, así como la obtención de resultados, conocido comúnmente como el equipo.

2) Software: 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 **"CIBERNÉTICA**" 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 esta ciencia, están relacionados con cualquier campo de estudio. Sus aspectos formales estudian una teoría general del control, extractada de los campos de aplicación y adecuada para todos ellos.

La noción de **"INFORMÁTICA",** 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". [1] 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. Lozano, caracteriza a la informática como un producto de la cibernética, en tanto un proceso científico relacionado con el tratamiento automatizado de la información en un plano interdisciplinario.

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 Internet es una libre asociación de miles de redes y millones de computadoras alrededor del mundo, que trabajan juntas compartiendo información".[2]

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.

---

[1] Julio Téllez Valdés, *Derecho Informático,* 3ª. ed., Mc Graw Hill, México, 2004, pág. 4.

[2] Finnie, Scott, Internet and on line services, http://webopedia.internet.com/ internet and on line services/internet/internet.html.

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.

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 súper 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, una de las redes más coordinadas, como CSNET (red de ciencias de cómputo) empezó 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 centros de investigación, reemplazando así a ARPANET en el trabajo de redes de investigación. ARPANET se da de baja en marzo de 1990 y CSNET (red de ciencias de cómputo) 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 cómputo, con la capacidad de transmitir comunicaciones rápidamente sin el control de persona o empresa comercial alguna y con la habilidad automática de reenrutar 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 esta 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 este medio puede viajar por cualquiera de

diversas rutas, hasta llegar a su destino, y en caso de no encontrarlo, será reenrutado 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 ha dado lugar a una normatividad sin fronteras y de lo cual podemos deducir, en términos jurídicos, cuál 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 e 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 cibercafeterías, lo cual está estrechamente relacionado con el número de proveedores de servicios de Internet.

Los orígenes de INTERNET en México se remontan a 1987. En 1992 se crea Mexnet, Asociación Civil, una organización de instituciones académicas que buscaba promover el desarrollo de Internet mexicano, establecer un blackbone nacional, crear y difundir una cultura de redes y aplicaciones en relación a Internet y contar con conexiones a nivel mundial.

INTERNET EN MÉXICO, fue el primer país latinoamericano en conectarse a Internet, en febrero de 1989, a través de los medios de acceso e interconexión de teléfonos de México.

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.

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

a) **correo electrónico**, 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 cómputo por interconexión, (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) **world 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 discusión (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.

2.2. Conceptos de Delitos Informáticos.

Las redes de comunicación electrónica y los sistemas de información forman parte integrante de la vida diaria de los ciudadanos en el mundo y desempeñan un papel fundamental en el éxito de la economía universal. Cada vez están más interconectados y es mayor la convergencia de los sistemas de información y las redes.

Esta tendencia implica sin duda, numerosas y evidentes ventajas, pero va acompañada también de un riesgo inquietante de ataques malintencionados contra los sistemas de información.

Los ataques contra los sistemas de información constituyen una amenaza para la creación de una sociedad de la información más segura y de un espacio de libertad, seguridad y justicia, por lo que es importante abordar la temática con la mayor seriedad posible.

Los delitos informáticos son aquellas actividades ilícitas que:

- Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o
- Tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos *per se*).

También se puede definir al delito informático como la conducta típica, antijurídica, culpable y punible, en que se tiene a las computadoras como instrumento o fin.

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.

Delitos Informáticos: Son todos aquellos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por medio de la utilización indebida de medios informáticos.

Delitos electrónicos o informáticos electrónicos: son una especie del género delitos informáticos en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios.

Son delitos electrónicos, por el tipo de bien afectado y salvo algunos casos nos encontramos frente a un caso de delito de daños. Los delitos electrónicos son perpetrados por medio del uso de la informática, razón por la cual no cabe menos que inferir que los delitos electrónicos son una especie del género de los informáticos.

Por lo que se refiere a nuestro país, cabe destacar lo mencionado por Julio Téllez Valdés, 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 países no ha sido objeto de tipificación aún.

Mencionando algunas de las diferentes definiciones que nos aportan estudiosos en la materia, sobre los Delitos Informáticos, Carlos Sarzana, en su obra Criminalista y Tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".[3]

[3] Gabriel Andrés Cámpoli, *Derecho Penal Informático en México,* INACIPE, México, 2004, pág.11.

Para Hilda Callegari, el delito informático es "aquel que se da con la ayuda de la informática o de técnicas anexas".[4]

Rafael Fernández Calvo, define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos…".[5]

María de la Luz Lima, dice que el "**delito electrónico** 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 como método, medio o fin".[6]

Delitos electrónicos o informáticos electrónicos. Son una especie del género delitos informáticos en los cuales el autor produce un daño o intromisión no autorizada en aparatos electrónicos ajenos –y que a la fecha por regla general no se encuentran legislados-, pero que poseen como bien jurídico tutelado en forma específica la integridad física y lógica de los equipos electrónicos y la intimidad de sus propietarios.[7]

---

[4] Gabriel Andrés Cámpoli, *op.cit.,* pág.11.

[5] Gabriel Andrés Cámpoli, *op.cit., pág.* 14.

[6] Gabriel Andrés Cámpoli, *op.cit.*, pág.14.

[7] Gabriel Andrés Cámpoli, *op.cit.*, pág.16.

El Dr. Julio Téllez Valdés, 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". [8]

En el **concepto atípico** menciona que "son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin".[9]

Ahora bien, 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".

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora" y "delincuencia relacionada con el ordenador".

En este orden de ideas, en el presente trabajo se entenderá como "delito electrónico en un sentido amplio cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin".

[8] Gabriel Andrés Cámpoli, *op.cit.*, pág.16.

[9] Gabriel Andrés Cámpoli, *op.cit.*, pág.17.

2.3. Características y Clasificación de los Delitos Informáticos.

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. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales y en ocasiones van más allá de la intención (preterintencionales).

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. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.[10]

[10] Julio Téllez Váldes, op.cit., pág. 81.

Para la comisión de dicha conducta, encontraremos a uno o varios sujetos activos como también pasivos.

Sujetos del delito: son las personas cuyos intereses (uno ilegítimo que arremete al otro) colisionan en la acción delictiva. Pueden ser indeterminados, cuando la ley no requiere una característica específica (*al que*), o determinados, cuando se requiere de una calidad especial para poder cometer el delito (ser servidor público para poder cometer uno de los delitos cometidos por los servidores públicos, por ejemplo, o ser mayor de doce años y menor de dieciocho para poder sufrir el delito de estupro).

El **sujeto activo**: Es la persona física que comete el delito; se llama también delincuente, agente o criminal. En lo que se refiere al delito que analizamos en el presente trabajo 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.

Lo puede ser sólo la persona física, pues una acción que constituye un delito tiene una naturaleza tal, que no puede ser realizada por un ente colectivo (*societas delinquere non potest*), aunque se ha establecido la posibilidad de aplicar consecuencias jurídicas a éstos, en casos determinados.

El **sujeto pasivo o víctima del delito** Es la persona física y moral sobre quien recae el daño o peligro causado por la conducta del delincuente. Por lo general, se le denomina también víctima u ofendido.

El maestro Carrara dice que el sujeto pasivo del delito es el hombre o la cosa sobre que recaen los actos materiales del culpable.

Para Cuello Calón, sujeto pasivo del delito es el titular del derecho o interés lesionado o puesto en peligro por el delito.

¿Quiénes pueden ser sujetos pasivos del delito?

1. La persona individual, sin distinción de sexo, estado mental, edad, posición social o económica, cualquiera que sea su condición jurídica durante el periodo vital.
2. Las personas jurídicas o morales, que pueden serlo en las infracciones contra su patrimonio (defraudaciones, etcétera) o contra su honor o reputación (injurias, etcétera).
3. El estado puede ser sujeto pasivo del delito, contra la seguridad de la nación y pública.
4. La colectividad social puede ser también sujeto pasivo del delito, de forma muy específica en aquellas infracciones atentatorias de su propia seguridad.[11]

El sujeto pasivo es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera, que usan sistemas automatizados de información, generalmente conectados a otros.

[11] Rafael Márquez Piñero, *op. cit*, pág.134.

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.

Por lo anterior, se puede apreciar que los que cometen este tipo de ilícitos, son personas con conocimientos sobre la informática y cibernética, los cuales, se encuentran en lugares estratégicos o con facilidad para poder acceder a información de carácter delicado, como puede ser a instituciones crediticias o del gobierno, empresas o personas en lo particular, dañando en la mayoría de los casos el patrimonio de la víctima, la cual, por la falta de una ley aplicable al caso concreto, no es denunciada quedando impune estos tipos de conductas.

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 objetivo. 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 Valdés, clasifica a los delitos informáticos:

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:

1. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
2. Variación de los activos y pasivos en la situación contable de las empresas.
3. Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).
4. Robo de tiempo de computadora.
5. Lectura, sustracción o copiado de información confidencial.
6. Modificación de datos tanto en la entrada como en la salida.
7. Aprovechamiento indebido o violación de un código para penetrar a un sistema con el fin de introducir instrucciones inapropiadas (esto es lo que se conoce en el medio como el método del Caballo de Troya).
8. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta apócrifa, método conocido como la técnica de salami.
9. Uso no autorizado de programas de cómputo.
10. Insertar instrucciones que provocan interrupciones en la lógica interna de los programas, a fin de obtener beneficios.
11. Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajo.
12. Acceso a áreas en forma no autorizada.
13. Intervención de las líneas de comunicaciones de datos o teleproceso.

Como Fin u Objetivo. En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

1. Programación de instrucciones que producen un bloqueo total al sistema.
2. Destrucción de programas por cualquier método.
3. Daño a la memoria.

4. Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).

5. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

6. Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etcétera.[12]

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

1.- Los que utilizan la tecnología electrónica como método. Los individuos utilizan métodos electrónicos para llegar a un resultado ilícito

2.- Los que utilizan la tecnología electrónica como medio. Son aquellas conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

3.- Los que utilizan la tecnología electrónica como fin. Son las dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Clasificación de las Naciones Unidas

Por su parte, el Manual de las Naciones Unidas para la prevención y control de delitos informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen trasnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera los problemas que rodean a la cooperación internacional en el área de delitos informáticos[13]:

[12] Pablo Andrés Palazzi, *Delitos Informáticos,* AD-HOC, Buenos Aires, Argentina, 2000, pág.166.

[13] Pablo Andrés Palazzi, *op. cit.*, págs. 167 y 168.

1. Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
2. Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
3. Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
4. No existe uniformidad entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
5. Carácter trasnacional de muchos delitos cometidos mediante el uso de computadoras.
6. Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

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

1. Acceso no autorizado: uso ilegítimo de passwords y la entrada a un sistema informático sin la autorización del propietario.
2. Destrucción de datos: los daños causados en la red mediante la introducción de virus, bombas lógicas, entre otros.
3. Infracción a los derechos de autor de bases de datos: uso no autorizado de información almacenada en una base de datos.
4. Intervención de e-mail: Lectura de un mensaje electrónico ajeno.
5. **Fraudes electrónicos: a través de compras realizadas haciendo uso de la red.**
6. Transferencias de fondos: engaños en la realización de este tipo de transacciones.
7. Spamming: Es el envío masivo de correos electrónicos en forma deliberada, con el propósito de bloquear un sistema.

Los ataques más graves contra los sistemas de información se dirigen a los operadores de comunicaciones electrónicas y a los servidores de servicios o a las sociedades de comercio electrónico.

Las violaciones en la seguridad de las bases de datos mercantiles del comercio electrónico en las que se tiene acceso a la información sobre los clientes, incluidos números de tarjeta de crédito, son también una causa de preocupación.

Estos ataques suponen cada vez más medios de fraude en el pago y obligan a la banca a cancelar y a expedir de nuevo miles de tarjetas. Otra consecuencia es el daño no cuantificable a la reputación mercantil y a la confianza del consumidor en el comercio electrónico.

Es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.

CAPÍTULO III. LEGISLACIÓN EN DIFERENTES PAÍSES SOBRE LOS DELITOS INFORMÁTICOS.

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

3.1. Tipos de Delitos Informáticos reconocidos por la Organización de las Naciones Unidas.

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

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

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución.

Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración ius comparativista de los derechos nacionales aplicables, así como de

las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

De esta forma, la Organización de Cooperación y Desarrollo Económico en 1986 publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica, en donde se reseñaban las normas legislativas vigentes y las propuestas de reformas en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales, como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

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

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

La lista mínima preparada por la Organización de Cooperación y Desarrollo Económico se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal.

El Comité Especial de expertos sobre delitos relacionados con el empleo de computadoras, del Comité Europeo para los Problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

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

Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989. Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente debe mencionarse que en 1992, la Organización de Cooperación y Desarrollo Económico, elaboró un conjunto de normas para la

seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos el mismo año.

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

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

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

Por tal motivo, si bien el problema principal era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados. Por todo ello, en vista que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran

contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas.

A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

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

Adicionalmente, deben mencionarse la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición. Teniendo presente esa situación, consideramos que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema.

En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada.

Durante la elaboración de dicho régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

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

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

Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta qué punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

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

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

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 informática de los procesos de cómputo. Es una técnica especializada que se denomina "técnica de salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

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 y sistemas informáticos; esto es por motivos diversos desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

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

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

3.2 Legislación en otros países.

Un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados por los ordenadores.

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

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

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho Penal tradicional, existen, al menos en parte, relevantes dificultades.

Éstas proceden en buena medida de la prohibición jurídico-penal de analogía, y en ocasiones son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales de occidente existe un amplio consenso sobre estas valoraciones que se refleja en las reformas legales de los últimos años.

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

A) ALEMANIA.

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

1. Espionaje de datos (artículo 202).
2. Estafa informática (artículo 263).
3. Falsificación de datos probatorios (artículo 269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).
4. Alteración de Datos (artículo 303) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
5. Sabotaje Informático (artículo 303 bis).

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

7. Utilización abusiva de cheques o tarjetas de crédito (artículo 266 bis).

8. Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita. Esta solución fue también adoptada en los Países Escandinavos y en Austria.[1]

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".

> ***Ley Federal Alemana sobre Protección de Datos de 27 de enero entró en vigor el 1 de enero de 1978. Bundesdatenschutzgesetz de 27 enero de 1977 modificada el 20 de diciembre de 1990 y que entró en vigor el 1 de junio de 1991.***
>
> Art. 1
>
> 1. "La dignidad del hombre es intangible. Respetarla y protegerla es obligación de todo poder público".
> 2. "El pueblo alemán se identifica por lo tanto, con los inviolables e inalienables derechos del hombre como fundamento de toda comunidad humana, de la paz y de la justicia en el mundo".
> 3. "Los siguientes derechos fundamentales vinculan a los poderes legislativo, ejecutivo y judicial a título de derecho directamente aplicable".

[1] Legislación y delitos informáticos Alemania. http://www.segu-info.com.ar/delitos/alemania.htm

Art. 2

1. “Todos tienen derecho al libre desenvolvimiento de su personalidad siempre que no vulneren los derechos de otro ni atenten al orden constitucional o a la ley moral”

2. “Todos tienen derecho a la vida y a la integridad física. La libertad de la persona es inviolable. Estos derechos sólo podrán ser coartados en virtud de una ley”.[2]

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, aunque tenga lugar de forma cualificada.

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho Penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo “modus operandi”, que no ofrece problemas para la aplicación de determinados tipos.

[2] http://www.informatica-juridica.com/anexos/anexo1.asp

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

B) AUSTRIA.

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

Además contempla sanciones para quienes cometen este hecho utilizando su profesión de especialistas en sistemas.

a) Destrucción de datos (artículo 126): se regulan no sólo los datos personales sino también los no personales y los programas.

b) Estafa informática (artículo 148): se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

C) CHILE.

Chile fue el primer país latinoamericano en sancionar una Ley Contra Delitos Informáticos, la cual entró en vigencia el 7 de junio de 1993.

Según esta ley, la destrucción o inutilización de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

Esta ley prevé en el Art. 1 el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta sea tendiente a impedir, obstaculizar o modificar su funcionamiento. En tanto, el artículo 3 tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

> **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 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".

D) ESTADOS UNIDOS.

Consideramos importante 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.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, etcétera, y en qué difieren de los virus, la nueva ley sanciona la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030(a) (5) (A)).

La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquéllos, que de manera temeraria, lanzan ataques de virus de aquéllos que lo realizan con la intención de hacer estragos.

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

Dicha y aclara que el creador de un virus no podrá escudarse en el hecho de que no conocía que con su actuar causaría daño a alguien o que él sólo quería enviar un mensaje. Con esta inclusión se elimina la concepción de que el sujeto activo debía poseer conocimientos superiores para la realización de estos actos.

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 qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley. Sin embargo es importante destacar la enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en las que, entre otras, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de diez mil dólares por cada persona afectada y hasta cincuenta mil dólares el acceso imprudencial a una base de datos.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente.

Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo el aumento de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras dependencias relacionadas con el Estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Cabe mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos, aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos, sino que contempla a otras instrucciones designadas a contaminar otros

grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

E) FRANCIA.

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

Asimismo, esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.

Por su parte, el artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de vulnerar los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

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

Por último, el artículo 462-2 de esta ley sanciona tanto el acceso al sistema resulta la supresión o modificación de datos contenidos en él o resulta la alteración del funcionamiento del sistema.[3]

F) ITALIA.

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

a) Acceso Abusivo. Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso a aquél sólo a las personas autorizadas.

La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.

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

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

d) Fraude Informático. Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un injusto

[3] Pablo Andrés Palazzi, *op. cit.*, pág. 178.

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.

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

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

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

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

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

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

G) PORTUGAL.

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

> **Artículo 35.** Utilización de la Informática.
>
> **I.** 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.
>
> **II.** 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.
>
> **III.** 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, se contemplen de una forma u otra.

En el presente capítulo se han dejado fuera muchos países que en la actualidad regulan las actividades informáticas en sus respectivas legislaciones, sin embargo se han mencionado las naciones que se mostraron más interesadas en incluir de una manera pronta dichos términos y conductas en sus ordenamientos legales.

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 a realizar una crítica a las anteriores disposiciones legales, ya que cada país contempló dichas normas de acuerdo a sus necesidades, 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.

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

3.3. Legislación Nacional de los Delitos Informáticos.

En México, Internet no se ha regulado de manera expresa, como tampoco en el resto de los países latinoamericanos. Su uso gira en torno a cierto Código Ético y la tendencia Institucional es que será un fenómeno "autorregulable".

A pesar de los índices de crecimiento del uso de la computadora y de Internet, México enfrenta un problema social consistente en lo que denominamos "analfabetismo informático", del cual el Poder Legislativo no está exento, por lo que muchos congresistas no entienden el concepto y la estructura de Internet.

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 alguna que se refiera 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.

TRATADO DE LIBRE COMERCIO DE AMÉRICA DEL NORTE (TLC)

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la Sexta Parte, Capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta, que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual

(artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse el contenido del párrafo 1 del artículo 1717 denominado Procedimientos y Sanciones Penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, Defensa de la Propiedad Intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.

Asimismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información.

Llama la atención que en su párrafo segundo habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que éstos consten en medios electrónicos o magnéticos.

En resumen, las provisiones insertas en el articulado del Tratado de Libre Comercio se ocupan básicamente de la protección a la propiedad intelectual,

dejando a las legislaciones de cada país las sanciones a los delitos que se desprendan de las acciones contra los mencionados derechos.

ACUERDO SOBRE LOS ASPECTOS DE LOS DERECHOS DE PROPIEDAD INTELECTUAL RELACIONADOS CON EL COMERCIO

Al inicializar el contenido de este apartado, debemos aclarar que si bien la institución del GATT *General Agreement on Tariffs and Trade* (Acuerdo general sobre comercio y aranceles) se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), todos los acuerdos que se suscribieron en el marco del GATT siguen siendo vigentes.

En este entendido, cabe mencionar que el Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT) manteniendo su vigencia hasta nuestros días.

Es de destacarse el hecho de que en este acuerdo, en el artículo 10 relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

Además, en la parte III sobre observancia de los derechos de propiedad intelectual, en la sección I de obligaciones generales, específicamente en el artículo 41, se incluye que los miembros del Acuerdo velarán porque en su respectiva legislación nacional se establezcan procedimientos de observancia de los derechos de propiedad intelectual.

Asimismo, en la sección 5, denominada Procedimientos Penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales además de que, "los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias".

Finalmente, en la parte VII, denominada Disposiciones Institucionales, Disposiciones Finales, en el artículo 69 relativo a la cooperación internacional, se establece el intercambio de información y la cooperación entre las autoridades de aduanas en lo que se refiere al comercio de mercancías de marca de fábrica o de comercio falsificadas y mercancías pirata que lesionan el derecho de autor.

Como se observa, el tratamiento que los dos instrumentos internacionales que se han comentado otorgan a las conductas ilícitas relacionadas con las computadoras es en el marco del derecho de autor.

En México, los delitos informáticos están regulados de manera indirecta en el Código Penal Federal, en el título noveno, referido a la revelación de secretos y acceso ilícito a sistemas y equipos de informática, en su capítulo II prescribe lo siguiente:

> **TÍTULO NOVENO**
> **REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA**
> **CAPÍTULO II**
> **ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA**
> **ARTÍCULO 211 BIS-1**. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
>
> Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

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

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

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

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

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

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

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

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

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

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

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

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.

Las ventajas y las necesidades de la circulación nacional e internacional de datos conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

Asimismo, nuestra legislación contempla de manera indirecta el delito de fraude informático, esto en el Código Penal para el Distrito Federal en su Título Décimo Quinto, llamado Delitos contra el Patrimonio, en su capítulo III, denominado Fraude considera indirectamente este tipo de delito informático, de la siguiente manera:

> **Artículo 230**.- Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero…
>
> **Artículo 231.-** Se impondrán las penas previstas en el artículo anterior, a quien:
>
> **XIV.** Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independiente de que los recursos no salgan de la Institución; o

Como vemos no se tipifica específicamente el fraude electrónico derivado de una compraventa por internet, ya que sólo hace referencia al cometido a sistemas

o programas de informática del sistema financiero y resultaría muy forzado y motivo de interpretación encuadrar ésta conducta en el tipo que se precisa.

Ahora bien, nuestro Código Penal para el Distrito Federal en su título vigésimo cuarto denominado Delitos contra la fe pública, capítulo I, llamado Producción, Impresión, Enajenación, Distribución, Alteración o Falsificación de Títulos al Portador, Documentos de Crédito Públicos o Vales de Canje, considera indirectamente a este tipo de delito informático, de la siguiente manera:

> **ARTÍCULO 336.** Se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa al que, sin consentimiento de quien esté facultado para ello:
>
> **IV.** Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios;
>
> **V.** Acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo;
>
> **VI.** Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma;

Ahora bien, toda ciencia emplea sus propios conceptos o categorías con los que aborda objetos o fenómenos propios de su campo de estudio, en el caso de la informática ésta no es la excepción, y con relación al delito que se comenta, precisamente, el legislador creó algunas de las categorías o conceptos de la informática, lo anterior da una idea de que se trata de su campo de acción, dichos términos son: **medios, electrónica, acceda y equipos electromagnéticos.**

Además de las palabras empleadas en el tipo descrito, entran en el escenario del delito, medios informáticos, en el caso concreto que se analiza éstos son electrónicos y electromagnéticos.

Como se mencionó en el artículo que precede en la elaboración de dicho tipo, el legislador hizo uso de categorías de carácter informático, ahora bien, en ambos casos utilizó conceptos análogos, como lo son las palabras **acceder** y **accesar** respectivamente, cuyo significado es ingresar.

Por otro lado por cuanto hace al delito de fraude informático que se estudia, cuando se emplean los conceptos **sistemas o programas de informática**, está haciendo referencia además, a los medios electrónicos de que se vale el sujeto activo en la perpetración del delito.

El Código Penal Federal contempla en seis artículos (del 386 al 389bis), el delito de fraude (genérico y específico) previendo penas y multas de acuerdo con el monto y valor de lo defraudado; sin embargo, ninguno de dichos artículos contempla el fraude cometido a través del uso de medios electrónicos o de Internet.

Cabe señalar que desde el año 2000, se han desarrollado en la Cámara de Diputados algunos esfuerzos e iniciativas para reformar el Código Penal Federal y su legislación, con el objeto de prever y castigar algunos delitos informáticos y financieros que se cometen a través de Internet.

Todos estos esfuerzos han sido en vano y ninguna de las iniciativas presentadas ha fructificado debido a la poca información que manejan los legisladores acerca de estos temas, protagonismos innecesarios, cambios políticos y administrativos, intereses encontrados; y sobre todo, la falta de voluntad de los legisladores y de una agenda específica bien planteada por parte de las

autoridades federales, estatales y municipales encargadas de perseguir y castigar los delitos.

3.4. Código 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, es 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:
>
> I. Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o
>
> II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.
>
> Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa."[4]

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

[4] Gabriel Andrés Cámpoli, *op. cit.*, pág. 83.

Considero que se ubico el delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, 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 país, 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.

Como podemos observar de la simple lectura del artículo 217 del Código Penal del estado de Sinaloa y los artículos 211 bis 1 al 211 bis 7 del Código Penal Federal, existen algunos elementos comunes que podemos equiparar para su estudio como son los elementos comunes del tipo:

El sujeto activo: En ambas legislaciones observamos que el sujeto activo puede resultar cualquier persona física, aunque, en algunos de los supuestos de la Federal éste requiere de algunas condiciones especiales, específicamente me refiero a los artículos 211 bis 3 y 211 bis 5, en los cuales se exige como parte del tipo básico que el sujeto activo cuente con autorización para acceder a sistemas y equipos de informática, ya se trate del estado o de instituciones pertenecientes al sistema financiero, aunque debo resaltar que en estos casos lo que se ha intentado es establecer una agravante sobre el tipo básico del 211 bis 1, ya que los verbos o acciones típicas son exactamente los mismos y la variación se produce en las penas que como advertimos han sido cuadruplicadas en su escala, pero no debe olvidarse que en estos casos en particular también hay limitaciones

en el sujeto pasivo, que sólo puede ser el Estado o las instituciones del sistema financiero.[5]

Por otra parte en el 211 bis 7 se establece una agravante genérica para todas las conductas si el sujeto activo utiliza la información en provecho propio o ajeno, cuestión que abarca a todos los sujetos activos posibles.

El sujeto pasivo: Salvo las limitaciones impuestas para los tipos agravados descritos en los artículos 211 bis 2 al 211 bis 5 en cuyo caso los sujetos activos pueden ser solamente el Estado y las instituciones financieras, tanto en la legislación de Sinaloa como en la Federal podemos decir que el sujeto pasivo puede ser cualquier persona moral o física.

La relación subjetiva: En ambos casos se tiene en cuenta solamente la relación dolosa, que el Estado exige que se haga "dolosamente y sin derecho" y la Federación si bien no hace mención específica sobre el tema, la define por exclusión al no integrar en el articulado los tipos culposos del delito.

Las penas: Si se observa en detalle, aunque no se trate exactamente de las mismas acciones punibles, estamos en una escala de penas que en sus tipos básicos (el Código de Sinaloa no posee agravados) es de seis meses a dos años, cuestión con la que me permito disentir ya que esta escala no permite en casi ningún caso la extradición cuando los sujetos activos se encontraran fuera del territorio, cuestión que favorece la impunidad de todas estas actividades tal y como ya se explicó.

En los tipos agravados este problema no se presentaría, pero ello no implica que la pena atribuida a los residuales no sea a mi criterio demasiado baja, cuestión que podría resolverse con la simple modificación del máximo que estimo

[5] Gabriel Andrés Cámpoli, *op. cit.*, pág. 85.

debería imponerse en al menos tres años para poder realizar una protección extraterritorial de la información que, como ya sabemos, puede verse violentada desde espacios geográficos muy lejanos al territorio mexicano en concreto, lo cual acarrearía la expresa necesidad de extradición que la misma norma impide con una pena tan baja.

Los elementos diferenciados en cada uno de los ordenamientos

Las acciones típicas: El ordenamiento federal como acciones típicas, modificar, destruir, provocar pérdida, conocer o copiar, mientras que el Código de Sinaloa establece en este elemento usar, entrar, interceptar, interferir, recibir, usar, alterar, dañar o destruir.

Es claro que no comparto la utilización de los términos de ambos códigos, ya que en todos los casos, las definiciones que utilizan son muy vagas o bien hasta contradictorias entre sí , pues, por ejemplo el verbo conocer, puede implicar desde simplemente haber visto hasta un proceso mental específico de asimilación conceptual que implique el haber adquirido plena conciencia del contenido de la información, y esto permite plena conciencia del contenido de la información, y esto permite desde la plena inclusión de cualquier conducta relacionada hasta la total exclusión de las mismas.

Por otra parte y siguiendo con la misma línea de razonamiento, destruir implica necesariamente provocar pérdida, razón por la cual si lo que se intentaba era proteger al sujeto pasivo en contra de las acciones de borrado deliberado de información, debió haberse utilizado el verbo borrar, ya que no existe razón alguna para que no se pudiere redactar de esa manera que a todas luces resulta técnicamente más correcta.

Tampoco es claro en sus definiciones el Código de Sinaloa, que utiliza dañar o destruir, cuando la correcta redacción hubiere sido por ejemplo provoque daño

total o parcial si lo que se buscaban era proteger en contra de daños parciales, ya que dañar y destruir como se expresan, al resultar sinónimos, pueden estar generando una redundancia innecesaria para los tipos penales.[6]

Por otra parte, debe tenerse en cuenta el significado literal e interpretativo de interceptar e interferir, ya que la interceptación hace una necesaria interferencia, con lo cual si lo que se deseaba era proteger contra la simple interferencia sin que el sujeto activo tome conocimiento del contenido del mensaje (acto que sí puede resultar incluido en el vocablo interceptar) creo que resultaba suficiente con la inclusión realizada de recibir, puesto que quien interfiere y recibe, en definitiva y por definición técnica intercepta, con la gran ventaja de que quien reciba sin haber interceptado también queda incluido en el tipo.

El bien jurídico protegido: Los bienes jurídicos que se protegen mediante la creación de estos tipos penales son específicamente la propiedad y la privacidad, lo cual no se desprende demasiado claramente de las relaciones de los ordenamiento que analizamos.

De hecho la correcta sistematización de los códigos penales impone que los delitos deben ordenarse en grupos que responden específicamente al bien jurídico que protegen, cosa que no ocurre en ninguno de los nombrados.

El Código Federal incluye a estos delitos con los de invasión a la privacidad, pero de la redacción de su articulado se desprende claramente el hecho de que lo que en todos los primeros párrafos protege es la propiedad, ya que a fin del análisis teórico, es claramente equiparable al delito de daños en la propiedad ajena por su redacción.

[6] Gabriel Andrés Cámpoli, *op. cit.*, pág. 87

El caso de Sinaloa es un poco más curioso, ya que requiere de un análisis más detallado para descubrir qué bien intenta proteger.

Es claro que los objetos materiales sobre los cuales recae el delito son bases de datos, sistemas de computadoras o red de computadoras o cualquier parte de las mismas, como asimismo los soportes lógicos o programas de computadora o los datos contenidos en la base, sistema o red. Lo que no surge tan simplemente es el significado que se haya querido dar a estos términos, ya que por ejemplo el soporte de la información siempre es físico, razón por la cual resulta poco menos que un absurdo hablar del soporte lógico, si lo que se quiere es proteger la integridad de los equipos, esto es innecesario puesto que la misma se encuentra cubierta por el delito de daños.

3.5. Ley Federal de Derechos de Autor y Código Penal para el Distrito Federal en Materia del Fuero Común y para toda la República en Materia del Fuero Federal.

Uno de los problemas más importantes que confronta el Derecho de la Informática es la protección jurídica derivada de las nuevas Tecnologías de la Información y la Comunicación (TIC). De entre toda la gama de problemas que genera, en el presente capítulo sólo se analizarán dos: la protección de los programas de computación y los nombres de dominio.

Los programas de cómputo se caracterizan por ser un medio necesario para ofrecer un conjunto de instrucciones comprensibles por una computadora, a efecto de resolver determinado problema. Los programas determinan ese problema, clasifican los datos y definen las estructuras y resultados esperados y prevén la evolución del mismo y los procedimientos de control necesarios.

La Organización Mundial de la Propiedad Intelectual (OMPI), considera a los programas como un conjunto de instrucciones expresadas en un lenguaje natural

o formal, pudiendo una vez traducidas y transpuestas en un soporte descifrable por una máquina de tratamiento de datos, o por parte de esta máquina, efectuar operaciones aritméticas y sobre todo lógicas, en vías de indicar o de obtener un resultado particular. [7]

Es conveniente enunciar que el problema de la protección de los programas no es estrictamente jurídico, sino que denota la presencia de dos elementos fundamentales como el técnico y el económico. En términos técnicos, los programas de cómputo son el conjunto de procedimientos o reglas que integran el soporte lógico de las máquinas que permiten la consecución del proceso de tratamiento de la información. En la práctica podemos distinguir los siguientes tipos de programas:

- Los programas fuente (conocidos también como sistemas operativos o de explotación): están ligados al funcionamiento mismo de la máquina, guardan estrecha relación con las memorias centrales y auxiliares del computador a través de dispositivos como los compiladores, traductores, intérpretes, editores, etcétera., que permiten el adecuado enlace entre la máquina y los trabajos del usuario.

- Los programas objeto: son aquéllos que se realizan para satisfacer las necesidades más variadas de los usuarios y permiten el tratamiento de datos definidos concretamente y son disociables de la máquina.

- Los programas de explotación (conocidos como sistemas operativos): son los ligados al funcionamiento mismo de la máquina y permiten aprovechar al máximo sus posibilidades. Guardan estrecha relación con las

[7] Pablo Andrés Palazzi, *op. cit.*, págs. 92 y 93.

memorias centrales y auxiliares del computador y toman en cuenta las funciones de enlace de los trabajos de los usuarios.

- Los programas de aplicación: son los realizados para satisfacer las necesidades más diversas y variadas de los usuarios; permiten el tratamiento de datos definidos concretamente y separables de la máquina. Entre ellos están aquellos que son concebidos para satisfacer las necesidades de un número elevado de usuarios (paquetes de software), de los que sobre medida responden a las necesidades del usuario (programas específicos).

Por lo que se refiere al aspecto económico, los programas de cómputo son una de las máximas manifestaciones del producto-información y han provocado un apuntalamiento de la industria de programación, lo cual ha traído consigo que los problemas en torno al software rebasen el aspecto técnico para alcanzar niveles económicos y por ende jurídicos.

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.

Cuando se inició la iniciativa correspondiente, se dijo que la importancia de pronunciarse al respecto era que con dicha iniciativa se atendía la complejidad que el tema de los derechos autorales había presentado en los últimos tiempos lo cual exigía una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión.

Además, se consideró que debido a que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de Decreto de Reforma al

Código Penal para el Distrito Federal y para toda la República en Materia de Fuero Federal, proponiendo la adición de un título Vigésimo Sexto denominado "De los Delitos en Materia de Derechos de Autor".

Al respecto, se consideró conveniente la inclusión de la materia en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas y por otro en un instrumento más adecuado para la procuración y la administración de justicia, al poderse disponer en la investigación de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.

En este orden, como se mencionó anteriormente, 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.

> **LEY FEDERAL DEL DERECHO DE AUTOR**
> **TÍTULO I**
> **Disposiciones Generales**
> **Capítulo Único**
>
> **Artículo 1o.-** La presente Ley, reglamentaria del artículo 28 constitucional, tiene por objeto la salvaguarda y promoción del acervo cultural de la Nación; protección de los derechos de los autores, de los artistas intérpretes o ejecutantes, así como de los editores, de los productores y de los organismos de radiodifusión, en relación con sus obras literarias o artísticas en todas sus manifestaciones, sus interpretaciones o ejecuciones, sus ediciones, sus fonogramas o videogramas, sus emisiones, así como de los otros derechos de propiedad intelectual.

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, los artículos 102 y 231 de esta ley, regulan el primero 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.

> **Capítulo IV**
> **De los Programas de Computación y las Bases de Datos**
>
> **Artículo 102.-** Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.
>
> **Capítulo II**
> **De las Infracciones en Materia de Comercio**
> **Artículo 231.-** Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto:
> **V.** Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación;

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 otra parte, el artículo 104 de dicha ley se refiere a la facultad del titular de los derechos de autor sobre un programa de computación o sobre una base de

datos, de conservar aún después de la venta de ejemplares de los mismos el derecho de autorizar o prohibir el arrendamiento de dichos programas.

Por su parte, el artículo 231, fracciones II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por esta Ley" y "usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular".

La redacción de estas fracciones trata de evitar la llamada piratería de programas en el área del comercio, permite la regulación administrativa de este tipo de conducta, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, al igual que las infracciones contempladas para los programas de virus.

Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, artículo 424 BIS, fracción II, del Código Penal 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.

> **"Artículo 215.-** Corresponde conocer a los Tribunales de la Federación de los delitos relacionados con el derecho de autor previstos en el Título Vigésimo Sexto del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal."
>
> **"Artículo 424 bis**.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

> **II.** A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación."

Se ha llegado a considerar que figuras como el robo, fraude, abuso de confianza o los secretos comerciales (figura estadounidense) y secretos de fabricación (figura europea) se presentan como medios de solución frente al problema; sin embargo, dichas instancias parecen no estar integradas por elementos que permitan atribuir una asimilación cabal.

Así por ejemplo, en el robo se requiere del apoderamiento físico de una cosa mueble, la cual, en los términos de la información como "algo" indiscutiblemente intangible o inmaterial, no resulta convincente el supuesto. Por otra parte, en el abuso de confianza se requiere de la disposición de una cosa ajena mueble, lo cual representa problemas a nivel de la carga de la prueba. En el fraude se requiere un engaño o aprovechamiento de un error que permita hacerse ilícitamente de alguna cosa (no se específica de qué tipo) o alcanzar un lucro indebido, lo cual, si bien pudiera ser aplicable a final de cuentas por su misma abstracción frente al problema, ofrece serias inconveniencias en la práctica.

Ahora bien, por lo que concierne a los secretos comerciales y de fabricación (si bien no son utilizados en México), en ellos se implica una divulgación intencional (o aun fortuita) de alguna información, en este caso referida o contenida en un programa de cómputo, dichas figuras si bien apropiadas en apariencia (sobre todo porque son castigadas penalmente), revisten dificultades a nivel probatorio en cuanto al apoderamiento y difusión de la información.

México ha alcanzado un grado de desarrollo relevante en la industria de programación, lo cual, evidentemente, ha motivado la aparición de considerables controversias con relación a la propiedad de los programas. La ley Federal de

Propiedad Industrial no considera a los programas de cómputo como invenciones y por tanto no son susceptibles de obtener los beneficios de una patente.

Por otro lado, la Ley Federal del Derecho de Autor de diciembre de 1996, contiene un capítulo que comprende los artículos 101 a 114, que regulan en forma específica la protección de los programas y las bases de datos, a través de la obtención de un certificado autoral expedido por el Instituto del Derecho de Autor (INDA).

Capítulo IV
De los Programas de Computación y las Bases de Datos

Artículo 101.- Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.
Artículo 102.- Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Artículo 103.- Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.
Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 104.- Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

Artículo 105.- El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

I. Sea indispensable para la utilización del programa, o

II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

Artículo 106.- El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;
II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;
III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y
IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

Artículo 107.- Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108.- Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

Artículo 109.- El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Artículo 110.- El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;
II. Su traducción, adaptación, reordenación y cualquier otra modificación;
III. La distribución del original o copias de la base de datos;
IV. La comunicación al público, y
V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111.- Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

> **Artículo 112.-** Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.
>
> **Artículo 113.-** Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.
>
> **Artículo 114.-** La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

En torno al problema de la protección jurídica de los programas, algunos autores han manifestado en el sentido de que debido a la complejidad de los programas y de una necesaria regulación bajo las consideraciones de una "reserva privativa", ésta puede llegar a darse tomando los elementos más significativos por parte de las instituciones jurídicas ya expresadas, y en especial en materia de patentes y derechos de autor, a fin de integrarlos en una estructura nueva y específica que constituya un derecho *sui generis* o particular acorde a las condiciones específicas de los programas.[8]

La protección mediante patente y derechos de autor son complementarias. Una patente protege una invención, dentro de los límites de las reivindicaciones, que determinan el alcance de la protección concedida. De esta forma, el titular de una patente por una invención implementada en computadora tiene derecho a impedir el uso de terceros de cualquier programa informático que aplique su invención.

[8] Pablo Andrés Palazzi, *op. cit.*, pág. 103.

CAPÍTULO IV. PRÁCTICAS DELICTIVAS A TRAVÉS DEL INTERNET.

4.1. Conductas ilegítimas más comunes.

a) Hacker

Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y 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.

Los hackers se dedican a “cortar” las defensas preestablecidas de los equipos informáticos ajenos o de las páginas web, para introducirse de esa forma y “espiar” la información ajena o bien producir daños que pueden llegar al borrado total de los datos del equipo al cual se le han “cortado” las defensas, conocidas comúnmente como *firewalls* o su acepción española “paredes de fuego”, lo cual en cierta medida explica la utilización del verbo cortar como sinónimo de vencer estas paredes informáticas.[1]

Se pueden considerar que hay dos tipos:

[1] Gabriel Andrés Cámpoli, *op. cit.*, pág. 30.

1) los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad;

2) los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables.

b) Cracker

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

Los fraudes electrónicos (*dot cons*) son más comunes de lo que imaginamos. Los defraudadores utilizan todo tipo de medios para engañar a los cibernautas: correos electrónicos, páginas ofreciendo servicios o promociones falsas, robo de identidad, *hacking*, etc. La *Federal Trade Commission* de los Estados Unidos después de un detallado estudio determinó cuáles son los tipos de fraudes más comunes en Internet:

- Subastas en línea
- Servicios de acceso a Internet
- Fraude con tarjeta de crédito
- Marcado internacional por módem
- Cargos "no autorizados" a tarjetas de crédito o recibos telefónicos (*Web Cramming*)
- Planes de mercadotecnia de multinivel (pirámides)

- Viajes y vacaciones
- Oportunidades de negocios
- Inversiones
- Productos y servicios relacionados con la salud

c) Phreacker

Es el que hace una actividad parecida a la anterior, aunque ésta se realiza mediante líneas telefónicas y con 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 informático

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

4.2. Conductas que se cometen a través de la Computadora y del Internet, tradicionalmente denominados "Delitos Informáticos".

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 (fraudes, estafas, apropiaciones indebidas, etcétera.).

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.

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.

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes.

Sin embargo, debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

a) Fraude informático.- El fraude informático sólo 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) Destrucción de datos.- Son daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático.

d) Infracción 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) Infracción del Copyrigth de bases de datos.- Aún no existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet.

f) Intercepción 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 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.

h) Transferencia de Fondos.- Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático. Como

se puede observar, muchas de estas conductas no son irreales, es decir, las encontramos de una manera palpable, y cualquier persona que tenga conocimientos básicos de informática puede llegar a cometerlos.

4.3. Delitos convencionales que se pueden trasladar 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.

En pocos años la revolución digital ha conquistado gran parte del mundo. En lo que a comunicaciones se refiere, Internet ha resultado ser el fenómeno de más rápida expansión que se haya dado nunca. Los adelantos que lo han hecho posible no sólo han contribuido a que se produzcan cambios en el terreno de las comunicaciones, sino que también han propiciado un desarrollo espectacular de la nueva economía digital, reflejado en los mercados financieros y el flujo comercial,

así como en las innovadoras formas de comercio y las nuevas posibilidades para los consumidores.[2]

Por el impresionante alcance de esas innovaciones, el comercio electrónico ha pasado a ser una actividad de gran trascendencia económica, política y social. A pesar de todas las formas de seguridad que hay para el comercio electrónico, estas transacciones tienen un alto porcentaje de riesgos, fraude o alteración de datos personales. La forma en que nos interrelacionamos con los demás está siendo atacada por nuevas prácticas (compras on-line, chats, e-mail, educación a distancia, foros de discusión, etcétera).

El fraude electrónico es una de tantas maneras que utilizan los espías cibernéticos para obtener información confidencial, especialmente de cuentas e instituciones bancarias. Engañan a los usuarios y los estafan a través de internet**.**

Una de las razones por las cuales el fraude electrónico es tan exitoso es que los correos electrónicos vinculan a la víctima a sitios web que parecen oficiales, donde utilizan imágenes, logotipos y textos extraídos de sitios de empresas genuinas para hacer que ofertas falsas parezcan legítimas.

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.

[2] Valentino F. Cornejo López, *Los medios electrónicos regulados en México: comercio electrónico, documentos electrónicos, firma electrónica y certificados digitales,* Sista, México, 2006, Pág. 184.

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.

Por lo anterior, 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; ya que este cambio no sólo conlleva beneficios, esto debido a que el cyberespacio puede ser también concebido como un ámbito propicio para la realización de conductas disvaliosas.

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.

En el caso contrario, se estaría sancionando como delitos hechos no descritos 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. Siendo está la mejor solución si queremos contar con un sistema jurídico seguro, que no dé 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 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.

Los problemas que se pueden plantear en caso de uso fraudulento de los servicios de Banca electrónica. El principal problema que se deriva en ambos casos es el de la atipicidad. Nos encontramos ante ámbitos y actuaciones que, o bien no aparecen regulados por parte del ordenamiento jurídico, o bien la regulación es escasa y con normas de rango jerárquico “bajo”. Y todo ello pese a que la importancia y el uso de la banca a distancia crece y seguirá creciendo en el futuro.

La seguridad aparece configurada como elemento principal, siendo necesarios niveles mayores de seguridad, como codificación criptográfica de 128 bits, firmas digitales y procedimientos de autenticación específicos (autenticación basada en fichas o en tarjetas inteligentes, o contraseñas dinámicas).

Uno de los principales miedos para la realización de compras por internet es el marco jurídico, el cual posee aún numerosas lagunas y vacíos que impiden garantizar, por ejemplo, el castigo a delitos como el fraude electrónico, robo de identidad, *phishing (*envío de correos basura que contienen links y URLs -direcciones falsas-, aparentemente provenientes de algún banco o empresa, donde se solicita el acceso por supuestas modificaciones o actualizaciones a sus bases de datos o sistemas*)* u otro tipo de ataques electrónicos.

Usuarios y proveedores podrían quedar desprotegidos legalmente debido a la ausencia de reformas a las leyes penales mexicanas, pues los delitos que tienen lugar en Internet no se encuentran tipificados en la legislación vigente.

El fraude con tarjetas de crédito hoy en día es la gran preocupación de los comercios online debido al fraude y su impacto en el comercio electrónico.

Con el crecimiento del comercio electrónico y el uso de los servicios de banca por Internet han aumentado en forma alarmante los fraudes electrónicos, especialmente el robo de identidad.

Esta nueva modalidad de fraude, comúnmente se refiere a toda aquella información de un individuo –nombre, fecha de nacimiento, dirección, número de licencia, de tarjeta de crédito y de cuentas bancarias, nombre de usuario y contraseña– que es obtenida y utilizada sin su consentimiento, y con el propósito de cometer actividades fraudulentas.

El robo de identidad normalmente involucra la adopción de la identidad de una persona, mediante la información que el delincuente obtuvo de su víctima.

Actualmente, el mayor número de casos de robo de identidad se dan a través del *phishing*, el cual consiste en el envío de correos spam que contienen links y URLs falsos, aparentemente provenientes de algún banco o empresa, donde se solicita el acceso por supuestas modificaciones o actualizaciones a sus bases de datos o sistemas; de esa forma, al darle clic el usuario a esos sitios falsos, los delincuentes obtienen sus datos y contraseñas y pueden rastrear fácilmente sus hábitos de navegación en la red.

El robo de identidad se torna cada día más común, ya que con un mínimo de recursos y conocimientos técnicos, los criminales pueden falsificar sitios web, marcas, logotipos e información de empresas y bancos para desviar fácilmente la atención de sus víctimas.

Los delincuentes explotan principalmente tres recursos:

- el uso y creación de plataformas técnicas basadas en la web;
- las técnicas de ingeniería social como vehículos alternativos para engañar y llevar a cabo fraudes;
- y la vulnerabilidad y falta de información de algunos usuarios, sobre todo aquellos que son nuevos o bien, tienen poco tiempo utilizando los sitios de subastas o de servicios financieros.

Asimismo, los criminales se aprovechan de los vacíos legales existentes y de la dificultad que representa a las autoridades ubicar exactamente el lugar físico donde se llevan a cabo las operaciones fraudulentas, así como la persecución hasta su lugar de origen.

El crecimiento de la tecnología en los últimos años, ha generado avances y cambios en todos los aspectos. La evolución de Internet ha sido uno de estos grandes cambios. Internet ha influido en nuestras vidas y en nuestras costumbres, en nuestra forma de buscar información, de entretenernos, de comunicarnos y por supuesto han aparecido nuevas formas de comprar y vender bienes.

Las empresas han encontrado grandes oportunidades en los desarrollos de las comunicaciones, destacando que los costos de las comunicaciones se reducen y que estas tecnologías están al alcance tanto de grandes como de pequeñas empresas.

Internet cambia para el derecho la noción de tiempo y de espacio, porque es posible realizar enlaces inmediatos a tiempo real sin importar el lugar del mundo donde se encuentren las partes.

El desarrollo de estas tecnologías y de las telecomunicaciones ha hecho que los intercambios de datos crezcan a niveles extraordinarios, simplificándose cada

vez más y creando nuevas formas de comercio, y en este marco se desarrolla el comercio electrónico.

Comercio electrónico

Se denomina comercio a la actividad socioeconómica consistente en la compra y venta de bienes, sea para su uso, para su venta o para su transformación. Es el cambio o transacción de algo a cambio de otra cosa de igual valor.

El comercio, es la actividad ancestral del ser humano, ha evolucionado de muchas maneras, pero su significado y su fin siempre es el mismo.

Para José Antonio de Vila Sobrino, el comercio electrónico "es toda forma de comercio en la cual se utilizan las redes de los ordenadores como medio de comunicación entre los diferentes agentes implicados".[3]

En el Código de Conducta del Comercio Electrónico se le define como a todas y cada una de las relaciones iniciadas con fines comerciales de intercambio, venta, promoción o prestación de bienes o servicios, que se realizan, bien en parte o en su totalidad, por vía electrónica, entre personas físicas o jurídicas, sin tener necesariamente la cualidad de comerciantes profesionales.

Lo interesante de esta definición es que no sólo se refiere a las compraventas sino que también a todas aquellas formas de comunicación por las

[3] Ernesto Galindo Sifuentes, *Derecho Mercantil: comerciantes, comercio electrónico, contratos mercantiles y sociedades mercantiles, prólogo de Consuelo Sirvent Gutiérrez,* 1ª. ed., Porrúa, México, 2004, pág. 38.

que se enuncie un bien o servicio; y se encarga tanto a las relaciones empresa-empresa como a las de empresa-cliente final.

Por todo lo anterior el comercio electrónico es cualquier acto de comercio que tenga por objeto el intercambio, la adquisición y el consumo de bienes y servicios a través de medios electrónicos, ópticos o cualquier otra tecnología a cambio de un precio.

Asimismo el comercio electrónico se entiende como cualquier forma de transacción comercial en la cual las partes involucradas interactúan de manera electrónica y no de la manera tradicional por medio de intercambios físicos o trato físico directo.

Actualmente la manera de comerciar se caracteriza por el mejoramiento constante en los procesos de abastecimiento, y como respuesta a ello los negocios a nivel mundial están cambiando tanto su organización como sus operaciones.

El comercio electrónico es el medio de llevar a cabo dichos cambios dentro de una escala global, permitiendo a las compañías ser más eficientes y flexibles en sus operaciones internas, para así trabajar de una manera más cercana con sus proveedores y estar más pendiente de las necesidades y expectativas de sus clientes. Además permiten seleccionar a los mejores proveedores sin importar su localización geográfica para que de esa forma se pueda vender a un mercado global.

Jaime Neilson nos dice que el comercio electrónico es cualquier actividad de intercambio comercial en la que las órdenes de compra - venta y pagos se realizan a través de un medio telemático, los cuales incluyen servicios financieros y bancarios suministrados por Internet.

El comercio electrónico es la venta a distancia aprovechando las grandes ventajas que proporcionan las nuevas tecnologías de la información, como la ampliación de la oferta, la interactividad y la inmediatez de la compra, con la particularidad que se puede comprar y vender a quién se quiera, y, dónde y cuándo se quiera. Es toda forma de transacción comercial o intercambio de información, mediante el uso de Nueva Tecnología de Comunicación entre empresas, consumidores y administración pública.

Por electrónico cabe entender la infraestructura mundial de tecnologías y redes de la informática y las telecomunicaciones que permite el procesamiento y la transmisión de datos digitalizados.

Clases de comercio electrónico

- **Directo:** aquel en el que todos los momentos de la contratación (tanto lo relativo al perfeccionamiento como a la ejecución del contrato) se llevan a cabo con la utilización de medios electrónicos. Como por ejemplo la entrega de cualquier tipo de software, como programas informáticos que se descargan por la red o canal de comunicación, archivos de imágenes, gráficos, sonidos, textos, animaciones accesibles en las páginas webs y bases de datos incorporadas a Internet.
- **Indirecto:** cuando la perfección el contrato (oferta y aceptación) se realizan a través de Internet, pero la fase final de ejecución (pago y entrega) se desarrolla por medios convencionales (pago contrareembolso, transferencia, entrega mediante servicio de mensajería, servicio público de correos, etcétera).

Tipos de comercio electrónico

- **"Business to business"** (entre empresas): las empresas pueden intervenir como compradoras o vendedoras, o como proveedoras de

herramientas o servicios de soporte para el comercio electrónico, instituciones financieras, proveedores de servicios de Internet, etc.

- **"Business to consumers"** (Entre empresa y consumidor): las empresas venden sus productos y prestan sus servicios a través de un sitio Web a clientes que los utilizarán para uso particular.

- **"Consumers to consumers"** (Entre consumidor y consumidor): es factible que los consumidores realicen operaciones entre sí, tal es el caso de los remates en línea.

- **"Consumers to administrations"** (Entre consumidor y administración): los ciudadanos pueden interactuar con las Administraciones Tributarias a efectos de realizar la presentación de las declaraciones juradas y/o el pago de los tributos, obtener asistencia informativa y otros servicios.

- **"Business to administrations"** (Entre empresa y administración): las administraciones públicas actúan como agentes reguladores y promotores del comercio electrónico y como usuarias del mismo.[4]

Características del comercio electrónico

- **Contratación sin presencia física de las partes**: la idea es que en un futuro las relaciones contractuales que se desarrollen en el mercado tendrán como escenario la falta de presencia simultánea física de las partes y la posibilidad de que los consumidores puedan revocar libremente o retractarse del contrato ya concluido en determinadas circunstancias.

[4] Ernesto Galindo Sifuentes, *op. cit.*, pág. 40

- **Transmisión electrónica por un canal de comunicación:** las partes para la celebración de la operación comercial deberán hacerlo por medios electrónicos, ópticos o cualquier tecnología, que permita comunicarse las condiciones del contrato.
- **Transmisión electrónica de información.**
- **Utilización de aparatos electrónicos.**
- **Interactividad:** posibilidad de diálogo individualizado y recíproco de contenidos informativos.
- **Carácter lucrativo de la operación.**

Ventajas del comercio electrónico

Para las Empresas

- Reducción de costo real al hacer estudio de mercado.
- Desaparecen los límites geográficos y de tiempo.
- Disponibilidad las 24 horas del día, 7 días a la semana, todo el año.
- Reducción de un 50% en costos de la puesta en marcha del comercio electrónico, en comparación con el comercio tradicional.
- Hacer más sencilla la labor de los negocios con sus clientes.
- Reducción considerable de inventarios.
- Agilizar las operaciones del negocio.
- Proporcionar nuevos medios para encontrar y servir a clientes.
- Incorporar internacionalmente estrategias nuevas de relaciones entre clientes y proveedores.
- Reducir el tamaño del personal de la fuerza.
- Menos inversión en los presupuestos publicitarios.
- Reducción de precios por el bajo coste del uso de Internet en comparación con otros medios de promoción, lo cual implica mayor competitividad.

- Cercanía a los clientes y mayor interactividad y personalización de la oferta.
- Desarrollo de ventas electrónicas.
- Globalización y acceso a mercados potenciales de millones de clientes.
- Implantar tácticas en la venta de productos para crear fidelidad en los clientes.

Para los clientes

- Abarata costos y precios
- Da poder al consumidor de elegir en un mercado global acorde a sus necesidades
- Un medio que da poder al consumidor de elegir en un mercado global acorde a sus necesidades.
- Brinda información pre-venta y posible prueba del producto antes de la compra.
- Inmediatez al realizar los pedidos.
- Servicio pre y post-venta on-line.
- Reducción de la cadena de distribución, lo que le permite adquirir un producto a un mejor precio.
- Mayor interactividad y personalización de la demanda.
- Información inmediata sobre cualquier producto, y disponibilidad de acceder a la información en el momento que así lo requiera.
- Permite el acceso a más información.

Desventajas del comercio electrónico

- **Desconocimiento de la empresa.** No conocer la empresa que vende es un riesgo del comercio electrónico, ya que ésta puede estar en otro país o en el mismo, pero en muchos casos las "empresas" o "personas-empresa"

que ofrecen sus productos o servicios por Internet ni siquiera están constituidas legalmente en su país y no se trata más que de gente que está "probando suerte en Internet".

- **Forma de Pago.** Aunque ha avanzado mucho el comercio electrónico, todavía no hay una transmisión de datos segura el 100%. Y esto es un problema pues nadie quiere dar sus datos de la Tarjeta de Crédito por Internet. De todos modos se ha de decir que ha mejorado mucho.

- **Intangibilidad.** Mirar, tocar, hurgar. Aunque esto no sea sinónimo de compra, siempre ayuda a realizar una compra.

- **El idioma**. A veces las páginas web que visitamos están en otro idioma distinto al nuestro; a veces, los avances tecnológicos permiten traducir una página a nuestra lengua materna. Con lo cual podríamos decir que éste es un factor "casi resuelto". (Hay que añadir que las traducciones que se obtienen no son excelentes ni mucho menos, pero por lo menos nos ayudan a entender de que nos están hablando o que nos pretenden vender).

- **Conocer quién vende**. Ya sea una persona o conocer de que empresa se trata. En definitiva saber quién es, como es, etc. Simplemente es una forma inconsciente de tener más confianza hacia esa empresa o persona y los productos que vende.

- **Poder volver (post y pre-venta).** Con todo ello podemos reclamar en caso de ser necesario o pedir un servicio "post-venta". Al conocerlo sabemos donde poder ir. El cliente espera recibir una atención "pre-venta" o "post-venta".

- **Privacidad y seguridad**. La mayoría de los usuarios no confía en el Web como canal de pago. En la actualidad, las compras se realizan utilizando el número de la tarjeta de crédito, pero aún no es seguro introducirlo en Internet sin conocimiento alguno. Cualquiera que transfiera datos de una tarjeta de crédito mediante Internet, no puede estar seguro de la identidad del vendedor. Análogamente, éste no lo está sobre la del comprador. Quien paga no puede asegurarse de que su número de tarjeta de crédito no sea recogido y sea utilizado para algún propósito malicioso; por otra parte, el vendedor no puede asegurar que el dueño de la tarjeta de crédito rechace la adquisición. Resulta irónico que ya existan y funcionen correctamente los sistemas de pago electrónico para las grandes operaciones comerciales, mientras que los problemas se centren en las operaciones pequeñas, que son mucho más frecuentes.

Seguridad en el comercio electrónico

La seguridad en el comercio electrónico y específicamente en las transacciones comerciales es un aspecto de suma importancia. Para ello es necesario disponer de un servidor seguro a través del cual toda la información confidencial es encriptado y viaja de forma segura, esto brinda confianza tanto a proveedores como a compradores que hacen del comercio electrónico su forma habitual de negocios.

Al igual que en el comercio tradicional existe un riesgo en el comercio electrónico, al realizar una transacción por Internet, el comprador teme por la posibilidad de que sus datos personales (nombre, dirección, número de tarjeta de crédito, etcétera.) sean interceptados por "alguien", y suplante así su identidad; de igual forma el vendedor necesita asegurarse de que los datos enviados sean de quien dice serlos.

Por tales motivos se han desarrollado sistemas de seguridad para transacciones por Internet: Encriptación, Firma Digital y Certificado de Calidad, que garantizan la confidencialidad, integridad y autenticidad respectivamente.

1. **La encriptación:** Es el conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Por lo general, la encriptación se basa en una clave, sin la cual la información no puede ser descifrada. Con la encriptación la información transferida solo es accesible por las partes que intervienen (comprador, vendedor y sus dos bancos).

2. **La firma digital:** Es el valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

   Evita que la transacción sea alterada por terceras personas sin saberlo. El certificado digital, que es emitido por un tercero, garantiza la identidad de las partes.

   La firma digital, es simplemente el nombre que se le da a cierto tipo de firma electrónica basada en el uso de criptografía, la más común es la llamada criptografía asimétrica o de llave pública. Es éste el tipo de firma alrededor del cual se han realizado las principales inversiones, esfuerzos y respuestas legislativas alrededor del mundo.

3. **Protocolo SET**: Secure Electronic Transactions es un conjunto de especificaciones desarrolladas por VISA y MasterCard, con el apoyo y asistencia de GTE, IBM, Microsoft, Netscape, SAIC, Terisa y Verisign, que

da paso a una forma segura de realizar transacciones electrónicas, en las que están involucrados: usuario final, comerciante, entidades financieras, administradoras de tarjetas y propietarios de marcas de tarjetas.

Secure Electronic Transactions (SET) constituye la respuesta a los muchos requerimientos de una estrategia de implantación del comercio electrónico en Internet, que satisface las necesidades de consumidores, comerciantes, instituciones financieras y administradoras de medios de pago.
Por lo tanto, Secure Electronic Transactions (SET) dirige sus procesos a:

- Proporcionar la autentificación necesaria.
- Garantizar la confidencialidad de la información sensible.
- Preservar la integridad de la información.
- Definir los algoritmos criptográficos y protocolos necesarios para los servicios anteriores.

4. **Firma electrónica:** las relaciones matemáticas entre la clave pública y la privada del algoritmo asimétrico utilizado para enviar un mensaje, se llama firma electrónica (digital signatures).

Quien envía un mensaje, cifra su contenido con su clave privada y quien lo recibe, lo descifra con su clave pública, determinando así la autenticidad del origen del mensaje y garantizando que el envío de la firma electrónica es de quien dice serlo.

No hay que perder de vista que una firma, sea en papel o electrónica, en esencia es un símbolo que acredita la voluntad. En consecuencia, las reformas de mayo de 2000 al Código Civil Federal señalan que en el consentimiento expreso de la voluntad puede manifestarse de forma verbal,

por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología o por signos inequívocos. [5]

Además de servir para demostrar la voluntad de contratar, una firma tiene otras dos funciones significativas: primero, la firma de una persona puede ser usada para identificar al firmante, y segundo, la firma puede usarse para acreditar la integridad de un documento (de ahí la costumbre de rubricar todas las hojas de un contrato).

En el ciberespacio, esas dos últimas características de una firma juegan un papel fundamental; especialmente en la medida que se automatizan los procesos y los contratos se realizan entre ausentes que muchas veces ni siquiera se conocen. Es en estos casos en los que la necesidad de identificar al firmante y garantizar la integridad del mensaje se tornan esenciales.

De este modo mientras la firma autógrafa en la mayoría de los casos sirve para acreditar el deseo de contratar, en el entorno electrónico tiene las tres funciones: a) evidenciar la voluntad de contratar, b) identificar al emisor, y c) garantizar la integridad del mensaje.

5. **Certificados de autenticidad**: como se ha visto la integridad de los datos y la autenticidad de quien envía los mensajes es garantizada por la firma electrónica, sin embargo existe la posibilidad de suplantar la identidad del emisor, alterando intencionalmente su clave pública. Para evitarlo, las claves públicas deben ser intercambiadas mediante canales seguros, a través de los certificados de autenticidad, emitidos por las Autoridades Certificadoras.

[5] Valentino F. Cornejo López, *op. cit*., pág. 211.

Para el efecto Secure Electronic Transactions (SET) utiliza dos grupos de claves asimétricas y cada una de las partes dispone de dos certificados de autenticidad, uno para el intercambio de claves simétricas y otro para los procesos de firma electrónica.

6. **Criptografía:** Es la ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente. En su sentido más amplio, la criptografía abarca el uso de mensajes encubiertos, códigos y cifras.

La palabra criptografía se limita a veces a la utilización de cifras, es decir, métodos de transponer las letras de mensajes (no cifrados) normales o métodos que implican la sustitución de otras letras o símbolos por las letras originales del mensaje, así como diferentes combinaciones de tales métodos, todos ellos conforme a sistemas predeterminados.

Hay diferentes tipos de cifras, pero todos ellos pueden encuadrarse en una de las dos siguientes categorías: transposición y sustitución.

Un ejemplo de fraude electrónico derivado de la práctica del comercio por internet: es el Phishing-Car

El Phishing Car conocido como ofertas falsas de vehículos es la captación de compradores de coches a un costo muy bajo, la venta nunca se efectúa, esta persona realiza un pago como señal, se queda sin dinero y sin coche.

Se producen por medio de llamativas ofertas en vehículos lujosos, incluso tienen web trampas con nombre de dominios muy similares a empresas con

mucho prestigio que se dedican a la venta de vehículos de ocasión, pero todas los fraudes tienen algo en común:

-El pago se realiza por medio de empresas de envió de dinero a otros países (Tipo Western Union, Money Gram).

- El vendedor le oferta la entrega a domicilio.

- En un 90% el vehículo que venden esta fuera de su país, de esta manera usted solo puede verlo en fotos.

- Le piden primero el 30% o el 40% del precio ofertado como primera señal.

- Captan a las víctimas por medio de anuncios en web de venta de coches o de segundamano y por supuesto la recepción de correos electrónicos.

- Muchas veces el vendedor dice que es un español que vive en Gran Bretaña y por motivos laborales de estancia en el país inglés, tiene que cambiar de forma urgente de coche por que se conduce por la izquierda y su coche al estar matriculado en España el volante está al lado contrario y no se adapta, por este motivo vende el coche de forma muy económica, te enseñan un coche matriculado en España.

- La mayoría de los estafados enviaron el dinero a Reino Unido, esto no quiere decir que cambien.

Las compañías "online" están comenzando a ofrecer medios de pago alternativos a la tarjeta de crédito, no por la desconfianza de los consumidores sino más bien por la creciente desconfianza de los vendedores ante la utilización fraudulenta de tarjetas.

En general, el comercio electrónico obliga a redefinir el papel de los intermediarios entre productor y consumidor, eliminándolos en algunos casos, pero también creando la necesidad de nuevas funciones de intermediación. Asimismo, el comercio electrónico afecta al papel de otros actores, como las entidades financieras y los fedatarios públicos.

Justo cuando se pensaba que era seguro entrar a la arena del comercio electrónico actual, surgió el fraude electrónico como una de las amenazas más peligrosas del mundo.

El fraude electrónico implica la distribución de mensajes de correo electrónico con direcciones de respuesta, enlaces y diseños que hacen que los correos electrónicos parezcan legítimos, como si hubiesen sido enviados por instituciones financieras a sus clientes.

Desafortunadamente, el único objetivo de estos correos electrónicos es engañar a los destinatarios, sin que ellos se den cuenta para que divulguen información de sus cuentas personales, tarjetas de crédito y otra información confidencial. Una vez que un consumidor ha compartido esta información, los estafadores obtienen los medios para robar identidades y efectuar transacciones fraudulentas con la información robada.

Los estafadores también roban información privada de los clientes al instarlos en forma engañosa a visitar un sitio web fraudulento, así como también a instalar programas espía en el computador del cliente, de manera que sea posible robar información cuando el usuario visita un sitio web legítimo.

El comercio electrónico plantea también problemas nuevos o agudiza algunos ya existentes en el comercio tradicional, entre ellos:

- La validez legal de las transacciones y contratos sin papel.
- La necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio.
- El control de las transacciones internacionales, incluido el cobro de impuestos.
- La protección de los derechos de propiedad intelectual.
- La protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales.
- La dificultad de encontrar información en Internet, comparar ofertas y evaluar la confianza del vendedor (y del comprador) en una relación electrónica.
- La seguridad de las transacciones y medios de pago electrónicos.
- La falta de estándares consolidados y la proliferación de aplicaciones y protocolos de comercio electrónico incompatibles.
- La congestión de Internet y la falta de accesos de usuarios de suficiente capacidad.[6]

Los problemas citados tienen, en mayor o menor medida, un componente legal y un componente tecnológico, por lo que su solución requiere actuaciones en ambos sentidos. Un buen ejemplo de este doble componente de los problemas que plantea el comercio electrónico es la seguridad de las transacciones y pagos electrónicos, en particular a través del Internet.

[6] Valentino F. Cornejo López, op. cit., pág. 190.

CAPÍTULO V. ARGUMENTOS CONTRA LA NO REGULACIÓN DE LA PRÁCTICA Y USO DEL INTERNET.

5.1. Derecho a la intimidad, a la libertad de expresión y al libre acceso a la información.

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".

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 g eneral 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 precedentes, 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, y en mi opinión, creo 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 en el mundo.

Así pues, en México, la libertad de expresión se fundamenta en los artículos 6° y 7° Constitucionales, así como en la Ley Federa l de Imprenta, la Ley de Radio, y Televisión y Cinematografía, así como en la reciente Ley Federal de Derechos de Autor.

Por lo tanto, considero 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.

El Artículo 109 de la Ley Federal del Derecho de Autor, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información.

Asimismo, la protección a este tipo de bases de datos es necesaria en virtud de que la información contenida en ellas, puede contener datos de carácter sensible, como son los de las creencias religiosas o la filiación política.

Adicionalmente pueden ser susceptibles de chantaje los clientes de determinadas instituciones de créditos que posean grandes sumas de dinero; en fin, la regulación de la protección de la intimidad personal es un aspecto de suma importancia que se encuentra regulado en este artículo.

Por lo anterior, el análisis de este artículo corrobora la posición que aquí se ha sostenido respecto a que en las conductas ilícitas relacionadas con la informática el bien jurídico a tutelar no es únicamente la propiedad intelectual sino la intimidad por lo que este artículo no debería formar parte de una ley de derechos de autor sino de una legislación especial tal y como se ha hecho en otros países.

Esta ley, además establece en el Título X, en su Capítulo Único, artículo 208, que el Instituto Nacional del Derecho de Autor es la autoridad administrativa en materia de derechos de autor y derechos conexos, quien tiene entre otras funciones, proteger y fomentar el derecho de autor además de que está facultado para realizar investigaciones respecto de presuntas infracciones administrativas e imponer las sanciones correspondientes.

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 Distrito Federal, 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 uno a 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.

5.2. La contemplación de los delitos informáticos en el Código Penal para el Distrito Federal.

Mucho se ha demostrado acerca de los beneficios que los medios tecnológicos y el uso de la informática en particular aportan a la sociedad actual.

Es indudable que la vertiginosidad del progreso no se presentaría si no intervinieran de manera directa los elementos electrónicos con los que contamos hoy en día.

Sin embargo, la utilización de dichos medios informáticos, al ser destinados al servicio de la sociedad, requieren de una inminente regulación jurídica con respecto a su utilización.

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

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

Urge que se regule en nuestro sistema penal el delito de fraude electrónico derivado de la práctica del comercio por internet para evitar que la comisión de este tipo delitos alcance en México los niveles de peligrosidad que se han registrado en otros países.

No obstante, que en nuestro país no se contemplan los delitos informáticos en ninguna legislación penal, con exclusividad del Estado de Sinaloa, considero que es importante adicionar estas conductas antijurídicas, para evitar, grandes daños tanto a las personas físicas, como las entidades públicas y demás sujetos, que utilizan la informática o telemático como medio de trabajo y desarrollo de sus actividades cotidianas.

Como se ha mencionado con antelación en capítulos pasados, en varios países sobre todo los más desarrollados ya se ha legislado al respecto, quizás el legislador nacional no está preparado todavía para introducirse en esta área y crear las normas jurídicas respectivas, empero, es de suma importancia que ya se comience a hacer algo al respecto, pues hay muchas conductas que implican responsabilidad para aquellos que las cometen, sin embargo, y en vista de que en nuestro país 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.

Por ello, considero que es importante legislar el delito de fraude electrónico derivado de la práctica del comercio por internet en nuestro Código Penal para el Distrito Federal, en los capítulos tanto de los Delitos contra el Patrimonio y de los Delitos contra la Libertad de las personas, lo referente a los "Delitos Informáticos", según mi apreciación con algunas hipótesis que se pudieran dar al cometer actos por medio del uso de las computadoras. A cada sociedad corresponde un Derecho Penal en específico, y el nacimiento de una sociedad del ciberespacio podría corresponder el del cyberderecho penal.

En el presente trabajo se ha perfilado el delito de fraude electrónico que merece ser regulado, a fin de poner a resguardo los principales bienes jurídicos involucrados, desde la intimidad hasta la vida misma, pasando por la propiedad y otros que resulta innecesario listar.

Como hemos visto, existen razones suficientes para la creación de un sistema penal único para el ciberespacio. Por lo demás, podemos considerar que nos encontramos ante una nueva sociedad que será la que quedará regulada por estas leyes especiales, lo cual no alteraría las soberanías nacionales, cuestión que hasta ahora es el mayor escollo para la creación de un organismo internacional dedicado a la persecución y juzgamiento de los delitos cometidos en la red.

Para concluir con esta aproximación a un tema de gran interés y de preocupación, se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (microprocesadores, inteligencia artificial, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

Por otro lado, se observa el gran potencial de la actividad informática como medio de investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

Finalmente, debe destacarse el papel del Estado, que aparece como el principal e indelegable regulador de la actividad de control del flujo informativo a través de las redes informáticas.

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 *world 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.

Es por ello, mi preocupación ante la poca o nula información que se cuenta sobre "Los Delitos Informáticos", definiéndolos en mi parecer como "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".

En México no se cuenta con una legislación que hable sobre los delitos Informáticos, con lo cual las conductas ilícitas que se realizan quedan impunes, y nuestro país no queda exento de ello.

La necesidad de regular estas conductas ilícitas ha llevado a varios países, especialmente a las grandes potencias a contemplar en sus legislaciones al respecto.

Así, podemos encontrar países como Alemania, donde se enfoca principalmente a la protección de datos personales contemplados en un soporte magnético, o Estados Unidos (siendo el más avanzado en cuanto a la regulación de los delitos Informáticos), el cual menciona el problema real de los virus informáticos así como también y de manera especial le da un enfoque a dichos delitos en su Ley de Privacidad; sin pasar por alto a Italia con una importante tradición criminalista, país que nos brinda una amplia gama sobre los Delitos Informáticos.

Todo lo anterior es de gran ayuda a países como el nuestro que aún no comienzan a legislar al respecto, así pues, los delitos informáticos constituyen una gran laguna en nuestras leyes penales, y el Derecho Comparado nos permite hacer una lista de los delitos que no están contemplados en nuestro Códigos Penales y que requieren análisis urgente por parte de nuestros académicos, penalistas y legisladores.

Son innumerables las conductas ilícitas que se pueden cometer a través de una computadora utilizándola ya sea como medio o fin, lo que nosotros denominamos "Delitos Informáticos", como lo son la destrucción de datos, el acceso no autorizado, el fraude informático, la transferencia de fondos o la intercepción del e-mail. Existen otros tantos que ya se encontraban, es decir, aquellos que tradicionalmente ya conocemos y que con el empleo de los medios informáticos se realizan de formas más novedosas; por mencionar algunos se encuentra la pornografía en el Internet o el propio narcotráfico, problemas sumamente difíciles de atacar que ahora, a través de ésta red de redes se pueden difundir a millones de personas, sin ninguna restricción.

Aún y cuando es innegable todos estos tipos de conductas que se están realizando con mayor frecuencia, también existen partidarios para la no regulación del uso del Internet.

Todas las actividades del hombre están regidas por el Derecho. Desde antes de su nacimiento, en el momento de la concepción, está protegido por la ley. Y cuando muere, sus decisiones tienen trascendencia más allá de su existencia, a través de los derechos y obligaciones que hereda a sus sucesores. Pensemos en cualquier actividad externa del hombre y veremos que está regida por el Derecho.

En esta época de avances tecnológicos, la informática, la cibernética, la computación y los sistemas no son materias ajenas a la ciencia jurídica. El uso de cajeros automáticos, las compras por internet, el navegar por la red, la contratación para accesar a internet, el chat, la pornografía infantil en línea, la piratería de programas, la piratería de la información (consistente en entrar a bases de datos sin autorización, actividad comúnmente conocida como hacker o piratas cibernéticos), los fraudes bancarios, los derechos de autor sobre material publicado en internet, las declaraciones fiscales, el uso de tarjetas de crédito en terminales, las declaraciones patrimoniales de los servidores públicos, los casinos en red, el correo electrónico, y la contaminación y destrucción de información que

se encuentra en equipos de cómputo (mediante el envío de virus), son algunas de las actividades y eventos regulados por el Derecho Informático o donde la Informática se aplica al Derecho.

El gran desarrollo tecnológico y su aplicación directa en la vida diaria, ha motivado que el Derecho esté desfasado respecto de los fenómenos que debe regular. En el mundo de la informática puede palparse un sentimiento de inseguridad, por falta de regulación específica y de un control efectivo respecto de todas las actividades que inciden en la materia.

El común de la gente puede ver dispersión y desconocimiento del marco jurídico que debe aplicarse a la informática, originándose temor y desconfianza. Es la labor del jurista superar la falta de sistematización en esta materia y tender hacia la consecución de un marco jurídico adecuado, que brinde seguridad jurídica en esta importante faceta de la vida moderna.

Uno de los usos más extendidos en materia informática, es la internet, a través del correo electrónico (e-mail), World Wide Web (www o web), FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos), listas de correos y grupos de discusión. Un aspecto que debe destacarse, es que la gran mayoría de los usuarios de internet se autorregulan, considerando los usos a que deben atenerse al utilizar la internet. Independientemente de lo que diga la legislación en esta materia, para ese gran número de usuarios existen modales y costumbres a los cuales se sujetan y que ellos mismos se imponen y hacen que los demás los respeten. Para esos usuarios seguir esos lineamientos cibernéticos que la propia comunidad ha creado, puede ser más obligatorio que sujetarse al marco jurídico en la materia.

Actualmente las normas del Derecho Informático están derivadas de otras ramas. Es así, que el comercio electrónico está regulado en el Código de Comercio; los delitos informáticos están previstos en el Código Penal Federal; la contratación entre ausentes, que se efectúe a través de medios informáticos, la

encontramos en la legislación civil; la presentación de declaraciones fiscales está en la normatividad fiscal; la presentación de declaraciones patrimoniales de los servidores públicos está contenida en el Derecho Administrativo. Esta dispersión es la que debe evitarse y tender a unificar y a sistematizar, que no recopilar, las diferentes disposiciones en materia de Derecho Informático.

Nuestro Código Penal Federal prevé, en sus artículos 211 bis 1 a 211 bis 7, las conductas tipificadas como acceso ilícito a sistemas y equipos de informática.

Estos delitos, entendidos en relación con lo previsto en el artículo 50, fracción I de la Ley Orgánica del Poder Judicial de la Federación, que establece cuales son los delitos federales, son competencia de la Procuraduría General de la República y, en su momento procesal, de los Juzgados de Distrito y de los Tribunales de Circuito. En materia local puede mencionarse el caso de los delitos informáticos, previstos con esta denominación en el artículo 217 del Código Penal para el Estado de Sinaloa, citados por Jesús Antonio Molina Salgado, en su estudio denominado Delitos y otros ilícitos informáticos en el Derecho de la Propiedad Industrial.

Por otra parte, este autor menciona, independientemente de las conductas previstas en la legislación penal mexicana (local y federal), como ilícitos o delitos informáticos muy particulares los siguientes: cracking; *cyber gangs* (ciber pandillas); *cyber grafitti defacements web hacks; cyber stalking* (ciber acoso); *cyber terrorism* (ciber terrorismo); *domain name service hacks* (hacking de un servicio de nombres de dominio); hacking; hacktivismo (hacking y activismo); *ID theft* (robo de identidad); *phreaking o phreaks* (hacking o cracking telefónico); *social engineering* (ingeniería social); y *warez* (piratería).

PROPUESTAS

En la presente investigación, se busca crear una conciencia sobre la necesidad urgente de regular este delito, 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.

Es importante mencionar que muchos de estos delitos serían contemplados en el Fuero Federal, como la pornografía, las sectas, el narcotráfico, la intercepción de e-mail, todos ellos a través del Internet; lo cual es también un reto importante para el legislador federal.

Después del estudio de las experiencias adquiridas por diferentes países al enfrentar el delito informático y la forma en que está siendo regulada esta problemática en México, además del evidente incremento de esta situación, es necesario a pesar de que en el país el delito informático no ha alcanzado el grado de peligrosidad existente en esos países, regular penalmente las conductas ilícitas derivadas del uso de la computadora.

En primer término, la difusión a las empresas, organismos, dependencias, particulares y a la sociedad en general, contribuirá notoriamente al nivel de concientización sobre el problema que nos ocupa.

El siguiente paso será dar a conocer las medidas preventivas que se deben adoptar para evitar estas conductas ilícitas. Sin embargo, con base en que en la Ley Federal del Derecho de Autor se considera como bien jurídico tutelado la propiedad intelectual y que, el bien jurídico tutelado en los delitos informáticos es fundamentalmente el patrimonio, se sugiere que en el Título Vigésimo Segundo

sobre los Delitos en Contra de las Personas en su Patrimonio del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal se añada un capítulo especial para los delitos informáticos.

Teniendo en cuenta también la gravedad que implican los delitos informáticos, es necesario que el Código Penal Federal incluya figuras delictivas que contengan los delitos informáticos ya que de no hacerlo, la ausencia de figuras concretas que se puedan aplicar en esa materia daría lugar a que los autores de esos hechos quedaran impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos.

Por otra parte, teniendo presente que el Estado de Sinaloa a través de su Congreso Local ha legislado sobre el tema de delitos informáticos, contemplando de forma general una amplia variedad de los mismos y estableciendo las sanciones correspondientes, se establece que es necesario que con objeto de que se evite un conflicto de competencia entre los congresos locales y el de la Unión, éste, con base en las facultades que la Constitución Federal le confiere, establezca los criterios necesarios para delimitar, dada la naturaleza de los delitos informáticos, que pueden emplear para su ejecución las vías generales de comunicación entre otros elementos, la jurisdicción federal y local de estos ilícitos.

Lo que pretendo, aparte de crear una conciencia general sobe los Delitos Informáticos, es que los usuarios que hagan mal uso de ello, sepan que pueden ser sancionados y sean sancionados. No permitir que estos delitos sigan quedando impunes por falta de una legislación adecuada o bien se tipifiquen en otro delito que no es aplicable muchas veces al caso concreto.

El derecho penal de los estados interesados en combatir esta nueva delincuencia, contiene vacíos jurídicos y diferencias importantes susceptibles de obstaculizar la lucha contra la delincuencia organizada y el terrorismo, así como los agraves ataques contra sistemas de información perpetrados por particulares.

La aproximación del Derecho Positivo en materia de delincuencia informática contribuirá a que las legislaciones nacionales sean lo suficientemente completas para que todas las formas de ataques contra los sistemas de información puedan ser objeto de investigaciones mediante técnicas y métodos disponibles en Derecho Penal.

Los autores de estos delitos deben ser identificados y llevados a juicio y los tribunales deben disponer de sanciones adecuadas y proporcionadas. Se enviará así un claro mensaje disuasivo a los autores potenciales de ataques contra los sistemas de información. Además, los vacíos jurídicos y las diferencias pueden impedir una cooperación policial y judicial eficaz en caso de ataques contra sistemas de información. Estos ataques son trasnacionales por su propia naturaleza y requieren una cooperación internacional.

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 cómo 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.

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

- 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 país 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 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.
- 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 está hablando sobre las comunicaciones electrónicas, el Internet o un soporte de datos.

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 estos 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.

Teniendo en cuenta la gravedad que implica este delito, considero que es necesario que el Código Penal Federal incluya una figura delictiva que contenga el delito de fraude electrónico derivado de la práctica del comercio por internet ya que de no hacerlo, la ausencia de una figura concreta que se pueda aplicar en esta materia daría lugar a que los autores de esos hechos quedaran impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos.

Por otra parte, teniendo presente que en nuestro país, el Estado de Sinaloa a través de su Congreso Local ha legislado sobre el tema de delitos informáticos, contemplando de forma general una amplia variedad de los mismos y estableciendo las sanciones correspondientes, consideramos que es necesario que con objeto de que se evite un conflicto de competencia entre los congresos locales y el de la Unión, éste con base en las facultades que la Constitución Federal le confiere, establezca los criterios necesarios para delimitar, dada la naturaleza de los delitos informáticos, que pueden emplear para su ejecución las vías generales de comunicación entre otros elementos, la jurisdicción federal y local de estos ilícitos.

CONCLUSIONES

PRIMERA. No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.

- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.
- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.
- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.
- La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

SEGUNDA. Desde la Criminología debemos señalar que el anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados, son un factor criminógeno que favorece la multiplicación de autores que utilicen los medios electrónicos para cometer delitos a sabiendas que no serán alcanzados por la ley.

TERCERA. No solo debe pensarse en la forma de castigo, sino algo mucho más importante como lograr probar el delito. Este sigue siendo el principal inconveniente a la hora de legislar por el carácter intangible de la información.

CUARTA. La dificultad de tipificar penalmente situaciones sometidas a un constante cambio tecnológico, la manifiesta insuficiencia de las sanciones en relación con la gravedad y el daño de los crímenes informáticos y la propia

inadecuación de los medios penales tradicionales para remediar esta situación, determinan que, el Derecho penal informático sea un ejemplo manifiesto de Derecho penal simbólico.

"Al final, la gente se dará cuenta de que no tiene ningún sentido escribir leyes específicas para la tecnología. El fraude es el fraude, se realice mediante el correo postal, el teléfono o Internet. Un delito no es más o menos delito si se utilizó criptografía (...). Y el chantaje no es mejor o peor si se utilizaron virus informáticos o fotos comprometedoras, a la antigua usanza. Las buenas leyes son escritas para ser independientes de la tecnología. En un mundo donde la tecnología avanza mucho más deprisa que las sesiones del Congreso, eso es lo único que puede funcionar hoy en día. Mejores y más rápidos mecanismos de legislación, juicios y sentencias...quizás algún día."

QUINTA. Debido a la ausencia en la legislación mexicana de una normatividad que tipifique las conductas delictivas que han surgido con el uso cada vez más generalizado de las redes electrónicas de información, se propone el siguiente tema de tesis “La necesidad de legislar el delito de fraude electrónico derivado de la práctica derivada del comercio por internet”, por el cual se modifica el Código Penal atendiendo a la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

SEXTA. En la actualidad han surgido muchos problemas relacionados con el uso de computadores, amenazas que afectan negativamente tanto a individuos como a empresas.

SÉPTIMA. La proliferación de éstos como la principal herramienta de funcionamiento en casi todos los niveles de convivencia, así como la creación de

la red global Internet ha provocado que cada vez más personas se las ingenien para lucrar, hacer daño o causar perjuicios a través del uso de estos instrumentos.

OCTAVA. Con la presente tesis se pretende legislar y sancionar los delitos electrónicos ya que son una serie de conductas que, sorprendentemente, no tienen aún mención alguna en Nuestra Legislación Penal, con esto se busca prevenir y solucionar problemas evidentes y manifiestos dentro de la práctica del comercio por internet.

NOVENA. Después del estudio de las experiencias adquiridas por diferentes países al enfrentar el delito informático y la forma en que está siendo regulada esta problemática en México, además del evidente incremento de esta situación, considero necesario a pesar de que en el país el delito informático no ha alcanzado el grado de peligrosidad existente en esos países regula penalmente las conductas ilícitas derivadas del uso de la computadora.

DÉCIMA. El objetivo de este trabajo fue el de analizar las conductas delictivas que puede generar el gran avance tecnológico, sobre todo en el campo de la informática.

Como se observo durante el desarrollo del presente trabajo las tecnologías informáticas ofrecen no sólo un aspecto positivo, sino uno negativo mismo que ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no eran posibles de imaginar.

DÉCIMA PRIMERA. Los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquélla. En ese entendido, el presente trabajo se dirige al análisis del los delitos electrónicos así como su manifestación en la red de redes Internet.

DÉCIMA SEGUNDA. Durante la etapa de investigación se encontró que no existe un concepto de delito electrónico, y que estudiosos del tema han definido desde diferentes puntos de vista como son el criminógeno, formal, típico y atípico, etc., únicamente al delito informático mencionando que el primero es solo una rama del informático, por lo que en el presente trabajo tomamos como concepto el mencionado por María de la Luz Lima. Además se han señalado los sujetos activos y pasivos, clasificación y los tipos de delitos informáticos considerados tanto en la doctrina como en la legislación de diferentes países.

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

DÉCIMA CUARTA. Por otra parte, analizamos la regulación que han tenido en la legislación mexicana las conductas ilícitas relacionadas con la informática. Para ello se estudiaron los antecedentes que han tenido las regulaciones vigentes en esta materia: Acuerdos celebrados en el marco del Acuerdo General de Aranceles Aduaneros y Comercio (GATT) y El Tratado de Libre Comercio de América del Norte (TLC).

DÉCIMA QUINTA. Se realizó una breve reseña del tratamiento administrativo que se realiza a través de la Ley Federal del Derecho de Autor, y en el penal que se ha establecido en el Título Vigésimo Sexto del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal.

Sobre el particular, debe aclararse que esta ley no regula delitos informáticos ya que su competencia es la de sancionar administrativamente conductas ilícitas cuyo bien jurídico a tutelar es la propiedad intelectual.

DÉCIMA SEXTA. Se incluye una propuesta para legislar el delito de fraude electrónico derivado de la práctica del comercio por internet, sustentada en el estudio comparativo antes mencionado, que trata de adecuar a la realidad existente en México, pero previendo que nuestro país no está exento de la velocidad del desarrollo tecnológico y de los vicios que éste genera.

DECIMA SÉPTIMA. La no regulación de este delito, a la larga podría traer implicaciones muy desventajosas para México, entre las que podemos citar: la pérdida de prestigio a nivel internacional por el actuar ilícito de empresas cuyo radio de acción no está reducido al ámbito nacional y la pérdida de credibilidad por parte de las empresas, lo que se traduciría en un mercado poco atractivo para ellas que pondrían al país en una situación marginada del desarrollo comercial. En este entendido, consideramos que por la gravedad de la conducta ilícita en sí, y las implicaciones que traería aparejadas, justifica su regulación penal.

DÉCIMA OCTAVA. Esperemos que durante este año, nuestros legisladores retomen el tema y puedan encontrar una fórmula correcta y apropiada para legislar el robo de identidad y otros delitos informáticos, tomando en cuenta los instrumentos internacionales existentes, las prácticas y políticas implementadas en otros países y estableciendo mecanismos de cooperación para compartir información con otros países, que permita el rastreo, localización y ejecución de los delincuentes en forma más rápida y flexible. En la medida en que esto se haga, las empresas de comercio electrónico y las instituciones financieras gozarán de mayor certeza jurídica y, sobre todo, se ayudará a proteger y brindar mayor confianza a la parte más vulnerable en Internet: el usuario final.

BIBLIOGRAFÍA

- AMUCHATEGUI REQUENA, Griselda, Derecho Penal, 3ª. edición, editorial Oxford, México, 2007.

- CASTELLANOS TENA, Fernando, Lineamientos elementales de Derecho Penal, 40ª. edición, editorial Porrúa, México, 2004.

- CÁMPOLI, Gabriel Andrés, Derecho Penal Informático en México, Instituto Nacional de Ciencias Penales, México, 2004.

- CARBALLAR FALCÓN, José Antonio, Internet: Libro del Navegante, 3ª. edición, editorial Ra- Ma, Madrid, 2002.

- CORNEJO LÓPEZ, Valentino F. Los medios electrónicos regulados en México: comercio electrónico, documentos electrónicos, firma electrónica y certificados digitales, editorial Sista, México, 2006.

- GALINDO SIFUENTES, Ernesto, Derecho Mercantil: comerciantes, comercio electrónico, contratos mercantiles y sociedades mercantiles, prólogo de Consuelo Sirvent Gutiérrez, 1ª. edición, editorial Porrúa, México, 2004.

- GONZÁLEZ QUINTANILLA, José Arturo, Derecho Penal Mexicano, (Parte General), editorial Porrúa, México, 1993.

- HANCE, Olivier, Leyes y Negocios en Internet (Trad. de Yazmín Juárez Parra), Mc Graw Hill, México. 1996.

- MALO CAMACHO, Gustavo, Derecho Penal Mexicano, 2ª. edición, editorial Porrúa, México, 1998.

- MARCELO RODAO, Jesús de, Piratas cibernéticos: cyberwars, seguridad informática e internet, editorial Ra-Ma, México, 2001.

- MÁRQUEZ PIÑERO, Rafael, Derecho Penal. Parte general, 4ª. edición., Trillas, México, 1999.

- MOLINA SALGADO, Jesús Antonio, Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial, editorial Porrúa, México, 2003.

- PALAZZI, Pablo Andrés, Delitos Informáticos, AD-HOC, Buenos Aires, Argentina, 2000.

- RIBAS, Alejandro Javier, Aspectos Jurídicos del comercio electrónico en internet**,** Editorial Aranzadi, segunda edición, Pamplona, 2003.

- TÉLLEZ VALDÉS, Julio, Derecho Informático, Editorial Mc Graw Hill, tercera Edición, México, 2004.

LEGISLACIÓN CONSULTADA:

- CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS. México 2007, Editorial SISTA.
- Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal contiene todas las reformas conocidas hasta el 17 de enero de 2007. Editorial Grupo ISEF. 19ª. Edición, México, 2007.
- Código Penal del Estado de Sinaloa, Culiacán Rosales, Sinaloa 1998.
- Ley Federal del Derecho de Autor, publicada en el Diario Oficial de la Federación el 24 de diciembre de 1996, texto vigente, última reforma publicada DOF 23-07-2003.

PÁGINAS WEB CONSULTADAS:

http://www.delitosinformaticos.com.mx

http://webopedia.internet.com/