UNIVERSIDAD SALESIANA

FACULTAD DE DERECHO

INCORPORADA A LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

"CREACIÓN DE LA UNIDAD ESPECIALIZADA DE INVESTIGACIÓN EN DELITOS INFORMÁTICOS EN LA PROCURADURÍA GENERAL DE LA REPÚBLICA"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

P R E S E N T A :

PATRICIA VALDIVIESO TREJO

ASESOR: MARIO ALBERTO MARTELL GÓMEZ

MÉXICO, D.F 2008

AGRADECIMIENTOS

A DIOS

Por mi existencia y por siempre tenerme presente.

A MIS PADRES

Por darme la vida, su amor, cuidados, consejos, regaños, y forjarme como ser humano.

A MI NIÑO HERMOSO (PATRICIO)

Por ser mi motor en la vida, por su sonrisa, su ternura y amor.

A MI ESPOSO

Por estar a mi lado y caminar junto a mí.

A ARACELY

Por ser tan buena amiga y estar conmigo en los momentos más difíciles.

A MI CHAPARRITO

Por todos los momentos que vivimos juntos.

A CLAUS, MARIBEL Y LOOPS

Por estos 14 años de amistad.

A UNISAL

Por los conocimientos adquiridos durante cinco años y por mi formación profesional.

A LOS LIC(S). MARTELL Y JUÁREZ

Su infinito agradecimiento por su ayuda, disponibilidad y apoyo.

ÍNDICE

INTRODUCCIÓN

ELECCIÓN Y JUSTIFICACIÓN DEL TEMA.

Para iniciar este proyecto de investigación, es necesario adentrarnos en la problemática que sucede en nuestra sociedad mexicana; para ello, comenzaremos con un breve análisis.

Al hablar de delitos informáticos, pensamos que es un delito contemporáneo, y que estas cuestiones sólo suceden en países desarrollados o que sucederán en un futuro lejano, pero estamos en un grave error; si bien es cierto que México no está al día con avances tecnológicos y por ende, jurídicos, es por la existencia de un vacío legislativo y aun más en materia de delitos informáticos, ya que para ser investigados se necesita una correcta interpretación penal ¿Por qué esperar a que sucedan en un futuro para ser tipificados en toda la República Mexicana?

Los delitos informáticos sólo se encuentran tipificados en algunos Códigos Penales de las Entidades Federativas.

Si bien es cierto se encuentra legislado en algunos estados, estas modificaciones no coinciden con las descripciones de los tipos penales, en donde más adelante del desarrollo de tesis abundaremos y haremos mención y crítica a éstas; ya que sólo han tratado cuestiones de forma y no de fondo lo peor es que ni en los delitos comunes se pueden manejar las cuestiones probatorias ni de procedimiento cuando los delitos se cometen por medios informáticos.

Por esta y más razones consideramos que es necesario y urgente el reformar el Reglamento de la Ley Orgánica de la Procuraduría General de la

República, en su artículo 2, donde se mencionan los asuntos de la competencia de la Procuraduría, de su titular y del ministerio público de la Federación, las unidades administrativas y órganos desconcentrados**,** donde se implemente la creación de la **UNIDAD ESPECIALIZADA DE INVESTIGACIÓN EN DELITOS INFORMÁTICOS**, para dar un seguimiento a las denuncias de los ciudadanos sobre hechos que constituyan ese tipo de ilicitudes, o bien que se deriven de la Policía Cibernética y acudan con el titular de dicha Unidad.

El ministerio público federal acreditará un curso de especialización en delitos Informáticos para la integración de la averiguación previa, todo lo anterior apegado de conformidad con los artículos, 8 y 27 del Reglamento de la Ley Orgánica de la Procuraduría General de la República.

La Secretaría de Seguridad Pública es la encargada de la prevención del delito; y por lo tanto con el crecimiento de los delitos informáticos se crea la Policía Cibernética, la cual tiene como fin vigilar o patrullar las páginas Web que existan y la comisión de delitos por medios informáticos como nos referimos en el Código Penal Federal (en los artículos 211 bis 1- 211 bis 7)

La Policía Cibernética junto con las personas que integran la Unidad Especializada en delitos informáticos deberán trabajar en paralelo, es decir en el caso de que la policía cibernética detectara por medio de la vigilancia de las páginas Web o reciban una denuncia de cualquier ciudadano de carácter en delitos informáticos, está le informe a la Unidad Especializada para intervenir con el fin de que la tarea de prevención del delito sea más efectiva o en su caso que surjan de la acción directa de la Policía Cibernética.

PLANTEAMIENTO DEL PROBLEMA.

Atendiendo a la necesidad que una sociedad informada tiene, con relación a los avances tecnológicos, jurídicos y principalmente en materia de delitos informáticos, estos surgen desde el momento en donde el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y son de diverso tipo por la utilización indebida de medios informáticos, y donde dichos Bienes Jurídicos que se protegen son a través de los tipos penales:

La propiedad

La privacidad

Son delitos cometidos por medio de equipos electrónicos y elementos informáticos, en donde para ser perseguidos dependen de una correcta interpretación penal y una toma de conciencia de las autoridades en donde para encajar éstos, es necesario definir los tipos penales, que causan un daño económico irreparable.

Los que cometen este tipo de delitos son personas con un conocimiento amplio adquirido por la experiencia, que cuentan con los medios electrónicos necesarios y en donde esta clase de delitos van siempre ligados a un dolo, ya que resulta imposible que se cometan por negligencia o simplemente los sujetos activos de esta clase de delitos son empleados de la empresa donde laboran y por lo tanto, sus conductas afectan el bien jurídico tutelado.

Es por consiguiente que el bien que se intenta proteger al penalizar estas acciones son:

La intimidad

La propiedad

Las principales **características** de esta clase de delitos, por mencionar algunas son:

a) Conductas criminales de cuello blanco. La similitud que tienen los delitos informáticos con los delitos de cuello blanco, es el sujeto activo quien es una persona con un status socioeconómico alto.
b) Son acciones ocupacionales (Las realiza el sujeto activo en su trabajo);
c) Son acciones de oportunidad;
d) Provocan serias pérdidas económicas (Casi siempre producen beneficios);
e) Demasiados casos y pocas las denuncias (Debido a un vacío legislativo);
f) Ofrecen facilidad para ser cometidos por menores de edad; (debido a que no figura el menor en la aplicación de la ley).

Como instrumento o medio:

a) Falsificación de documentos vía computarizada (tarjetas de crédito).
b) Modificación de datos.
c) Alteración en el funcionamiento de los sistemas, a través de virus informáticos.
d) Sustracción o copiado de información confidencial; por mencionar algunas.

Como Fin:

a) Destrucción de programas.
b) Atentado físico contra el equipo informático.
c) Sabotaje político o ciberterrorismo; (por mencionar algunos)

Tipos de delitos:

Acceso no autorizado: Uso ilegítimo de claves para entrar de esta forma a sistemas informáticos.

Destrucción de datos: Daños causados en la red por virus.

Transferencia de fondos: Engaños en la realización de transacciones financieras.

Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y a empresas e interceptación de correos electrónicos por mencionar algunos.

Todo lo anterior nos lleva a una serie de pérdidas económicas, que al paso de los años es más de difícil de prever. Estas pérdidas son cuantiosas para una sociedad y por lo mismo, van ligadas a una impunidad que existe por parte de las autoridades como la indiferencia o el desconocimiento del delito, ya que quien realiza este tipo de delitos en su mayoría son sancionados de forma administrativa y no privativa de la libertad, estando tipificado.

Es por eso que se hace mención de una serie de conductas dentro de la cuales cabe señalar la evasión de impuestos, crimen organizado, lavado de dinero, tráfico de armas, tráfico de drogas, compra venta de menores, compra venta de órganos, que si bien no son delitos informáticos son cometidos por medios informáticos.

HIPÓTESIS DE TRABAJO.

Si argumentamos que una **UNIDAD ESPECIALIZADA DE INVESTIGACIÓN EN DELITOS INFORMÁTICOS,** requiere ser autónoma en tanto ejercicio y competencia, entonces las autoridades requerirán realizar una labor ardua, en donde el ciudadano cuando descubra que ha sido afectado, recurra al ministerio público y en donde la investigación esté a cargo de la policía cibernética, la cual tendrá como uno de sus fines vigilar las páginas Web que pudiesen afectar lo contenido con relación a los artículos 211 BIS 1- 211 BIS 7 del Código Penal Federal.

OBJETIVOS.

Estudiar el concepto básicamente *jurídico-penal*; así como los delitos informáticos, con el fin de pasar a lo substancial para ofrecerles una crítica de la misma legislación vigente. Posteriormente identificar sus características, clasificación, tipo de los delitos informáticos, así como sus orígenes y evolución.

Continuar con un análisis de los códigos estatales que contemplan los delitos informáticos, así como el Reglamento de Ley Orgánica de la Procuraduría General de la República para la implementación de la unidad especializada.

METODOLOGÍA.

El análisis de los delitos informáticos respecto de su evolución histórica a través de una Legislación comparada con otros países y en México, requiere del estudio de los conceptos básicos, partiendo de una descomposición de los elementos de los delitos informáticos y del Derecho Penal Informático en México; Así como la interpretación de los ordenamientos jurídicos, que serán, el Reglamento Interior de la Procuraduría General de la República, Código Penal Federal, así como demás códigos estatales en materia de Delitos Informáticos que nos indique la regulación nacional actual de nuestra figura jurídica en estudio.

Para satisfacer este análisis utilizaremos los siguientes métodos:

1) Histórico-descriptivo de los Delitos Informáticos y de su Legislación.
2) Derecho comparado:
3) Análisis critico:
4) Hermenéutica:

CAPÍTULO 1.- MARCO CONCEPTUAL DEL DELITO INFORMÁTICO

1. 1. DERECHO INFORMÁTICO, ORIGEN, CONCEPTOS, EVOLUCIÓN Y CARACTERÍSTICAS.

Antes de entrar al desarrollo del tema que nos ocupa, es necesario retomar sus antecedentes y conceptos (nociones básicas del Derecho Informático) tales como: cibernética, informática, computadora, sociedad de la información, hasta adentrarnos al Derecho Informático, ya que todo avance tecnológico e intelectual sienta sus bases en los antecedentes, mismos que dan su origen. Así tenemos por ejemplo a la escritura que permite conservar el conocimiento a través de textos dejando atrás a la palabra como único medio de transmisión de conocimiento; igual sucede con la imprenta de Gutemberg que permitió que esos textos transmisores de conocimiento se pudieran reproducir, mismos que llegaron a todas partes del mundo.

La Informática surge desde luego antes que el Derecho Informático; sin embargo es necesario adentrarse lo que da su origen que es la cibernética. Esta proviene del griego kybernetes, “piloto” y Kybernes, lo cual es un concepto que se refiere al arte de gobernar.

En sí la palabra **cibernética** es la ciencia de la comunicación y el control entre el hombre y la máquina. (1)

La **cibernética** es la ciencia que se ocupa de los sistemas de control y de comunicación en las personas y en las máquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes. (2)

Esta ciencia tiene sus orígenes en el año de 1942, en la celebración de un congreso sobre la inhibición cerebral celebrado en la Ciudad de Nueva York, del cual surgió la idea de la fecundidad de un intercambio de conocimiento entre fisiólogos y técnicos en mecanismos de control. Cinco años más tarde, Norbert Wiener uno de los principales fundadores de esta ciencia (matemático estadounidense), quien propuso el nombre de cibernética derivado de una palabra griega, puede traducirse como piloto, timonel o regulador.

Por tanto la palabra **cibernética** podría significar ciencia de los mandos. (3)

Así mismo, estos mandos son estructuras con elementos especialmente electrónicos y en correlación con los mecanismos que regulan la psicología de los seres vivientes y los sistemas sociales humanos, y a la vez permiten la organización de máquinas capaces de reaccionar y operar con más precisión y rapidez que los seres vivos; ofrecen posibilidades nuevas para penetrar más exactamente las leyes que regulan la vida en general y especialmente la del hombre en sus aspectos psicológicos, económicos, sociales, etc.

Así tenemos que la **cibernética** es una ciencia de la comunicación y por tal existe una relación causal entre el hombre y ésta, donde los aspectos aplicados se relacionan con cualquier campo de estudio.

La **informática** surge de la necesidad de información por parte del hombre y por lo tanto éste desarrolla nuevos métodos o técnicas para satisfacer esas necesidades.

Es decir, la palabra **informática** proviene de los vocablos información y automatización o bien, es el conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información.

Informática: Conjunto de disciplinas y técnicas desarrolladas para el tratamiento automático de la información mediante máquinas computadoras (hardware) que funcionan con distintos programas (software). (4)

Una de las primeras creaciones del hombre para darse a la tarea de operaciones de cálculo fue el ábaco, las tablas de logaritmos por John Napier en 1614, multiplicaciones y divisiones por medio de sumas y restas, regla de cálculo en 1630 que constaba de la medición de longitudes, máquina de Pascal en 1642 -fue la primera máquina de cálculo semiautomática construida por el hombre-; La tarjeta perforada en 1804 por Joseph Marie, fue la primera máquina que leía tarjetas perforadas que contenían información; máquina de Babbage en 1834, creada por Charles Babbage, la cual realizaba cálculos reduciendo errores logaritmos y donde fue determinante en el desarrollo de las computadoras actuales.

Por lo tanto, la computadora es un instrumento operativo y está presente en la sociedad moderna, pero no solo es una herramienta de apoyo a las actividades humanas sino un medio para conseguir información; son un fenómeno de tipo social, es decir científico-tecnológico, ya que es útil tanto para particulares como para gobiernos, debido a su ahorro de tiempo en el trabajo, el avance en aspectos científicos, en lo escolar, en rápido acceso de información y por supuesto en delitos donde más adelante entraremos a profundidad.

Se habla de cuatro generaciones de las computadoras que fueron evolucionando al paso de los años desde la primera generación, donde las máquinas funcionaban a base de bulbos hasta la última que lo hace con microchips.

La primera generación consistió en la sustitución de los bulbos por los de transistores, se introducen memorias de ferrita que permitieron la reducción del tamaño, surgiendo así la segunda generación.

La tercera generación fue en 1963, (que consistió en el uso de circuitos integrados monolíticos que aumentaron la velocidad y redujeron el tamaño y costo.

Y por último, la cuarta generación, consistió en la integración a larga escala (LSI) y la aparición de microcircuitos integrados en las plaquetas de sicilio que conocemos como microchips.

Así, las primeras computadoras fueron desarrolladas por:

Mark I (1937-1944), Eniac (1943-1945), Edvac (1945- 1952) y la Univac (1951).

Por lo tanto, es evidente que todos los procesos y avances mundiales son gracias a las computadoras.

Computadora: Es una máquina automatizada de propósito general, integrada por elementos de entrada, procesador central, dispositivo de almacenamiento y elementos de salida.

De manera operacional la computadora consta de los siguientes elementos:

Los elementos de entrada son aquellos que representan la forma de alimentación e información a la computadora, por medio de datos e instrucciones realizadas por equipos periféricos como pantallas, cintas, discos, disquetes, etc.

El procesador central es un dispositivo donde se ejecutan las operaciones lógico-matemáticas, conocido comúnmente como unidad central de proceso (CPU).

El dispositivo de almacenamiento es el que almacena la información a procesar.

Y por último los elementos de salida son medios en los que se reciben los resultados del proceso efectuado (pantalla, impresora, etc.)

A manera de estructura la computadora se compone de:

Hardware: Esta integrado por parte mecánicas, electromecánicas y electrónicas; o sea, es la estructura física de la computadora, que se encarga de la captación, almacenamiento y procesamiento de información, así como de obtención de resultados.

Software: Es la estructura lógica que permite a la computadora la ejecución de actividades, es decir son los programas. (5)

La **sociedad de la información** es el uso masivo de las Tecnologías de la Información y Comunicación (TIC) para difundir el conocimiento y los intercambios en una sociedad. (6)

¿A que nos referimos con una sociedad de la información? Como se mencionó anteriormente, la informática surge de la necesidad de la información por parte del hombre y ésta como tal, ha repercutido en el desarrollo de varios ámbitos de una sociedad tales como lo social, cultural, político y principalmente en lo tecnológico; por lo tanto, ésta se encuentra en ascendente y no se sabe hasta qué nivel pueda llegar.

Los factores para lograr o alcanzar una sociedad de la información son la contribución para mejorar la vida de los ciudadanos y debe ser por medio de las tecnologías de la información y comunicación (TIC), con el fin de lograr una democracia, transparencia y un gobierno eficaz.

Otro de los tantos factores es la participación de personas, organismos, interesados en alianzas nacionales, regionales y mundiales.

Es necesario dar un enfoque de lo anterior a través de la "Cumbre Mundial sobre la Sociedad de la Información", la cual se convocó el pasado 21 de diciembre de 2001 por la Asamblea General de las Naciones Unidas y se celebró en Ginebra, del 10 al 12

de diciembre de 2003, y la segunda tuvo lugar en Túnez, del 16 al 18 de noviembre de 2005.

Por lo tanto, el organismo de las Naciones Unidas encargado de dirigir la organización de la Cumbre es la **Unión Internacional de Telecomunicaciones (UIT)**, con sede en Ginebra (Suiza).

Esta cumbre es derivada de una evolución tecnológica en la información y comunicación; es decir, una serie de ideas y conocimientos repartidos en todo el mundo a través de diferentes medios tal es como Internet y en donde uno de los fines de esta cumbre es garantizar que estos beneficios sean para todos y promover ciertas ventajas como en la igualdad de género, educación, salud, etc., así como el acceso a la información y en donde además la comunicación permita solucionar los conflictos y alcanzar la paz mundial.

En la Cumbre de Ginebra de diciembre de 2003, los líderes mundiales declararon: "Nuestro deseo y compromiso comunes de construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos". (7)

Así, al hablar de Derecho Informático nos vienen a la mente conceptos como computadoras, tecnología, Internet, etc., lo que es correcto, pero pocos saben que es

una rama de reciente creación del conocimiento jurídico y en continua evolución que ha venido a trastocar a varias disciplinas jurídicas existentes.

El Derecho Informático como tal, en el año de 1949 por Norbert Wiener, en su libro Cibernética y Sociedad en cuyo capítulo IV, consagrado al Derecho y las Comunicaciones, manifiesta la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más prominentes: el jurídico; así mismo en ese año el juez estadounidense Lee Loevinger publicó en un artículo en la revista de Minnesota Law Review "The Next Step Forward", en donde menciona que el próximo paso en el largo camino del progreso del hombre, debe ser el de la transición de la Teoría General del Derecho hacia la Jurimetría, que es la investigación científica acerca de los problemas jurídicos.

Por lo tanto el **Derecho Informático** es una rama de la ciencia jurídica que considera a la informática como instrumento y objeto de estudio del Derecho. (8)

Derecho Informático: Consiste en el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la Informática. (9)

Derecho Informático: Es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática. (10)

Para Héctor Peñaranda, El **Derecho Informático** constituye el conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática. (11)

Por nuestra parte, consideramos que el derecho informático es el conjunto de normas, principios e instituciones jurídicas que regulan las relaciones entre el

estado, entre los particulares y del estado con los particulares, en las cuales se encuentra presente la tecnología informática.

Los orígenes del Derecho Informático se dieron por medio o a través de la informática jurídica, es decir como hace mención el Dr. Julio Téllez en su obra Derecho Informático, la clasificación del Derecho Informático se hace en base a dos vertientes; la informática jurídica y el derecho de la informática.

Antes de ser llamada informática jurídica, ésta tuvo varias interpretaciones tales como Jurimetrics (Jurimetría), término dado por Lee Loevinger en 1949 de nacionalidad estadounidense; más tarde fue Giuscibernética que consiste en que la cibernética aplicada al derecho no solo ayuda a la depuración cuantitativa sino también a la cualitativa, y por último Computers and Law en países Anglosajones o Rechtsinformatique en Alemania, o Jurismática en México; sin embargo el más adecuado y preciso fue dado por los franceses Informatique Juridique.

Por tal, la informática jurídica es el conjunto de aplicaciones de la informática en el ámbito del Derecho, es decir la relación entre Derecho e Informática.

La informática jurídica surge como tal en Estados Unidos en el año de 1959 por Healtth Law Center de la Universidad de Pittsburg donde sus primeras manifestaciones fueron de recuperación de documentos jurídicos de manera automatizada. Cabe señalar que en los años 50 empiezan a utilizarse las primeras computadoras y toda esta recuperación tuvo el propósito de encontrar medios satisfactorios para tener acceso a la información legal.

Es decir, la informática jurídica consistía en la recuperación de información que contenían datos jurídicos tales como (Leyes, Jurisprudencia, etc.), más tarde se vio la

posibilidad que estos bancos de datos jurídicos se obtuviera no solo información sino programas de verdaderos actos jurídicos tales como (sentencias, certificaciones, etc.) y así es como nace la Informática Jurídica de Gestión.

En base a lo anterior se da una clasificación:

a) Informática Jurídica Documentaria (consiste en el almacenamiento y recuperación de textos jurídicos).
b) Informática Jurídica de Control y Gestión (consiste en el desarrollo de actividades jurídico-adjetivas).
c) Sistemas Expertos Legales o Informática Jurídica Metadocumentaria (Consiste en el apoyo en la decisión educación, investigación, redacción y previsión del Derecho). (12)

Ese mismo año se colocaron los ordenamientos legales de Pensylvania en cintas magnéticas, y este sistema fue demostrado el año siguiente ante la American Associaton Boreal of Lawyers. Siendo esta la primera demostración de un sistema legal automatizado de búsqueda de información.

Todo lo antes mencionado en cuanto a la informática jurídica se hace más consistente a la época de los años setenta ya que en 1964 la American Corporation of Data Recovery comercializó sistemas de procesamiento de datos legislativos; mas tarde en 1967, la Ohio Bar Automatizad Research (OBAR), se enfocó a abogados litigantes y consistió en que esta barra de abogados firmara un contrato con la Data Corporation de Datos de Dayton, Ohio, y en donde estos sistemas continuaran hasta 1970 a través de la Mead Data Central, que fue constituida después de la fusión de Data Corporation con Mead Corporation y en 1973 la Mead Data Central comercializó el

sistema LEXIS y hasta nuestro días es el sistema de Informática Jurídica más importante y rentable en el mundo entero.

Esta rama del derecho a pesar de su poco tiempo de existencia, ha rebasado en su desarrollo a varias materias jurídicas; esto es así, en razón de su propia naturaleza que va encaminada a la globalización, hoy no podemos imaginarnos un país sin comunicación esto es, gracias a las grandes tecnologías de hoy día y las que están futuras a desarrollarse.

Resulta importante hablar de la autonomía de esta nueva rama del derecho, consideración que podría controvertirse; sin embargo, la realidad es una, el derecho informático es autónomo y en razón de lo que a continuación se expone.

En primer término, habrá que hacerse el siguiente cuestionamiento ¿Cómo o por qué se considera a una rama del derecho autónoma?

Para que una rama del derecho se le considere como autónoma, es necesario que reúna ciertas características; Según la teoría empleada por Héctor Peñaranda para demostrar que es una disciplina jurídica autónoma, procura probar que se satisfacen cuatro criterios:

LEGISLATIVO.- significa que el derecho familiar empieza a independizarse de la rama civil, en razón de que se elaboran leyes regulatorias de la materia derecho familiar que incluso van a generar la creación de códigos sobre la materia.

CIENTIFICO.- consistente en la bibliografía que existe sobre esta rama.

DIDACTICO.- señala el hecho de que en la enseñanza universitaria, hace referencia al derecho de familia, es decir se imparte la cátedra sobre esta materia fuera del campo civil.

JURISDICCIONAL.- consiste en la existencia de tribunales autónomos enfocados a esta materia. (13)

1. 2. DIFERENCIAS Y SIMILITUDES ENTRE DELITOS INFORMÁTICOS Y DELITOS ELECTRONICOS.

Los conceptos **Informático** y **electrónico**, no son sinónimos como muchos piensan, son conceptos diferentes tanto teóricamente como en la práctica y por tal es necesario hacer una correcta interpretación de la legislación.

ELECTRONICA: Ciencia que estudia dispositivos basados en el movimiento de los electrones libres en el vacío, gases o semiconductores, cuando dichos electrones están sometidos a la acción de campos electromagnéticos. (14)

INFORMÁTICA: Computación.

Computación: Informática, conjunto de disciplinas y técnicas desarrolladas para el tratamiento automático de la información mediante máquinas computadoras (hardware) que funciona con distintos programas (software). (15)

Después de estas definiciones comprendemos que la electrónica es “por medio de” y la informática “en contra de”

Derivado de lo anterior existen:

a) delitos cometidos en contra de equipos electrónicos: Son aquellos en los cuales el receptor físico del daño resulta el equipo electrónico, y

b) delitos cometidos en contra de equipos informáticos; es decir todos los equipos informáticos están constituidos de elementos electrónicos, pero no todos los equipos electrónicos son equipos informáticos; es como hablar de un silogismo, un ejemplo sería una televisión, un radio, etc.

Por lo tanto, todos los equipos que procesan datos, pueden ser utilizados o son medios para cometer delitos que afectan el bien jurídico protegido.

Pero nos preguntaremos ¿Cual es el bien jurídico protegido?

En el caso de los delitos cometidos en contra de equipos electrónicos, en donde el receptor del daño es el aparato o equipo electrónico, se afecta la integridad física de este aparato y el derecho de propiedad del sujeto pasivo ya que constituyen una especie particular y especifica del género de los informáticos que no se incluiría en nuestra legislación penal.

En cambio, el delito cometido por medio de elementos informáticos si es una ilicitud especifica, ya que afecta a bienes jurídicos a proteger tales como el patrimonio, la protección de datos y que se presentan, como lo menciona el Dr. Campoli en su obra Derecho Penal Informático en México, que consiste en una serie de gamas que pasa por daños; un ejemplo claro y preciso son las subastas on line, en donde este tipo de delito si requiere una correcta interpretación penal y toma de conciencia de las autoridades, ya que está determinado el bien jurídico.

Esta serie de gamas o facetas se encuentran protegidas por medio de figuras como el robo, la estafa, las injurias y calumnias, etc., que se encuentran contenidas en el Código Penal Federal.

Por tal existen, delitos que no se encuentran tipificados y que corresponden a bienes jurídicos protegidos como el hacking, consiste en la intromisión de un tercero, a

un equipo de computo o a una página, y por medio de la utilización de código de programación o software específico produce daños que puedan variar de simples agregados no deseados en la misma, pasando por el hurto de información a la completa inutilización del equipo o la página. Estamos en presencia de un delito que afecta un bien jurídico protegido u otros más, es por eso que se requiere una definición de los tipos penales, ya que sólo nos encontramos ante nuevas formas para robar, estafar por medios informáticos pero no son delitos nuevos.

En conclusión podemos mencionar que el género delito informático reconoce dos especies:

a) Delitos informáticos electrónicos.
b) Delitos informáticos no electrónicos.

La violación por la fuerza de un cajero automático no es un delito electrónico, sino que por su tipo, es un delito contra la propiedad por medio del uso de la fuerza física por apoderarse de forma ilegítima de algo ajeno, definido como *robo*.

Pero si en este acto se utilizara una computadora para violar el código de acceso al cajero y de esta forma se sustrajera el dinero por el mismo sistema electrónico, ¿como se tipifica este delito?

Estamos en un caso de un delito electrónico, aunque no se encuentre tipificado y por tal, no puede hablarse de un delito en sentido formal, ya que no encuadra o encaja en los que existen, aunque se produjo un daño a un bien jurídico protegido, ya que es un acto doloso.

Es por eso que en los delitos electrónicos se induce a cualquier sistema sin la autorización del sujeto activo, como el (hacking). Ya que la mayoría de los sistemas electrónicos, de almacenamiento o procesamiento de datos poseen una clave para

ingresar a estos es decir, hablamos de un mecanismo de defensa y por tal al violar esta clave estamos en la presencia de un delito.

Siempre que se hablara de un delito electrónico, éste tiene con el autor una relación dolosa, ya que alguien negligente no puede acceder a los sistemas o mecanismos de defensa en los equipos. (DOLO DIRECTO)

Por lo tanto los delitos electrónicos solo son posibles por dolo y resulta imposible que sean por negligencia. Es por tal que estamos en presencia de un vacío penal ya que no existe la protección de la integridad de los equipos electrónicos y se da la relación entre autor- hecho, como hace mención el Dr. Campoli en su obra Derecho Penal Informático en México al referir que solo se preste la atención a otros elementos o aun a los bienes jurídicos a proteger, en virtud de la velocidad con que las nuevas tecnologías se desarrollan, las cuales permitirán violar intereses legítimos, quedando impunes por falta de previsión especifica.

En conclusión los legisladores definirán los nuevos tipos penales y agregarlos a los que rigen actualmente con el fin de que las nuevas tecnologías no sean los medios comisivos para la realización de los delitos; por ende, se requiere hacer la diferencia entre delitos electrónicos y delitos informáticos, a fin de dar una correcta interpretación de cada una y se legisle en los casos de los delitos electrónicos, ya que los delitos informáticos en su mayoría dependen, para su persecución penal, de la correcta interpretación de la legislación que consiste en usar los términos adecuados. Por tal, los delitos electrónicos no sean perpetrados por medio del uso de la informática.

1. 3. CONCEPTOS DE DELITOS ELECTRÓNICOS Y DELITOS 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 especifica la integridad de los equipos electrónicos y la intimidad de sus propietarios.

Por lo tanto el delito electrónico surge de las nuevas tecnologías aplicadas y tiene como objeto material del delito expresamente a las mismas. Un ejemplo claro es el hacking, ya que en esta conducta se manifiesta la intrusión, la adulteración de identidad informática y los daños producidos por virus.

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 consiguen ser de diverso tipo por medio de la utilización indebida de medios informáticos, un ejemplo las subastas on line, los fraudes electrónicos, transferencia de fondos, etc. (16)

Delitos Informáticos: Actos ilícitos en que se tiene a las computadoras como instrumento o fin. (17)

Delitos Informáticos: Consiste en 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. (18)

Pero en realidad ¿Qué es un delito informático? Es el realizado por personas a través de las computadoras y con fines ilícitos.

La computadora es el blanco para la comisión de la conducta ilícita a realizar; en este caso, el fin del criminal es sustraer la información de la computadora o causar un daño a esta.

1. 4. CARACTERÍSTICAS DE DELITOS INFORMÁTICOS.

Las características de los Delitos Informáticos, como hace mención el autor Julio Téllez Valdez (19): son las siguientes:

- Son conductas delictivas de cuello blanco (white collar crimes), en tanto que solo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
- Son acciones ocupacionales porque muchas veces se realizan cuando el sujeto está en el trabajo.
- Son acciones de oportunidad debido a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas para los afectados y casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.
- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin la necesaria presencia física pueden llegar a cometerse.
- Son muchos los casos y pocas las denuncias, todo ello debido a la falta de regulación jurídica a nivel internacional.
- Son sumamente sofisticados y frecuentes en el ámbito militar.

- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- 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).
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica a nivel internacional.

De todas las características antes mencionadas agregaríamos otras tales como:

- En su gran mayoría dependen, para su persecución penal de la correcta interpretación de la legislación penal.
- La falta de legislación en materia de delitos informáticos.
- El bien jurídico lesionado, no solo es el patrimonio, sino la propiedad y la privacidad.

Al adentrarnos en la consistencia de los delitos informáticos, nos preguntamos ¿Quiénes cometen esta clase de delitos y con qué fines?

La mayor parte la realizan sujetos con un alto índice de conocimientos acerca de la informática con años de estudio y práctica, con una gran capacidad intelectual y desde luego que cuentan con esos medios para lograr sus fines. Es por eso que el bien jurídico protegido en este caso sería la integridad de los sistemas informáticos o electrónicos, ya que son realizados por sujetos capacitados para causar alteraciones a un medio aunque lo que se protege en realidad es la integridad física y la propiedad o bien son personas que debido a su situación laboral tienen ventajas en cuanto a la

comisión de estos delitos y por supuesto son hábiles en el uso de los sistemas de informática.

En el Manual de las Naciones Unidas en la prevención y control de delitos informáticos menciona que el 90% de los delitos cometidos a través de las computadoras fueron empleados de la propia empresa afectada.

El concepto a que hace mención Julio Téllez Váldez en su obra Derecho Informático acerca de que son conductas delictivas de cuello blanco, los estudiosos en la materia las han catalogado como delitos de cuello blanco, término dado por Edwin Sutherland en el año de 1943; este mismo autor señala varias conductas que se consideran como delitos de cuello blanco, aun cuando muchas de estas no estén tipificadas en los ordenamientos jurídicos como delitos. Un ejemplo sería las violaciones a las leyes de patentes, y de derechos de autor, la evasión de impuestos, etc.

Este mismo autor destaca que tanto la definición de delitos informáticos como la de los delitos de cuello blanco no son de acuerdo al interés protegido, como sucede en los demás tipos de delitos, sino conforme al sujeto activo que los comete.

Por último, todo lo antes mencionado se ve afectado de forma nacional e internacional ya que el agresor y la victima estén sujetos a leyes diferentes. (19)

1. 4.1. CLASIFICACIÓN DE DELITOS INFORMÁTICOS.

De igual forma como en las características, nos referiremos a Julio Téllez para la clasificación:

Como **instrumento o como medio:** Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito y son:

- Falsificación de documentos vía computarizada (tarjetas de crédito cheques).
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeación o simulación de delitos convencionales (robo, fraude).
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema con el fin de introducir instrucciones inapropiadas (conocido en el medio como **Método del Caballo de Troya**).
- Acceso no autorizado de programas de cómputo.
- Alteración en el funcionamiento de los sistemas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa (método conocido como la **Técnica de Salami**).
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención de las líneas de comunicación de datos.

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 y son:

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

- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo.

El Dr. Julio Téllez en su obra Derecho Informático, nos da una clasificación enfocada a un criterio formal y materialista, que cuando es como instrumento o medio, se está en una presencia de una conducta desplegada por el sujeto activo del delito tendiente a provocar un daño a un individuo o grupo, o en su patrimonio, y cuando es como fin u objetivo nos encontramos en la situación en donde el sujeto activo despliega una conducta tendiente a provocar un daño a la computadora entendiendo a ésta como una entidad física. (20)

1. 4. 2. TIPOS DE DELITOS INFORMÁTICOS.

Los tipos de delitos informáticos de acuerdo con el Manual de las Naciones Unidas es el siguiente:

Características:

- Manipulación de Datos de Entrada.- Consiste en un tipo de fraude informático conocido también como sustracción de datos; es el más común, ya que es el más fácil de cometer y difícil de descubrir. Este tipo de delito no requiere conocimientos técnicos o informáticos y puede ser ejecutado por cualquier persona que tenga acceso a una base de datos.
- Manipulación de Programas.- En este tipo de delitos el sujeto activo debe poseer una serie de conocimientos técnico informáticos, es difícil de descubrir y consiste

en alterar o modificar programas existentes en el sistema de computadoras o en insertar nuevos programas.

- Manipulación de Datos de Salida.- Se realiza fijando un objetivo al funcionamiento del sistema informático.
- Fraude efectuado por manipulación informática.- Consiste en una técnica especializada que se le denominada técnica del salami, en la que da la apariencia de rodajas finas de transacciones financieras, que se van sacando de una cuenta y se transfieren a otra.

Falsificaciones informáticas:

Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos: son computadoras que pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones de programas o datos computarizados:

Este tipo de delitos comprende la destrucción parcial o modificación total o parcial de los programas informáticos y dentro de estos encontramos:

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. Las técnicas que permiten cometer sabotajes informáticos son:

Virus.- una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Gusanos.- Se fabrica en forma análoga 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. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica.- Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla la bomba.

- Acceso no autorizado a servicios y sistemas informáticos.- Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

  Sin embargo este tipo de delito puede agravarse por las siguientes situaciones:

a) La producción de daños.
b) El fin específico de la intrusión (generalmente con fines económicos o cualquier otro que no corresponda directamente con un simple detrimento patrimonial).
c) La consecución de un resultado especifico.
d) La violación de derechos intelectuales.

- Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

  Reproducción no autorizada de programas informáticos de protección legal.

La reproducción no autorizada de programas informáticos puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. (21)

Otros tipos de delitos informáticos sin pertenecer al Manual de la Organización de las Naciones Unidas la hace Gabriel Campoli, en donde se hace una revisión de los casos más comunes y en donde este propone una creación de nuevos tipos penales.

Es necesario dar unos conceptos básicos, que son de reciente creación en el vocabulario jurídico- informático.

Hack: Hacha, azuela, cuchilla, tajar. To hack (22)

De ahí la relación Hackers donde todos al navegar en Internet lo hemos escuchado y en donde estos se dedican a cortar los equipos informáticos ajenos o en páginas Web, con el fin de introducirse y generar daños que puedan llegar al borrado total de datos del equipo.

Por lo tanto esta clase de acciones no se encuentran definidos en casi ninguna legislación mundial.

Intrusión Informática.- Es la acción de ingresar a un equipo informático ajeno sin la autorización del titular y puede cometerse a través de una red telemática o por la apertura directa del equipo o del disco rígido extraído del mismo. (23)

Este tipo de delito sí requiere de determinado software de aplicación donde permita salir o inutilizar las claves de acceso precisadas por el titular, lo cual implicaría un delito doloso o una acción deliberada.

Hacking.- Es la acción en la cual un tercero, no titular de un equipo o un sitio web determinado, accede al mismo por la utilización de código de programación o software especifico; produce daños que pueden variar de simples agregados no deseados en el mismo, pasando por el hurto de información a la completa inutilización del equipo o la página. (24)

Cracker: Su nombre proviene de la voz inglesa to crack, que significa romper.

Este tipo de delito requiere de conocimientos técnico informático y es por tanto una acción voluntaria del agente que implica una relación dolosa.

Son una versión violenta y refinada del Hacker, que si bien utilizan técnicas del hacking para ingresar sin autorización a equipos o redes ajenas, estos tienen fines más peligrosos; un ejemplo que si bien no ha ocurrido pero sí puede darse, es cuando un cracker que a través de sus conocimientos, el equipo informático apropiado y las herramientas informáticas se introduce en el sistema de control de tráfico aéreo de un aeropuerto internacional con el fin de destruir el sistema de control y planificación o alterar algunas frecuencias o rutas de vuelo o aterrizaje.

Por lo general el cracking puede generar atentados terroristas de alto nivel.

Otra modalidad delictiva que se presenta a diario es una variante del cracking pero sin la acción directa del sujeto activo, como la distribución dolosa de un virus, la cual consiste en crear programas de cómputo sin autorización del usuario e instalarlos y en donde se otorga un grado de impunidad al sujeto activo por el tiempo transcurrido.

Se han presentado casos, en donde el virus por medio de mecanismos de tiempo permanecen varios meses inactivos y en determinada fecha desatan su poder destructivo sin que el usuario lo pueda evitar.

Daño electrónico simple (cracking).- Es la acción en la cual el sujeto activo, luego de introducirse de forma no autorizada en equipo electrónico o página Web ajena, produce algún detrimento patrimonial mediante el menoscabo de la integridad física o lógica de cualquiera de ellos, sin más motivo que la producción misma del daño. (25)

Este tipo de delito se puede agravar ya que lesiona la intimidad y el patrimonio.

Intrusión agravada por la finalidad (hacking económico o agravado por la finalidad).- Es la acción consistente en el acceso no autorizado a un equipo informático

ajeno o una página Web de propiedad de un tercero, por cualquier medio, cuando el sujeto activo lo hiciere a fin de obtener un beneficio económico o de cualquier otro tipo para sí o un tercero.

Este tipo de delito es uno de lo más graves, ya que el sujeto activo ingresa en forma ilegitima a fin de obtener un beneficio económico para sí o para un tercero.

Y por último los siguientes conforman los tipos penales más graves.

Robo electrónico.- Es la acción por la cual el agente se apodera ilegítimamente de bienes o dinero del sujeto pasivo, por medio de la utilización de medios informáticos.

Fraude electrónico.- Es la acción por la cual el sujeto activo modifica o adultera por cualquier medio la información contenida en el equipo o página Web del sujeto pasivo a fin de inducir al mismo a un error en su procesamiento para obtener de ella un beneficio económico para sí o para un tercero. (26)

Si bien es cierto que no se contemplan todas las acciones consideradas como delitos informáticos, sí es urgente y necesario una legislación penal es decir, unificar los tipos penales en delitos informáticos lo más pronto en manera internacional para evitar que se creen situaciones como las que existen, en las que por ausencia de una correcta tipificación penal resulta imposible la extradición o la persecución del delito por razones estrictamente territoriales.

1. 4. 3. SUJETO ACTIVO DEL DELITO INFORMÁTICO.

El tipo penal, es el elemento constitutivo de los delitos electrónicos, que resulta esencial en la mayoría de las legislaciones del mundo a fin de evitar superposiciones y falta de

punibilidad por diferencias en las calificaciones de los posibles actos violatorios de bienes jurídicos que deben ser protegidos.

Así mismo resulta imposible resumir todos los tipos penales a crear y consideramos los más universales como:

Hacking.- Consideramos que es el más dañino y por tal su clasificación incluye varios tipos penales diferenciados en un tipo básico y cuatro categorías de agravados. (27)

Los tipos penales clásicos hacen mención a un bien en particular: honor, propiedad, intimidad, vida, libertad, etc. Por lo tanto el bien que se intenta proteger al penalizar estas acciones no tiene una respuesta tan simple como en los delitos comunes, ya que existen dos bienes vulnerados en forma simultanea por este tipo de acciones: La intimidad.- Consiste en el ingreso de un tercero no autorizado a un equipo informático ajeno. Si el sujeto activo produce alguna anomalía funcional o extrae de forma ilegítima autorización del equipo al cual ingresa, se ve profanada la propiedad, ya que ocasiona un daño; si extrae información produce un detrimento patrimonial sobre el sujeto pasivo aunque éste no pierda la posesión efectiva de la cosa, pues ella permanece de todas formas en su equipo, perro ésta pasa también a poder del sujeto activo. Es por ello que surge la necesidad de la Creación de nuevos tipos penales, para esta clase de acciones jurídicamente reprochables.

Los sujetos del delito no varían con respecto del delito, pero si tienen ciertas peculiaridades que cada uno representa.

Las personas que cometen esta clase de delitos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es,

los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

A través del tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y lo que los diferencia entre sí es la naturaleza de los delitos cometidos es decir, la persona que entra a una base de datos sin intenciones delictivas es diferente a un empleado que desvía fondos de cuentas de clientes o en otro caso, una persona que sin autorización modifique, destruya o provoque pérdidas de información.

1. 4. 4. SUJETO PASIVO DEL DELITO INFORMÁTICO.

Los bienes jurídicos que se pueden afectar mediante el uso de equipos informáticos son:

- El patrimonio
- La Intimidad
- La integridad física y / o Lógica de los equipos de cómputo y/ o páginas Web

Por tal el sujeto pasivo o víctima del delito es aquel en el cual recae la conducta acción que realiza el sujeto activo y en donde en los delitos informáticos varía según el modus operandi. Un ejemplo sería el que manipula datos de salida, en donde el sujeto pasivo sería una institución bancaria.

De acuerdo con los artículos 211bis 2 al 211 bis 5, los sujetos pasivos pueden ser solamente el Estado y las Instituciones Financieras; sin embargo, consideramos que el sujeto pasivo puede ser cualquier persona física o moral que sufra detrimento en su patrimonio o intimidad.

Todo lo antes expuesto nos lleva a la conclusión de la unificación de los tipos penales, a fin de evitar la impunidad.

1. 5. ESTADÍSTICAS SOBRE DELITOS INFORMÁTICOS

Existe una institución que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos a través de las computadoras llamado Instituto de Seguridad de Computadoras (CSI) en los Estados Unidos de Norteamérica que derivado de los resultados de un estudio anual denominado "Estudio de Seguridad y Delitos Informáticos" realizado a un total de 273 Instituciones principalmente grandes corporaciones y gobierno.

Así mismo el Estudio de Seguridad y Delitos Informáticos es dirigido por CSI con la participación Agencia Federal de Investigación (FBI) de San Francisco, División de delitos informáticos. El fin de lo anterior es levantar el nivel de conocimiento de seguridad, así como ayudar a determinar el alcance de los Delitos Informáticos en los Estados Unidos de Norteamérica.

Violaciones a la seguridad informática

Respuestas	PORCENTAJE (%)

No reportaron Violaciones de Seguridad	10%
 Reportaron Violaciones de Seguridad	90%

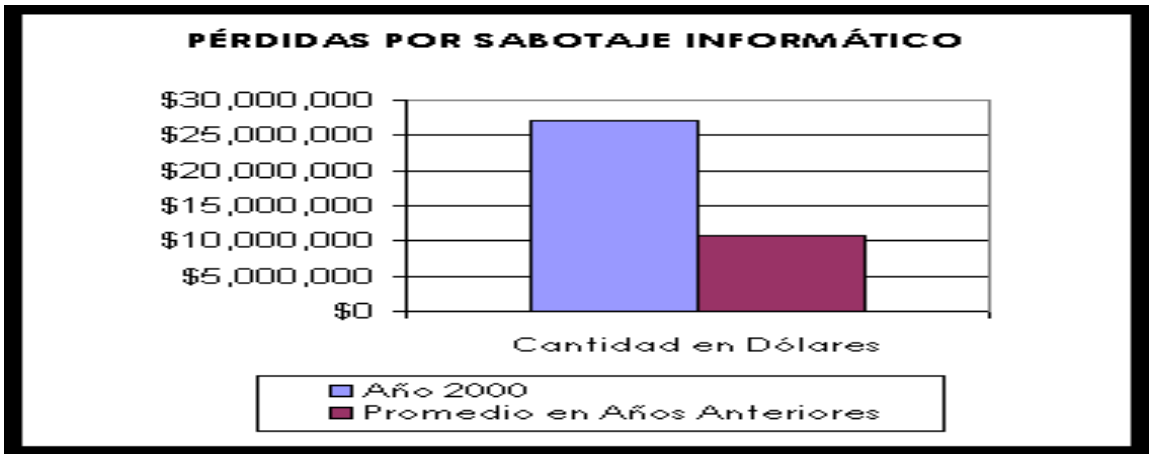
90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.

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

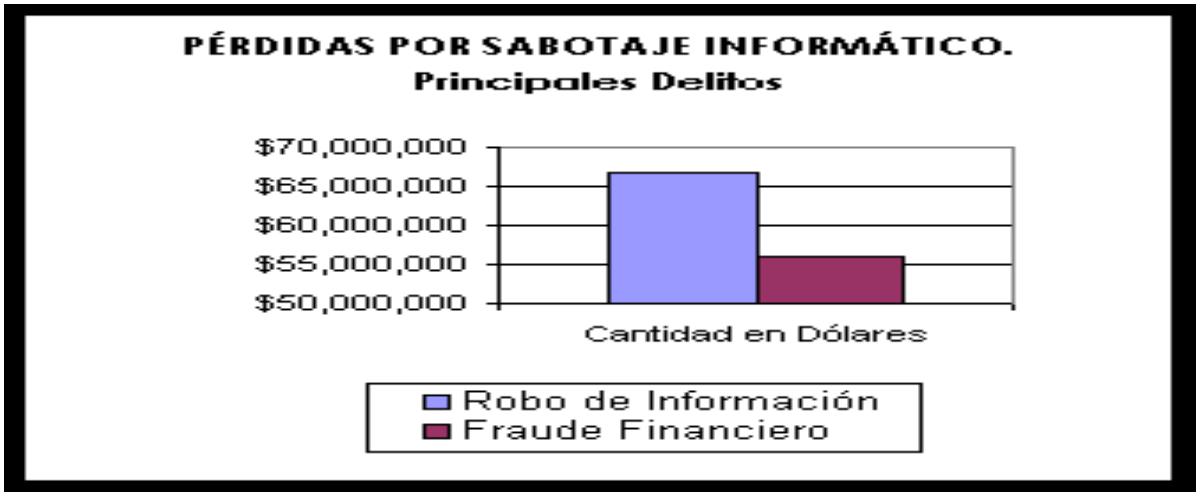
Pérdidas Financieras

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

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



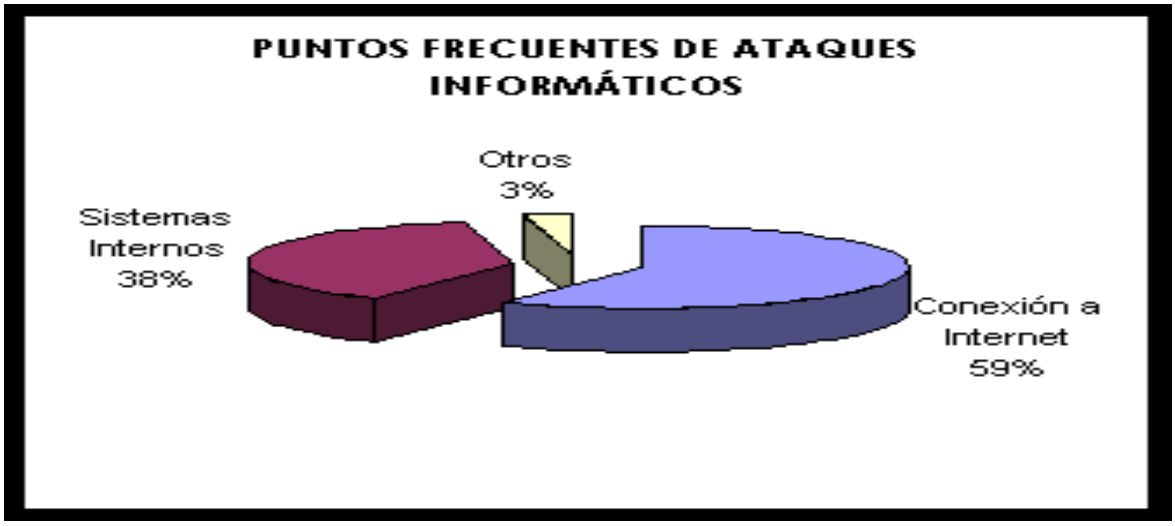
6l encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27,148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10,848,850.



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

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

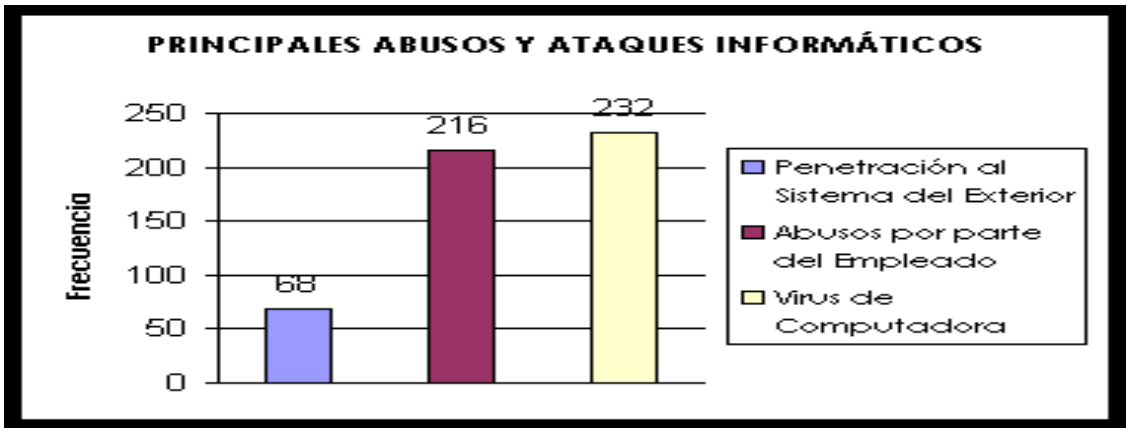
Accesos no autorizados



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

Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del "Estudio de Seguridad y Delitos Informáticos 2000" confirman que la amenaza del crimen por computadoras y otras

violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo.



25% de encuestados descubrieron penetración al sistema del exterior.

79% descubrieron el abuso del empleado por acceso de Internet (por ejemplo, transmitiendo pornografía o pirateó de software, o uso inapropiado de sistemas de correo electrónico).

85% descubrieron virus de computadoras.

Comercio electrónico

Por segundo año, se realizaron una serie de preguntas acerca del comercio electrónico por Internet:

93% de encuestados tienen sitios de www.

43% 19% experimentaron accesos no autorizados o inapropiados en los últimos doce meses.

32% dijeron que ellos no sabían si hubo o no, acceso no autorizado o inapropiado.

35% reconocieron haber tenido ataques, reportando de dos a cinco incidentes.

19% reportaron diez o más incidentes.

64% reconocieron ataques reportados por vandalismo de la Web.

8% reportaron robo de información a través de transacciones.

3% reportaron fraude financiero.

Conclusión sobre el estudio:

Las tendencias que el estudio de CSI/FBI ha resaltado por años son alarmantes. Los "Cyber crímenes" y otros delitos de seguridad de información se han extendido y diversificado. El 90% de los encuestados reportaron ataques. Además, tales incidentes pueden producir serios daños. Las 273 organizaciones que pudieron cuantificar sus pérdidas, informaron un total de $265,589,940. Claramente, la mayoría fueron en condiciones que se apegan a prácticas legítimas, con un despliegue de tecnologías sofisticadas, y lo más importante, por personal adecuado y entrenando, practicantes de seguridad de información en el sector privado y en el gobierno.

Otras estadísticas:

La "línea caliente" de la Internet Watch Foundation (IWF), abierta en diciembre de 1996, ha recibido, principalmente a través del correo electrónico, 781 informes sobre unos 4.300 materiales de Internet considerados ilegales por usuarios de la Red. La mayor parte de los informes enviados a la "línea caliente" (un 85%) se refirieron a pornografía infantil. Otros aludían a fraudes financieros, racismo, mensajes maliciosos y pornografía de adultos.

Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson "Acecho cibernético: delito, represión y responsabilidad personal en el mundo online", publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.

En Singapur el número de delitos cibernéticos detectados en el primer semestre del 2000, en el que se han recibido 127 denuncias, alcanza ya un 68 por ciento del total del año pasado, la policía de Singapur prevé un aumento este año en los delitos por Internet de un 38% con respecto a 1999.

En relación con Internet y la informática, la policía de Singapur estableció en diciembre de 1999 una oficina para investigar las violaciones de los derechos de propiedad y ya ha confiscado copias piratas por valor de 9,4 millones de dólares.

En el Salvador, existe más de un 75% de computadoras que no cuentan con licencias que amparen los programas (software) que utilizan. Esta proporción tan alta ha ocacionado que organismos Internacionales reacciones ante este tipo de delitos tal es el caso de BSA (Bussines Software Alliance) (28)

En el caso de México, tenemos el caso del Instituto Federal Electoral, en el cual por lo menos 58 millones de personas vieron vulnerada su privacidad.

CAPÍTULO 2.- LEGISLACIÓN EN MÉXICO

2. 1. Legislación Informática en México.

El impacto que han tenido los avances tecnológicos sin duda han repercutido en México, pero no podemos decir lo mismo en legislación informática, debido a que varias entidades federativas tratan cuestiones de forma y no de fondo en dicha materia, la diferencia en el ámbito federal es evidente y respecto al tema es mejor en todos sus aspectos, no cabe duda que todo deriva de la falta de interés, del vacío legislativo y por qué no de decir, de la ignorancia.

Si bien es cierto que este no ha sido estudiado como la informática jurídica, no es de menor importancia ya que algunos lo consideran como una categoría propia que se rige por sus propias reglas y que se deriva del fenómeno informático.

La **Legislación Informática** es un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso (fundamentalmente inadecuado) de la informática, es decir, que aquí se trata de una reglamentación de puntos específicos. (1)

La definición y análisis a que hace mención el Dr. Téllez es certera y preocupante, ya que varios términos informáticos que conllevan a delitos informáticos no son incluidos de manera adecuada en nuestra legislación, o bien los legisladores desconocen del tema.

Algunas cuestiones que deberían de incluirse en la legislación son:

Propiedad Intelectual e Informática: Se debe comprender la protección de los programas de cómputo y la regulación de nombres de dominio, ambos derivados de las acciones de piratería. (2)

Regulación jurídica de Internet: Implica favorecer o restringir la circulación de datos a través de las fronteras nacionales. (3)

La regulación del Internet es de suma importancia para México, ya que es una vertiente para el ciber-terrorismo, la pornografía infantil, la venta de drogas, entre otras; Periódico “El Norte” menciona una estadística de suma importancia de las páginas Web patrulladas con los mayores índices delictivos: 43% son ataques a sitios; 23% a ciberterrorismo; 22% a venta de drogas; 5% satánico; 4% a inhibidores de toxinas y el 3% a la venta de armas de fuego.

El total de denuncias por fraude recibidas y atendidas por la policía federal preventiva contra sitios de subastas on-line; Los productos con los que se cometen los fraudes son teléfonos celulares 34%; notebooks 28%; videocámaras y cámaras fotográficas 16%; equipos informáticos 13% y videojuegos 8%.(4)

Sin embargo han surgido varias propuestas de la sociedad civil y de empresas para la autocensura, en donde las compañías que ofrecen portales gratuitos, prohíben la publicación de imágenes pornográficas y el lenguaje no adecuado, con el fin de desarrollar y estructurar la red de manera armónica y equilibrada para que responda a vitales intereses de la sociedad y del hombre actual. (5)

Delitos Informáticos: Se debe sancionar la comisión de verdaderos actos ilícitos en los que se tengan a las computadoras como instrumentos para realizarlos, es decir los delitos cometidos por elementos electrónicos.

Son delitos donde su marco conceptual es “por medio de”; todos los equipos informáticos están construidos con elementos electrónicos, donde el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos, en donde el bien jurídico tutelado debe ser la integridad de los equipos electrónicos y la intimidad de sus propietarios. Un ejemplo claro sería el hacking, ya que este se introduce o altera la identidad informática u ocasiona daños por virus a un equipo ajeno o a un sitio Web.

Por lo tanto, la materia en comento comprende:

- Legislación Federal

Código Civil Federal.- Mediante reforma publicada el 29 de mayo del año 2000, se reformó el Libro Cuarto denominado de las Obligaciones, en su primera parte de las Obligaciones en General, título primero Fuentes de las Obligaciones Capitulo I, en el cual se empiezan a reconocer cuestiones en el cual el derecho informático se incorpora al derecho civil

En lo relativo al Consentimiento, se le da validez a aquel que se presenta a través de medios electrónicos, lo cual demuestra un avance importante del reconocimiento de la utilización de esos medios dentro del derecho civil:

Artículo 1803.- El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:

I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, ***por medios electrónicos, ópticos o por cualquier otra tecnología***, o por signos inequívocos, y

II.- El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente.

De igual forma, se le da validez plena sin la necesidad de contar con otro requisito, a la propuesta y aceptación de un acto acordado o convenido a través de medios electrónicos, para que este surta sus efectos legales:

Artículo 1811.-…

Tratándose de la propuesta y aceptación hechas a través de ***medios electrónicos, ópticos*** o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos.

Por cuanto a la forma y cuando esta requiera ser por escrito, la reforma da la pauta para que a través de medios electrónicos se cumpla con la misma, es decir, cuando se tenga que firmar, las personas a las cuales se imponga esa obligación,

podrá realizarse a través de medios electrónicos; para el caso de que se requiera de fedatario público, las partes podrán realizar el trámite a través de medios electrónicos ante notario, en los cuales señalaran los términos en los cuales se obligan, circunstancia que el fedatario debe hacer constar en el instrumento:

Artículo 1834 bis.- Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de ***medios electrónicos,*** ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesibles para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo su resguardo una versión íntegra de la misma para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.**"**

Código Federal de Procedimientos Civiles

La reforma al Código Federal de Procedimientos Civiles, mismas que encontramos en su Título Cuarto denominado de la Prueba, Capítulo IX de la valuación de la prueba, en sin duda una de las más importantes para el campo del litigio, al reconocer como prueba a la información generada con medios electrónicos:

"Artículo 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las

personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta."

- Legislación Estatal (en algunos casos)
- Legislación sobre Derechos de Autor

Los Derechos de Autor constituyen el reconocimiento del Estado en favor del creador de obras literarias y/o artísticas; en México, están protegidos los programas de cómputo así como las bases de datos que por su composición constituyan obra intelectual. El autor es la persona física que crea una obra; así, la Ley lo protege para estimular su creatividad y asegurar que su trabajo sea recompensado. De igual forma autoriza al usuario legítimo a hacer las copias que le permita la licencia, o bien, una sola que sea indispensable para la utilización del programa o sea destinada sólo para resguardo

Al respecto, el ordenamiento encargado de regular los derechos de autor, es la **Ley Federal del Derecho de Autor**, Publicada en el Diario Oficial de la Federación el 26 de diciembre de 1996, la cual dentro de su Título Segundo denominado del Derecho Autor, encontramos una serie de reglas que se relacionan con el tema a tratar. Siendo una ellas la ***protección de los programas tanto operativos como aplicativos y deja fuera a los que tienen por objeto causar efectos nocivos***

El hardware de una computadoras por si sola no resulta un instrumento útil para el usuario, es por ello que para lograr un optimo resultado, se debe de contar con programas (software) que faciliten la operación del ordenador. Estos programas o paquetes son el resultado del trabajo intelectual de una persona, y esos trabajos merecen ser protegidos para evitar lo que se conoce como robo de ideas. Al respecto el

artículo 13 de la citada ley señala las obras que guardan cierta relación con el derecho informático.

Artículo 13

Los derechos de autor a que se refiere esta Ley se reconocen respecto de las obras de las siguientes ramas:

XI. Programas de cómputo;

XIV. De compilación, integrada por las colecciones de obras, tales como las enciclopedias, las antologías, y de obras u otros elementos como las bases de datos, siempre que dichas colecciones, por su selección o la disposición de su contenido o materias, constituyan una creación intelectual.

Las demás obras que por analogía puedan considerarse obras literarias o artísticas se incluirán en la rama que les sea más afín a su naturaleza.

En el Titulo Quinto Capitulo IV denominado de los Programas de Computación y las Bases de Datos, encontramos la regulación legal en materia de derecho de autor que tienen estos. Como inicio se nos señala la definición de programa de computación, mismo que es la siguiente:

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.

Ahora bien, con base a los artículos subsecuentes se procede a señalar lo más importante:

Los programas de computación se protegen en los mismos términos que las obras literarias. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos

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.

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.

El acceso a información de carácter privado relativa a las personas contenidas 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. Exceptuándose las investigaciones de las autoridades encargadas de la procuración e impartición de justicia.

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.

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.

Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto, 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;

- Legislación sobre Seguridad Informática
- Legislación sobre Protección al Consumidor

Con las reformas a la **Ley Federal de Protección al Consumidor** en el año 2000, se busca la protección del consumidor "electrónico", por lo que con dichas reformas, se pretenden entre otras cosas, que la información del consumidor sea tratada en forma confidencial, que la página Web en la que se publiciten los productos y servicios, cuenten con elementos de seguridad y confidencialidad, se deberán señalar los datos generales de proveedor, el proveedor deberá dar a conocer las condiciones, términos, cargos adicionales, formas de pago y se les prohíbe a los proveedores de llevar a cabo prácticas de mercadotecnia dirigidas a población vulnerable. De igual forma, se establecen las sanciones en caso de contrariar la normatividad aplicable.

CAPITULO VIII BIS DE LOS DERECHOS DE LOS CONSUMIDORES EN LAS TRANSACCIONES EFECTUADAS A TRAVES DEL USO DE MEDIOS ELECTRONICOS, OPTICOS O DE CUALQUIER OTRA TECNOLOGIA

Artículo 76 bis.- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:

El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;

El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;

El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;

El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;

El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;

El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y

El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, y cuidará las prácticas de mercadotecnia dirigidas a población vulnerable, como niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.

Artículo 128.- Las infracciones a lo dispuesto por los artículos……, 76 bis, …. Serán sancionadas con multa por el equivalente de una y hasta dos mil quinientas veces el salario mínimo general vigente para el Distrito Federal. **..."**

- Legislación sobre Competencia
- Legislación sobre Comercio
- Legislación sobre Contratos Informáticos
- Legislación sobre Telecomunicaciones
- Legislación sobre Responsabilidad Civil

- Legislación sobre Protección de Datos

“Con el auge de los sistemas informáticos, se genera un poder informático de dimensiones insospechadas, la capacidad de registro de las computadoras, la rapidez de consulta y de transferencia de datos y la cobertura de toda esa información genera para quien la posee o puede acceder a ella una fuerte dosis de poder, que puede ser tanto de poder económico ("la información se compra y se vende, viaja de un lugar a otro sin que el interesado lo sepa") como poder político (ya que conocer minuciosamente la vida de los demás permite, en buena medida, regular controlar y vigilar su comportamiento)”.

La **Ley Federal de Transparencia y Acceso a la Información Pública** Gubernamental, publicada en el Diario Oficial de la Federación el 11 de junio de 2002, es la encargada de velar por la protección de datos personales en nuestro país.

Los datos personales, es la información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

Los responsables de los datos personales se les denominaran Sujetos Obligados y estos serán:

a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República;

b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos;

c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;

d) Los órganos constitucionales autónomos;

e) Los tribunales administrativos federales, y

f) Cualquier otro órgano federal.

El Título Primero, denominado de las Disposiciones Comunes para los Sujetos Obligados en su Capítulo IV de la Protección de Datos Personales articulo 20, dispone los deberes de los sujetos obligados

Artículo 20

Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;

II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;

IV. Procurar que los datos personales sean exactos y actualizados;

V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y

VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

El artículo 21 del mencionado ordenamiento, establece la prohibición que tienen los sujetos obligados de hacer mal uso de los datos personales y los casos en que si pueden utilizarse los mismos. Así mismo, el artículo 22 señala claramente los casos en

los cuales se pueden hacer uso de los datos personales aún sin el consentimiento de los individuos:

Artículo 21

Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

Artículo 22

No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:

I. Los necesarios para la prevención o el diagnóstico médico, la prestación de asistencia médica o la gestión de servicios de salud y no pueda recabarse su autorización;
II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;
III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
IV. Cuando exista una orden judicial;
V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y
VI. En los demás casos que establezcan las leyes.

Por lo que respecta a los articulo 24, 25 y 26, bien podríamos señalar que se trata del incipiente Habeas Data mexicano, en el cual podemos como gobernados

acudir con el sujeto obligado para que nos proporcione la información que sobre nuestra persona existe en su banco de datos, igualmente se puede solicitar la corrección cuando nuestros datos estén asentados de manera incorrecta y se establece el recurso de revisión cuando la autoridad sea omisa al respecto; es decir, a la solicitud de entrega de datos o a la corrección de los mismos, dentro de los términos señalados en la ley.

Artículo 24

Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27.

Artículo 25

Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación

que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones.

Artículo 26

Contra la negativa de entregar o corregir datos personales, procederá la interposición del recurso a que se refiere el Artículo 50. También procederá en el caso de falta de respuesta en los plazos a que se refieren los artículos 24 y 25.

Cabe señalar que la Legislación Estatal es publicada en, Periódicos Oficiales, Gacetas Oficiales o Boletines Oficiales según la entidad federativa.

2. 2. Legislación sobre delitos informáticos y su situación actual.

Sin duda uno de los campos que en el cual ha tenido una clara influencia el Derecho Informático es el Derecho Penal, esto es así, en virtud de que con el gran avance tecnológico que encontramos en la actualidad también ha traído aparejada un buen número de casos en los cuales el Derecho Penal se encuentra inmiscuido.

La Secretaría de Seguridad Pública mediante la Policía Federal Preventiva, desarrolló en México la primera Unidad de Policía Cibernética, que además de las acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores de edad, como existen en los países desarrollados.

De igual forma, como una medida para combatir delitos cibernéticos en México y proporcionar las condiciones de seguridad para el desarrollo integral de la red Internet, se creó el grupo DC México, que encabeza como secretaría técnica la Policía Federal Preventiva.

DC MEXICO, como instancia de control y apoyado en la participación de las autoridades persecutoras de delitos, se convierte en un canal confiable de enfrentamiento inmediato y con seguimiento de toda denuncia de ilícitos informáticos en

México y en el extranjero donde se afecten los intereses del país. También, es el único punto de contacto oficial con sus contrapartes en los Estados Unidos, en términos de los acuerdos bilaterales con esa nación y los que se propicien con otras entidades internacionales. A través de la Secretaría Técnica, DC México representa a nuestro país en el grupo internacional de respuesta inmediata denominado “24X7”.

2. 2.1. Código Penal Federal.

En México los delitos informáticos están regulados en el Código Penal Federal, en su Título Noveno, en cuanto a la revelación de secretos y el acceso ilícito a sistemas y equipos de informática que a continuación se transcriben:

TITULO NOVENO

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

Capitulo II

Acceso ilícito a sistemas y equipos de informática

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

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

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

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

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

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

Lo antes establecido nace de que la norma penal solo tutela los sistemas o equipos protegidos por sistemas de seguridad, cuestión que nos parece infundada ya que la violación de la propiedad o la privacidad es la misma; se trata de un sistema protegido o de uno sin clave alguna. En conclusión lo que se quiere proteger es el bien jurídico, ya que en nada afecta a la conducta del sujeto activo que exista o no un sistema de seguridad.

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.

ANALISIS

En el caso de los artículos 211 bis 3 y 211 bis 5 en donde el sujeto activo está autorizado para acceder a los sistemas o equipos de informática del Estado o de Instituciones del Sistema Financiero, debemos recalcar que en estos artículos lo que se ha intentado es establecer una agravante sobre el tipo, ya que las acciones típicas son las mismas y la variable son las penas, que han sido cuadruplicadas. Así mismo, el sujeto pasivo sólo serán el Estado o las Instituciones Financieras.

Por los que se refiere al artículo 211 bis 7 se establecerá una agravante para las conductas, cuando el sujeto activo utilice la información para su provecho propio o ajeno. Por lo tanto, el sujeto pasivo puede ser en los casos descritos del 211 bis 2 al 211 bis 5 cualquier persona física o moral.

En conclusión, el Código Penal Federal sólo tutela la propiedad y sin embargo lo que se debe de proteger también es la privacidad, ya que ambos son bienes jurídicos.

2. 2. 2. Código Penal para el Estado de Baja California.

TITULO TERCERO

DELITOS CONTRA LA INVIOLABILIDAD DEL SECRETO

CAPITULO UNICO

REVELACION DEL SECRETO

ARTÍCULO 175.- Fue reformado por Decreto No. 161, publicado en el Periódico Oficial No. 24, de fecha 12 de junio de 1998, Sección I, Tomo CV, expedido por la H. XV Legislatura, siendo Gobernador Constitucional del Estado, el C. Lic. Héctor Terán Terán, 1995- 2001; para quedar vigente como sigue:

ARTICULO 175.- Tipo y punibilidad.- Al que sin consentimiento de quien tenga derecho a otorgarlo revele un secreto, de carácter científico, industrial o comercial, o lo obtenga a través de medios electrónicos o computacionales o se le haya confiado, y obtenga provecho propio o ajeno se le impondrá prisión de uno a tres años y hasta cincuenta días multa; si de la revelación del secreto resulta algún perjuicio para alguien, la pena aumentará hasta una mitad más. Al receptor que se beneficie con la revelación del secreto se le impondrá de uno a tres años de Prisión y hasta cien días multa.

REVELACION DEL SECRETO: Se entiende por revelación de secreto cualquier información propia de una fuente científica, industrial o comercial donde se generó, que sea transmitida a otra persona física o moral ajena a la fuente.

QUERELLA: El delito de revelación de secreto se perseguirá por querella de la persona afectada o de su representante legal.

ANALISIS

Se refiere a la divulgación o como lo Indica el capítulo, a la revelación de secretos que pueden ser de diferentes tipos o que se obtenga a través de medios electrónicos o computacionales y por lo tanto, la pena aumentará hasta una mitad más si de la revelación del secreto resulta algún perjuicio para alguien.

Por lo tanto, los equipos informáticos resultan el blanco del hacking, craking o en presencia del spam, los cuales no se encuentran contemplados en este Código.

2. 3. 3. Código Penal para el Estado de Colima.

TITULO SEGUNDO

DELITO Y DELINCUENTE

CAPITULO I

CONDUCTA O HECHO

(REFORMADO, P.O. 9 DE JULIO DE 1994)

ARTÍCULO 9.- El delito puede ser realizado por acción u omisión.

Cuando el agente lleve a cabo una conducta idónea para producir un resultado, éste le será atribuido, salvo que hubiese sobrevenido en virtud de una causa extraña a su propia conducta.

Responde también del resultado típico producido, el que omite impedirlo, si podía hacerlo de acuerdo con las circunstancias, y si debía jurídicamente evitarlo.

ULTIMA REFORMA DECRETO NO. 402, aprobado el quince de julio de 2006

ARTICULO 10.- Se califican como delitos graves, para todos los efectos legales, por afectar de manera importante valores fundamentales de la sociedad, los siguientes delitos previstos por este Código: REBELIÓN tipificado por el artículo 104; los

supuestos previstos por el artículo 108; FALSEDAD ANTE LA AUTORIDAD establecido por el artículo 117; EVASIÓN DE PRESOS conforme al segundo párrafo del artículo 121; PECULADO tipificado por el artículo 131; DELITOS CONTRA LA SEGURIDAD VIAL Y LOS MEDIOS DE TRANSPORTE establecidos en el segundo párrafo del artículo 145; CORRUPCION DE MENORES en su modalidad de procurar o facilitar de cualquier forma el consumo de algún tipo de estupefaciente, psicotrópico o vegetales que determine la Ley General de Salud, como ilegales, a un menor o de quien no tenga capacidad para comprender el significado del hecho, tipificado por el segundo párrafo del articulo 155; así como en su modalidad de EXPLOTACIÓN PORNOGRÁFICA, prevista por el artículo 157 Bis, segundo párrafo, tratándose de la realización de acto de exhibicionismo corporal lascivo o sexual, con el objeto de videograbarlo, fotografiarlo o exhibirlo mediante anuncio impreso o electrónico;

LENOCINIO del numeral 161; HOMICIDIO tipificado por los artículos 169, 170, 171, 172 tratándose del provocador, y las fracciones II y III del 173; LESIONES conforme los artículos 174 fracciones VI y VII, 175, 176, 177, 178, 179 Y 183; HOMICIDIO Y LESIONES CULPOSAS previstas en el artículo 184 BIS; PRIVACIÓN DE LA LIBERTAD previsto por el artículo 197; SECUESTRO previsto por el artículo 199; VIOLACIÓN en todas sus formas y modalidades que comprenden los artículos 206, 207, 208, 209 Y 210; ROBO respecto de los supuestos del inciso B) del artículo 227; los FRAUDES ESPECÍFICOS previstos en las fracciones III, IV, V Y VI del artículo 234; DAÑOS tipificado por el artículo 238. Igualmente se consideran graves los delitos de Tentativa de Homicidio y Secuestro, así como la Tentativa de Robo previsto por el inciso b) del artículo 227 y la Tentativa de Violación previsto por los artículos 207, 208, 209 Y 210; así como los DELITOS CONTRA EL AMBIENTE, previstos por los artículos 243 en su segundo párrafo y la fracción III del 244. En tratándose de delitos de lesiones, se exceptúa de lo dispuesto por el párrafo anterior los casos previstos en los artículos 175, 176, 177 y 178, cuando las lesiones sean de las señaladas en las fracciones I y II del artículo 174.

(REFORMADO P.O. 28 DIC. 2002)

ARTICULO 157 BIS.- Al que explote a un menor o a quien no tenga capacidad para comprender el significado del hecho, con fines de lucro o para conseguir una satisfacción de cualquier naturaleza, se le impondrá de dos años seis meses a ocho años de prisión y multa hasta por quinientas unidades.

Para los efectos de este artículo se tipifica como explotación de menor o de quien no tenga capacidad para comprender el significado del hecho, el permitir, inducir u obligar al sujeto pasivo, a la practica de la mendicidad, o a realizar acto de exhibicionismo corporal, libidinoso o de naturaleza sexual, con el objeto de videograbarlo o fotografiarlo o exhibirlo mediante cualquier tipo de impreso o medio electrónico.

ANALISIS

Es acertada su legislación ya que considera a los medios electrónicos como elementos comisitos del delito.

2. 3. 4. Código Penal para el Estado de México.

CAPITULO IV

FALSIFICACION Y UTILIZACION INDEBIDA DE TITULOS AL

PORTADOR, DOCUMENTOS DE CREDITO PUBLICO

Y DOCUMENTOS RELATIVOS AL CREDITO

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

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

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

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

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

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

ANALISIS

No cabe duda que los únicos sujetos pasivos afectados son las instituciones financieras, sin mencionar o importar las personas físicas.

CAPITULO IV

FALSIFICACION Y UTILIZACION INDEBIDA DE TITULOS AL PORTADOR, DOCUMENTOS DE CREDITO PÚBLICO Y DOCUMENTOS RELATIVOS AL CREDITO

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

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

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

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

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

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

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

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

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

ANALISIS

Esta orientado solamente a las Instituciones Financieras (personas morales) y por lo tal deja desprotegida a las personas físicas.

2. 3. 6. Código Penal para el Estado de Guanajuato.

CAPÍTULO II

VIOLACIÓN DE CORRESPONDENCIA

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

I.- Abra, intercepte o retenga una comunicación que no le esté dirigida.

II.- Accese, destruya o altere la comunicación o información contenida en equipos de cómputo o sus accesorios u otros análogos.

No se impondrá pena alguna a quienes ejerciendo la patria potestad o la tutela, ejecuten cualquiera de las conductas antes descritas, tratándose de sus hijos menores de edad o de quienes se hallen bajo su guarda.

Se requerirá querella de parte ofendida cuando se trate de ascendientes y descendientes, cónyuges o concubinos, parientes civiles o hermanos.

ANALISIS

Solo se protege la intimidad, y queda desprotegido el patrimonio.

2. 3. 7. Código Penal del Estado de Guerrero

TITULO X

(REFORMADA SU DENOMINACION, P.O. 20 DE ABRIL DE 1999)

DELITOS EN CONTRA DE LAS PERSONAS EN SU PATRIMONIO

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

I.- Se apodere de una cosa propia, si ésta se halla por cualquier título legítimo en poder de otro, y

II.- Aprovechando energía eléctrica, algún fluído, programas computarizados, señales televisivas o de Internet, sin consentimiento de la persona que legalmente pueda disponer y autorizar aquéllas. (REFORMADA, P.O. 20 DE ABRIL DE 1999)

ANALISIS

Solamente se protege el patrimonio, pero no la información; únicamente se contempla el robo como tal.

2. 3. 8. Código Penal para el Estado Libre y Soberano de Jalisco

CAPÍTULO VII

Secuestro

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

I. Al responsable de secuestro se le sancionará con una pena de veinticinco a cuarenta años de prisión y multa por el importe de mil a tres mil días de salario mínimo, y en su caso destitución, e inhabilitación del servidor público para desempeñar otro empleo, comisión o cargo público, cuando:

….

…..

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

ANALISIS

Los términos que manejan son confusos tal como marcada ventaja ¿A qué se refieren los legisladores?

Y por ende carece de sentido.

2. 3. 9. Código Penal para el Estado de Morelos

TÍTULO DÉCIMO SEGUNDO

DELITOS CONTRA LA MORAL PÚBLICA

CAPÍTULO I

ULTRAJES A LA MORAL PÚBLICA

ARTÍCULO *213.- Se aplicará prisión de seis meses a tres años y de trescientos a quinientos días-multa:

I.- Al que ilegalmente fabrique, reproduzca o publique libros, escritos, imágenes u objetos obscenos y al que los exponga, distribuya o haga circular; y

II.- Al que realice exhibiciones públicas obscenas por cualquier medio electrónico, incluyendo Internet, así como las ejecute o haga ejecutar por otro;

En caso de reincidencia, además de las sanciones previstas en este artículo, se ordenará la disolución de la sociedad o empresa.

No se sancionarán las conductas que tengan un fin de investigación o divulgación científica, artística o técnica.

CAPÍTULO III

CORRUPCIÓN DE MENORES E INCAPACES

ARTÍCULO *213 quater.- Al que induzca, procure u obligue a un menor de edad o a quien no tenga la capacidad para comprender el significado del hecho, a realizar actos de exhibicionismo corporal, lascivos o sexuales, de prostitución, de consumo de narcóticos, a tener prácticas sexuales, a la práctica de la ebriedad o a cometer hechos

delictuosos, se le aplicará de cinco a diez años de prisión y de cien a quinientos días-multa. Se duplicará la sanción a la persona que cometa o consienta cualquiera de las conductas descritas, si fuere ascendiente, hermano, hermana, padrastro, madrastra, tutor, tutora o todo aquel que tenga sobre el menor el ejercicio de la patria potestad.

Si además del delito citado resultase cometido otro, se aplicarán las reglas de acumulación.

Al que procure, facilite o induzca por cualquier medio a un menor, o a un incapaz, a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbarlo, fotografiarlo o exhibirlo mediante anuncios impresos o electrónicos, incluyendo la Internet, se le impondrá de seis a quince años de prisión y de cien a quinientos días-multa. Se duplicará la sanción a la persona que cometa o consienta cualquiera de las conductas descritas, si fuere ascendiente, hermano, hermana, padrastro, madrastra, tutor, tutora o todo aquel que tenga sobre el menor el ejercicio de la patria potestad.

Al que filme, grabe o imprima los actos a que se refiere el párrafo anterior, se le impondrá una pena de diez a catorce años de prisión y de doscientos cincuenta a mil días-multa. La misma pena se impondrá a quien con fines de lucro, elabore, reproduzca, venda, arriende, exponga, publicite o difunda el material referido.

ANALISIS

Consideramos que falta la necesidad de nuevos tipos penales para otras conductas delictivas.

2. 4. 1. Código Penal para el Estado de Nuevo León.

TÍTULO VIGÉSIMO SEGUNDO

DE LOS DELITOS POR MEDIOS ELECTRÓNICOS

ARTÍCULO 427.- A QUIEN INDEBIDAMENTE ACCESE A UN SISTEMA DE TRATAMIENTO O DE TRANSMISIÓN AUTOMATIZADO DE DATOS, SE LE IMPONDRÁ DE 2 MESES A 2 AÑOS DE PRISIÓN Y MULTA DE 200 A 1000 CUOTAS.

ARTÍCULO 428.- A QUIEN INDEBIDAMENTE SUPRIMA O MODIFIQUE DATOS CONTENIDOS EN EL SISTEMA, O ALTERE EL FUNCIONAMIENTO DEL SISTEMA DE TRATAMIENTO O DE TRANSMISIÓN AUTOMATIZADO DE DATOS, SE LE IMPONDRÁ DE 2 A 8 AÑOS DE PRISIÓN Y MULTA DE 300 A 1500 CUOTAS.

ARTÍCULO 429.- A QUIEN INDEBIDAMENTE AFECTE O FALSEE EL FUNCIONAMIENTO DE UN SISTEMA DE TRATAMIENTO O DE TRANSMISIÓN AUTOMATIZADA DE DATOS, SE LES IMPONDRÁ DE 2 A 8 AÑOS DE PRISIÓN Y MULTA DE 350 A 2000 CUOTAS.

ANALISIS

Lo antes mencionado no es claro y a la vez confuso en sus términos supuestamente Informáticos; las penas no varían con relación a las multas, que al parecer es lo más importante en cuanto a delitos informáticos.

De igual manera, el sujeto activo corresponde a cualquier persona física y el sujeto pasivo a cualquier persona física o moral.

2. 4. 2. Código Penal para el Estado Libre y Soberano de Puebla

Artículo 245 bis.-Se impondrá prisión de tres a nueve años y multa de ciento cincuenta a cuatrocientos días de salario:

IV.- Al que adquiere, copie o falsifique los medios de identificación electrónica, cintas o dispositivos magnéticos de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo; y

V.- Al que acceda indebidamente a los equipos y sistemas de cómputo o electromagnéticos de las Instituciones emisoras de tarjetas, títulos, documentos o instrumentos, para el pago de bienes y servicios o para disposición de efectivo.

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

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

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

Artículo 246.- Si el infractor fuere funcionario o empleado público, además de las sanciones indicadas, se le destituirá de su empleo o cargo y se le inhabilitará hasta por diez años para obtener cualquier otro.

Artículo 247.- En los supuestos previstos por el artículo 245, si el infractor fuere abogado, se le inhabilitará para el ejercicio de su profesión hasta por doce años y, en su caso, para ejercer la función notarial si fuese Notario.

ANALISIS

Se considera su legislación acertada ya que maneja meramente lenguaje informático.

2. 4. 3. Código Penal para el Estado Libre y Soberano de Quintana Roo

ADICIONADO P.O. 29 DIC. 2000.

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

I. Produzca, imprima, enajena aún gratuitamente, distribuya o altere tarjetas, títulos, documentos o instrumentos utilizados para el pago de bienes o servicios o para disposición en efectivo, sin consentimiento de quien esté facultado para ello.

II. Adquiera, posea o detente ilícitamente tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo a sabiendas que son alterados o falsificados.

III. Copie o reproduzca, altere los medios de identificación electrónica, cintas o dispositivos magnéticos de documentos para el pago de bienes o servicios o para disposición en efectivo.

IV. Accese indebidamente los equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

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

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

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

ANALISIS

Consideramos que solo trata el sujeto pasivo como institución financiera, desprotegiendo a cualquier persona física que sufra detrimento.

2. 4. 4. Código Penal para el Estado de Sinaloa.

CAPÍTULO V

DELITO INFORMÁTICO

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

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

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

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

ANALISIS

Las penas no son agravadas, varían de 6 meses a 2 años y esto ayuda a la impunidad.

El sujeto activo corresponde a cualquier persona física, y el sujeto pasivo a cualquier persona física o moral.

No es claro en sus definiciones el Código Penal de Sinaloa, ya que se utilizan los términos dañar o destruir, cuando la correcta redacción hubiese sido provoque daño total o parcial si lo que se buscaba 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. (5)

Por otra parte, debe tenerse en cuenta el significado literal e interpretativo de interceptar e interferir, ya que la interceptación nace de una necesaria interferencia, con lo cual si lo que se que se deseaba era proteger contra la simple interferencia sin que el sujeto activo tome conocimiento del contenido del mensaje (acto que si puede ser incluido en el vocablo interceptar) (6)

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 quien reciba sin haber interceptado también queda incluido en el tipo. (7)

2. 4. 5. Código Penal para el Estado de Tabasco

CAPITULO V

VIOLACION DE LA COMUNICACION PRIVADA

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

ANALISIS

No protege las conductas que se consideran en los delitos informáticos; no basta con considerar solamente la intervención.

2. 3. 6. Código Penal para el Estado de Tamaulipas.

CAPÍTULO II

ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

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

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

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

ARTÍCULO 207-QUINQUIES.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente modifique, destruya o provoque pérdida de información que contengan se impondrá una sanción de tres a ocho años de prisión y multa de trescientos a ochocientos días salario.

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

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

ANALISIS

El Código Penal para el Estado de Tamaulipas en cuanto a delitos informáticos, es semejante al Código Penal Federal, al establecer una agravante sobre el tipo, ya que las acciones típicas son las mismas y la variable son las penas. Así mismo, el sujeto pasivo solo será el Estado o las Instituciones Financieras.

2. 4. 7. Código Penal para el Estado de Yucatán

CAPÍTULO II

Corrupción de Menores e Incapaces, Trata de

Menores y Pornografía Infantil

Artículo 211.- Al que procure o facilite por cualquier medio que uno o más menores de dieciséis años, con o sin su consentimiento, los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de cuatrocientos a quinientos días-multa.

ANALISIS

Consideramos que es incompleta, pues no abarca todos los delitos informáticos.

2. 4. 8. Código Penal para el Estado de Zacatecas

CAPITULO II

CORRUPCION DE MENORES

ARTICULO 183 Bis.- También cometen el delito de corrupción de menores y se harán acreedores a las sanciones previstas:

I Quienes vendan o alquilen a menores de edad, material audiovisual clasificado como exclusivo para adultos;

II Quienes propicien o permitan que menores de dieciocho años presencien, por medio de aparatos electrónicos la exhibición de las cintas de vídeo a que se refiere la fracción anterior.

ANALISIS

Consideramos que es incompleta, pues no abarca todos los delitos informáticos.

2. 4. 9. Código Penal para el Distrito Federal

TÍTULO VIGÉSIMO CUARTO

DELITOS CONTRA LA FE PÚBLICA

CAPÍTULO I

PRODUCCIÓN, IMPRESIÓN, ENAJENACIÓN, DISTRIBUCIÓN, ALTERACIÓN O FALSIFICACIÓN DE TÍTULOS AL PORTADOR, DOCUMENTOS DE CRÉDITO PÚBLICOS O VALES DE CANJE

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

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

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

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

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

Artículo 346.- Se le impondrán de 2 a 6 años de prisión y de 1,000 a 5,000 días multa, a quien ilícitamente:

I. Emita gases o partículas sólidas o líquidas a la atmósfera, provenientes de fuentes fijas ubicadas en el Distrito Federal o de fuentes móviles que circulan en el Distrito Federal;

II. Descargue, deposite o infiltre aguas residuales, residuos sólidos o industriales no peligrosos, líquidos químicos o bioquímicos;

III. Descargue, deposite o infiltre residuos sólidos, líquidos o industriales de manejo especial, conforme a lo previsto en las disposiciones jurídicas aplicables en el Distrito Federal;

IV. Genere emisiones de energía térmica o lumínica, olores, ruidos o vibraciones, provenientes de fuentes fijas ubicadas en el Distrito Federal o de fuentes móviles que circulan en el Distrito Federal;

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, independientemente de que los recursos no salgan de la institución; o

….

ANALISIS

Consideramos que esta incompleta, no abarca todos los delitos informáticos. así mismo solo comprende delitos que vulneran el sistema financiero.

2. 5. 1. Código Penal para el Estado Libre y Soberano de Veracruz de Ignacio de la Llave.

CAPÍTULO III

DELITOS INFORMÁTICOS

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

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

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

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

ANALISIS

El sujeto activo puede resultar cualquier persona, y el sujeto pasivo cualquier persona física o moral, como sucede casi en todos los Códigos.

De igual forma no es claro en sus términos tal como sucede con el concepto de soporte lógico ¿Qué entendemos por éste concepto?

Por otro lado no se hace mención en cuanto a instituciones financieras o al estado y todas las definiciones no tienen un fin.

2. 5. 2. Ley de Protección de Datos Personales del Estado de Colima.

ANALISIS

La presente Ley será aplicable a los datos de carácter personal que sean registrados en cualquier soporte físico que permita su tratamiento, tanto por parte del sector público como privado dentro del Estado.

En nuestra Carta Magna no se contempla en las garantías individuales la protección de datos personales, la cual es de suma importancia como las existentes, ya

que la protección de datos personales sobre la familia, posesiones, documentos y en cuestión penal, la violación de correspondencia, revelación de secretos, o el uso ilícito de las computadoras está totalmente desprotegidá; sin embargo, la legislación nacional existente como la Ley de Información Estadística y Geográfica, y su Reglamento, la Ley Federal de Transparencia y Acceso Gubernamental y otros Ordenamientos Jurídicos existentes son suficientes para regular de manera adecuada y ordenada la materia de datos personales.

2. 5. 3. Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios.

ANALISIS

La presente tiene por objeto agilizar, accesibilizar y simplificar los actos, convenios, comunicaciones, procedimientos administrativos, trámites y la prestación de servicios públicos que corresponden al Poder Ejecutivo, al Poder Legislativo, al Poder Judicial, a los Organismos Autónomos, a los Ayuntamientos y a las dependencias y entidades de la administración pública estatal o municipal, promoviendo y fomentando el uso de medios electrónicos en las relaciones entre el Poder Ejecutivo, el Poder Legislativo, el Poder Judicial, los Organismos Autónomos, los Ayuntamientos y cualquier dependencia o entidad de la administración pública estatal o municipal, y entre éstos y los particulares; y el uso de la firma electrónica certificada, su eficacia jurídica y la prestación de servicios de certificación relacionados con la misma.

2. 5. 4. Lineamientos de Protección de Datos Personales.

ANALISIS

El anterior ordenamiento fue publicado en el Diario Oficial de la Federación el 30 de septiembre de 2005, con el propósito de establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la administración pública federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado

tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.

Por lo tanto, los lineamientos establecen las condiciones y requisitos mínimos para el debido manejo y custodia de los sistemas de datos que se encuentren en posesión de la administración pública federal en el ejercicio de sus atribuciones.

Como mencionamos anteriormente, la legislación nacional existente sobre datos personales no es suficiente para regular este desorden en cuestión de datos personales, el cual se requiere llevar a rango constitucional.

2. 5. 5. Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico.

ANALISIS

El fin de la Comisión es promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones, mediante la adecuada coordinación de las acciones que al efecto proponga la Secretaría de la Función Pública, con las dependencias de la administración pública federal y, a través de éstas, con las entidades paraestatales.

El avance tecnológico en el uso de la información y comunicación ha transformado la relación entre el Gobierno y los ciudadanos por lo que se crea el gobierno digital.

El gobierno digital es un plan de políticas públicas en el que el fin son las relaciones eficientes entre los elementos de esté: Gobierno, empresas y ciudadanos; así se crea un espacio informático, de modo que todos los sectores de la población puedan acceder a los datos que necesitan tales como trámites y servicios en línea, temas de gobierno, foros de gobierno, temas acerca del financiamiento a los tres niveles de gobierno, consulta del Diario Oficial de la Federación, búsqueda de trabajo, consulta de disposiciones jurídicas, rendición de cuentas, registro de avisos de testamentos Registro Nacional de Avisos de Testamentos (RENAT), entre otras.

2. 6. Crimen Organizado.

La delincuencia organizada cuenta con lo más avanzado en cuestión tecnológica y que por ende, es capaz de desafiar a los gobiernos que no han actualizado su legislación, ajustándose a las transformaciones que se han establecido en materia informática a la vida pública de los ciudadanos, a los estados y las organizaciones. Por lo tanto, nos conlleva a la ciber-delincuencia organizada.

El narcotráfico consiste en la transmisión de fórmulas para la fabricación de estupefacientes, para el lavado de dinero y la coordinación de entrega y recepción de drogas. (8)

Así los narcotraficantes usan Internet para delitos tales como el lavado de dinero, venta de droga, tráfico de armas, proselitismo de sectas, etc. (9)

2. 6. 1. Delincuencia en Internet.

El Internet llega a México en 1987 y en 1992 surge una organización de instituciones académicas llamado Mexnet, A.C; donde ésta promovía el desarrollo del internet mexicano, estableciendo un backbone nacional donde a través de la difusión de cultura de redes se pretendía la conexión a nivel mundial y donde actualmente este backbone cuenta con dos salidas internacionales.

La delincuencia en Internet comprende varios delitos y los que realizan estos son conocidos como cyberdelincuentes. Algunos de los tantos delitos cometidos en Internet y que tan solo enumeraremos, ya que son explicados en el anterior capítulo son:

- Fraudes cibernéticos (subastas on line)
- Pornografía Infantil
- Spam (Envío masivo de correos electrónicos con el fin de bloquear un sistema)
- Cyberterrorismo (mensajes anónimos por un cierto grupo de terroristas para remitirse consignas y planes de actuación internacional)

- Espionaje (acceso no autorizado a sistemas informáticos gubernamentales y empresas a intervención de cuentas de correos)

Uno de los principales problemas que afrontamos es la cuestión de la regulación del Internet para los menores infractores, ya que no existe un sistema penal que contemple la situación jurídica de los menores ante los delitos informáticos.

Por otro lado también nos encontramos en la situación internacional, en donde no existe una norma internacional de unificación de criterios en materia de delitos informáticos, ya que para cada sistema jurídico la edad punible es diferente. Por lo tanto, la actividad en la red que violan los derechos de terceros es cometida por menores que oscilan entre los 15 a 16 años de edad.

CAPÍTULO 3.- ANÁLISIS DESCRIPTIVO DE LA SITUACIÓN INSTITUCIONAL

3. 1. Análisis del Reglamento Interior de la Ley Orgánica de la Procuraduría General de la República

El Reglamento Interior de la Ley Orgánica de la Procuraduría General de la República fue publicado en el Diario Oficial de la Federación el 25 de junio de 2003 sin contemplación de reforma alguna.

Por lo tanto, el citado ordenamiento tiene por objeto establecer la organización y funcionamiento de la Procuraduría General de la República, para el despacho de los asuntos que la Constitución Política de los Estados Unidos Mexicanos, su Ley Orgánica y otros ordenamientos le encomiendan a la Institución, al Procurador y al Ministerio Público de la Federación; así mismo para el cumplimiento de los asuntos de la competencia de la Procuraduría, de su Titular y del Ministerio Público de la Federación. Cuenta con unidades administrativas y órganos desconcentrados, por lo que se justifica la necesidad de crear la Unidad Especializada en Investigación de Delitos Informáticos.

El citado ordenamiento en base a su **artículo 2** cuenta con:

- 5 Subprocuradurías
- Fiscalía Especializada para la Atención de Delitos Electorales;
- Oficialía Mayor;
- Visitaduría General;
- Agencia Federal de Investigación;
- 3 Coordinaciónes

- *10 Unidades Especializadas en Investigación:*

Unidad Especializada en Investigación de Delitos contra la Salud;

Unidad Especializada en Investigación de Terrorismo, Acopio y Tráfico de Armas;

Unidad Especializada en Investigación de Operaciones con Recursos de Procedencia Ilícita y de Falsificación o Alteración de Moneda;

Unidad Especializada en Investigación de Secuestros;

Unidad Especializada en Investigación de Tráfico de Menores, Indocumentados y Órganos;

Unidad Especializada en Investigación de Asalto y Robo de Vehículos;

Unidad Especializada en Investigación de Delitos contra los Derechos de Autor y la Propiedad Industrial;

Unidad Especializada en Investigación de Delitos Fiscales y Financieros;

Unidad Especializada en Investigación de Delitos Cometidos por Servidores Públicos y contra la Administración de Justicia;

Unidad Especializada en Investigación de Delitos contra el Ambiente y Previstos en Leyes Especiales;

- Unidad de Operaciones;
- 42 Direcciones Generales

- Órganos Desconcentrados:
- Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia;
- Centro de Evaluación y Desarrollo Humano;
- Instituto de Capacitación y Profesionalización en Procuración de Justicia Federal;
- Delegaciones, y
- Agregadurías.

De conformidad con su **artículo 3** se entiende por:

I. Agencia: La Agencia Federal de Investigación;

II. Agregadurías: Las Agregadurías de la Procuraduría General de la República en el extranjero;

III. Consejo: El Consejo de Profesionalización a que se refiere la Ley Orgánica de la Procuraduría General de la República;

IV. Delegaciones: Las Delegaciones de la Procuraduría General de la República en las entidades federativas;

V. Ley Orgánica: La Ley Orgánica de la Procuraduría General de la República;

VI. Policía: Policía Federal Investigadora;

VII. Procuraduría: La Procuraduría General de la República;

VIII. Procurador: El Procurador General de la República, y

IX. Servicio de Carrera: El Servicio de Carrera de Procuración de Justicia Federal.

Conforme a su **artículo 4** son Agentes del Ministerio público de la Federación:

I. El Procurador;

II. Los Subprocuradores;

III. El Fiscal Especializado para la Atención de Delitos Electorales;

IV. El Visitador General;

V. El Titular de la Coordinación de Asuntos Internacionales y Agregadurías;

VI. El Titular de la Coordinación General de Delegaciones;

VII. Los Titulares de las Unidades Especializadas;

VIII. Los Directores Generales:

a) De Asuntos Jurídicos;

b) De Constitucionalidad;

c) De Normatividad;

d) De Extradiciones y Asistencia Jurídica;

e) De Control de Averiguaciones Previas;

f) De Control de Procesos Penales Federales;

g) De Amparo;

h) De Atención a Recomendaciones y Amigables Conciliaciones en Derechos Humanos;

i) Jurídico en Materia de Delitos Electorales;

j) De Averiguaciones Previas en Materia de Delitos Electorales;

k) De Control de Procesos y Amparo en Materia de Delitos Electorales;

l) De Visitaduría;

m) De Inspección Interna;

n) De Supervisión e Inspección Interna para la Agencia Federal de Investigación, y

ñ) De Delitos Cometidos por Servidores Públicos de la Institución,

IX. Los titulares de las Delegaciones, y

X. Aquellos servidores públicos a los que el Procurador confiera dicha calidad mediante Acuerdo.

ANALISIS

Conforme al artículo 89, fracción I, de la Constitución Política de los Estados Unidos Mexicanos, de las facultades y obligaciones del Presidente para promulgar y ejecutar las Leyes que expida el Congreso de la Unión; y con fundamento en el artículo 1.- donde se tiene por objeto organizar la Procuraduría General de la República, ubicada en el ámbito del Poder Ejecutivo Federal para el despacho de los asuntos que al Ministerio Público de la Federación y al Procurador General de la República donde la certeza, legalidad, objetividad, imparcialidad y profesionalismo serán principios rectores en el ejercicio de las funciones y acciones en materia de procuración de justicia; artículo 2.- donde al frente de la Procuraduría General de la República estará el Procurador General de la República, quien presidirá al Ministerio Público de la Federación; artículo 6.- de las atribuciones del Procurador General de la República, en su fracción VI donde se somete a consideración del Ejecutivo Federal el proyecto de Reglamento de la Ley en comento; así como el de las reformas al mismo, que juzgue necesarias; artículo 10.- donde los asuntos que competen a la Procuraduría General de la República y al Ministerio Público de la Federación conforme a la Constitución Política de los Estados Unidos Mexicanos el Procurador General de la República se auxiliará de Subprocuradores; Oficial Mayor; Visitador General; Coordinadores; Titulares de Unidades Especializadas; Directores Generales; Delegados; Agregados; Agentes del Ministerio Público de la Federación, agentes de la policía federal investigadora y peritos, y Directores, Subdirectores, Subagregados, jefes de departamento, titulares de órganos y unidades técnicos y administrativos, centrales y desconcentrados, y demás servidores públicos que establezca el Reglamento Interior de la Ley Orgánica de la

Procuraduría General de la República; artículo11.- del desarrollo de las funciones de la Procuraduría General de la República y del Ministerio Público de la Federación, donde se contará con un sistema de especialización y desconcentración territorial y funcional sujeto a bases generales; y artículo 13.- de la Ley Orgánica de la Procuraduría General de la República, el Reglamento Interior de la Ley Orgánica de la Procuraduría General de la República establecerá las unidades y órganos técnicos y administrativos, centrales y desconcentrados, de la Procuraduría General de la República, así como sus atribuciones. El Procurador General de la República, de conformidad con las disposiciones presupuestales, podrá crear unidades administrativas especializadas distintas a las previstas en el Reglamento, para la investigación y persecución de géneros de delitos, atendiendo a las necesidades del servicio, así como fiscalías especiales para el conocimiento, atención y persecución de delitos específicos que por su trascendencia, interés y características así lo ameriten; y de la Ley Orgánica de la Administración Pública Federal, artículo 27, fracción II. A la Secretaría de Gobernación corresponde el despacho de publicar las leyes y decretos del Congreso de la Unión, alguna de las dos Cámaras o la Comisión Permanente y los reglamentos que expida el Presidente de la República, en términos de lo dispuesto en la fracción primera del artículo 89 constitucional, así como las resoluciones y disposiciones que por ley deban publicarse en el Diario Oficial de la Federación.

Justificación de la Unidad Especializada en Investigación en delitos informáticos conforme a las atribuciones del Procurador General de la República

Para la implementación de una Unidad Especializada en Investigación en materia de Delitos Informáticos, el surgimiento de ésta es meramente exclusiva del Procurador General de la República, por lo que se fundamenta la cuestión a tratar:

De acuerdo con el *artículo 13 de la Ley Orgánica de la Procuraduría General de la República*, el Procurador General de la República, conforme a las disposiciones presupuéstales, podrá **crear unidades administrativas especializadas** distintas a las previstas en el Reglamento de esta Ley, para la investigación y persecución de géneros de delitos, atendiendo a las necesidades del servicio, así como fiscalías especiales para el conocimiento, atención y persecución de delitos específicos que por su trascendencia, interés y características así lo ameriten.

Así mismo el *artículo 14 de la Ley* en cuestión, el Procurador General de la República podrá adscribir orgánicamente las unidades y órganos técnicos y administrativos que establezca el Reglamento de esta Ley y demás disposiciones aplicables; de igual forma conforme al *artículo 15 de la Ley Orgánica de la Procuraduría General de la República*, los acuerdos por los cuales se disponga la **creación de unidades administrativas especializadas** y fiscalías especiales, se deleguen facultades o se adscriban los órganos y unidades, se publicarán en el Diario Oficial de la Federación y conforme al *artículo 11 fracción II del Reglamento Ley Orgánica de la Procuraduría General de la República,* el Procurador podrá nombrar a los coordinadores, **titulares de las unidades especializadas**, jefes de unidad, directores generales, delegados, agregados y fiscales especiales, a excepción del Fiscal Especializado para la Atención de Delitos Electorales, quien será nombrado en términos de lo previsto en el artículo 17 de la Ley Orgánica.

Así mismo, el artículo 5 del *Reglamento Ley Orgánica de la Procuraduría General de la República,* refiere que el Procurador determinará la organización y funcionamiento de la Procuraduría, la adscripción de sus unidades subalternas y órganos técnicos, así como la modificación de las áreas y sus atribuciones, en la medida en que lo requiera el servicio. El Procurador podrá fijar o delegar facultades a los servidores públicos de la Institución, según sea el caso, mediante disposiciones de carácter general o especial, sin perder por ello la posibilidad del ejercicio directo y expedirá acuerdos, circulares, instructivos, manuales de organización, de procedimientos y de servicios al público, necesarios para el mejor funcionamiento de la Institución y, en su caso, ordenará su publicación.

Estructura de la Unidad Especializada en Investigación en Delitos Informáticos

La Unidad Especializada en Investigación de delitos informáticos contará con un titular que en su defecto es el Ministerio Público, el cual conforme al artículo 4 del Reglamento de la Ley Orgánica de la Procuraduría General de la República deberá contar con título y cédula profesional de licenciado en Derecho, y no será considerado miembro del Servicio de Carrera conforme lo establece el artículo 4 fracción X, párrafo I del Reglamento de la Ley Orgánica de la Procuraduría General de la República y de igual forma deberá reunir lo siguiente de conformidad con el artículo 8 del Reglamento en cuestión:

I. Ser ciudadano mexicano por nacimiento y en los casos en que la Ley lo requiera, no adquirir otra nacionalidad;

II. Tener cuando menos treinta y cinco años cumplidos el día de la designación;

III. Contar con título y cédula profesional de Licenciado en Derecho, con ejercicio profesional de diez años, contados a partir de la expedición de la cédula;

IV. Gozar de buena reputación, y

V. No haber sido condenado por delito doloso.

De igual manera se auxiliara de:

a) La policía federal investigadora, y

b) Los servicios periciales.

II. Suplementarios:

a) La Policía Federal Preventiva;

b) Los agentes del Ministerio Público del fuero común, de las policías en el Distrito Federal, en los Estados integrantes de la Federación y en los Municipios, así como los peritos, en las instituciones de procuración de justicia de las entidades federativas, en términos de las disposiciones legales aplicables y los acuerdos respectivos;

c) El personal del Servicio Exterior Mexicano acreditado en el extranjero;

d) Los capitanes, patrones o encargados de naves o aeronaves nacionales, y

e) Los funcionarios de las entidades y dependencias de la Administración Pública Federal, en términos de las disposiciones aplicables.

Así mismo el titular de la unidad deberá de capacitarse en materia de delitos informáticos y el personal a su cargo con el fin de aconsejar a las victimas y garantizar sus derechos.

Obligaciones y Atribuciones del personal de la Unidad Especializada en Investigación en Delitos Informáticos

De conformidad con el artículo 4 de la Ley Orgánica de la Procuraduría General de la República, al frente de cada Unidad Especializada habrá un titular (Ministerio Público); donde ejercerá las siguientes atribuciones y trabajará en coordinación con las unidades administrativas y órganos competentes.

I. Investigar y perseguir los delitos del orden federal. El ejercicio de esta atribución comprende:

A) En la averiguación previa:

a) Recibir denuncias o querellas sobre acciones u omisiones que puedan constituir delito;

b) Investigar los delitos del orden federal, así como los delitos del fuero común respecto de los cuales ejercite la facultad de atracción, conforme a las normas aplicables con la ayuda de los auxiliares a que se refiere el artículo 20 de esta Ley Orgánica de la Procuraduría General de la República, y otras autoridades, tanto federales como del Distrito Federal y de los Estados integrantes de la Federación, en los términos de las disposiciones aplicables y de los convenios de colaboración e instrumentos que al efecto se celebren;

c) Practicar las diligencias necesarias para la acreditación del cuerpo del delito y la probable responsabilidad del indiciado, así como para la reparación de los daños y perjuicios causados;

d) Ordenar la detención y, en su caso, retener a los probables responsables de la comisión de delitos, en los términos previstos por el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;

e) Realizar el aseguramiento de bienes de conformidad con las disposiciones aplicables;

f) Restituir provisionalmente al ofendido en el goce de sus derechos, en los términos del Código Federal de Procedimientos Penales y demás disposiciones aplicables;

g) Conceder la libertad provisional a los indiciados en los términos previstos por el artículo 20, apartado A, fracción I y último párrafo, de la Constitución Política de los Estados Unidos Mexicanos;

h) Solicitar al órgano jurisdiccional las órdenes de cateo, las medidas precautorias de arraigo, el aseguramiento o el embargo precautorio de bienes que resulten indispensables para los fines de la averiguación previa, así como, en su caso y oportunidad, para el debido cumplimiento de la sentencia que se dicte;

i) En aquellos casos en que la ley lo permita, el Ministerio Público de la Federación propiciará conciliar los intereses en conflicto, proponiendo vías de solución que logren la avenencia;

j) Determinar la incompetencia y remitir el asunto a la autoridad que deba conocer, así como la acumulación de las averiguaciones previas cuando sea procedente;

k) Determinar la reserva de la averiguación previa, conforme a las disposiciones aplicables;

l) Determinar el no ejercicio de la acción penal, cuando:

1. Los hechos de que conozca no sean constitutivos de delito;

2. Una vez agotadas todas las diligencias y los medios de prueba correspondientes, no se acredite el cuerpo del delito o la probable responsabilidad del indiciado;

3. La acción penal se hubiese extinguido en los términos de las normas aplicables;

4. De las diligencias practicadas se desprenda plenamente la existencia de una causa de exclusión del delito, en los términos que establecen las normas aplicables;

5. Resulte imposible la prueba de la existencia de los hechos constitutivos de delito por obstáculo material insuperable, y

6. En los demás casos que determinen las normas aplicables.

m) Poner a disposición de la autoridad competente a los menores de edad que hubieren incurrido en acciones u omisiones correspondientes a ilícitos tipificados por las leyes penales federales;

n) Poner a los inimputables mayores de edad a disposición del órgano jurisdiccional, cuando se deban aplicar medidas de seguridad, ejerciendo las acciones correspondientes en los términos establecidos en las normas aplicables, y

ñ) Las demás que determinen las normas aplicables.

Cuando el Ministerio Público de la Federación tenga conocimiento por sí o por conducto de sus auxiliares de la probable comisión de un delito cuya persecución dependa de querella o de cualquier otro acto equivalente, que deba formular alguna autoridad, lo comunicará por escrito y de inmediato a la autoridad competente, a fin de que resuelva con el debido conocimiento de los hechos lo que a sus facultades o atribuciones corresponda. Las autoridades harán saber por escrito al Ministerio Público de la Federación la determinación que adopten.

En los casos de detenciones en delito flagrante, en los que se inicie averiguación previa con detenido, el Agente del Ministerio Público de la Federación solicitará por escrito y de inmediato a la autoridad competente que presente la querella o cumpla el requisito equivalente, dentro del plazo de retención que establece el artículo 16, párrafo séptimo, de la Constitución Política de los Estados Unidos Mexicanos.

B) Ante los órganos jurisdiccionales:

a) Ejercer la acción penal ante el órgano jurisdiccional competente por los delitos del orden federal cuando exista denuncia o querella, esté acreditado el cuerpo del delito de que se trate y la probable responsabilidad de quien o quienes en él hubieren intervenido, solicitando las órdenes de aprehensión o de comparecencia, en su caso;

b) Solicitar al órgano jurisdiccional las órdenes de cateo, las medidas precautorias de arraigo, de aseguramiento o embargo precautorio de bienes, los exhortos o la constitución de garantías para los efectos de la reparación de los daños y perjuicios, salvo que el inculpado los hubiese garantizado previamente;

c) Poner a disposición de la autoridad judicial a las personas detenidas y aprehendidas dentro de los plazos establecidos por la ley;

d) Aportar las pruebas y promover las diligencias conducentes para la debida comprobación de la existencia del delito, las circunstancias en que hubiese sido cometido y las peculiares del inculpado, de la responsabilidad penal, de la existencia de los daños y perjuicios así como para la fijación del monto de su reparación;

e) Formular las conclusiones en los términos señalados por la ley y solicitar la imposición de las penas y medidas de seguridad que correspondan y el pago de la reparación de los daños y perjuicios o, en su caso, plantear las causas de exclusión del delito o las que extinguen la acción penal;

f) Impugnar, en los términos previstos por la ley, las resoluciones judiciales, y

g) En general, promover lo conducente al desarrollo de los procesos y realizar las demás atribuciones que le señalen las normas aplicables.

C) En materia de atención a la víctima o el ofendido por algún delito:

a) Proporcionar asesoría jurídica a la víctima u ofendido e informarle de los derechos que en su favor establece la Constitución Política de los Estados Unidos Mexicanos y, cuando lo solicite, sobre el desarrollo del procedimiento penal;

b) Recibir todos los elementos de prueba que la víctima u ofendido le aporte en ejercicio de su derecho de coadyuvancia, para la comprobación del cuerpo del delito y la probable responsabilidad del inculpado, así como para determinar, en su caso, la procedencia y monto de la reparación del daño. Cuando el Ministerio Público de la Federación considere que no es necesario el desahogo de la diligencia, deberá fundar y motivar su negativa;

c) Otorgar las facilidades para identificar al probable responsable y, en los casos de delitos contra la libertad y el normal desarrollo psicosexual, privación ilegal de la libertad, o cuando así lo considere procedente, dictar todas las medidas necesarias para evitar que se ponga en peligro la integridad física y psicológica de la víctima u ofendido;

d) Informar a la víctima u ofendido que desee otorgar el perdón en los casos procedentes, el significado y trascendencia jurídica de dicho acto;

e) Dictar las medidas necesarias y que estén a su alcance para que la víctima u ofendido reciba atención médica y psicológica de urgencia. Cuando el Ministerio Público de la Federación lo estime necesario, tomará las medidas conducentes para que la atención médica y psicológica se haga extensiva a otras personas;

f) Solicitar a la autoridad judicial, en los casos en que sea procedente, la reparación del daño, y

g) Informar a la víctima o al ofendido menor de edad, que no está obligado a carearse con el inculpado cuando se trate de los delitos de violación o secuestro. En estos casos, las declaraciones respectivas se efectuarán conforme lo establezcan las disposiciones aplicables.

II. Vigilar la observancia de la constitucionalidad y legalidad en el ámbito de su competencia, sin perjuicio de las atribuciones que legalmente correspondan a otras autoridades jurisdiccionales o administrativas. En ejercicio de esta atribución el Ministerio Público de la Federación deberá:

a) Intervenir como parte en el juicio de amparo, en los términos previstos por el artículo 107 constitucional y en los demás casos en que la Ley de Amparo, Reglamentaria de los Artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos, disponga o autorice esta intervención;

b) Intervenir como representante de la Federación en todos los negocios en que ésta sea parte o tenga interés jurídico. Esta atribución comprende las actuaciones necesarias para el ejercicio de las facultades que confiere al Procurador General de la República la fracción III del artículo 105 de la Constitución Política de los Estados Unidos Mexicanos.

Tratándose de asuntos que revistan interés y trascendencia para la Federación, el Procurador General de la República mantendrá informado al Presidente de la República de los casos relevantes, y requerirá de su acuerdo por escrito para el desistimiento;

c) Intervenir como coadyuvante en los negocios en que las entidades paraestatales de la Administración Pública Federal sean parte o tengan interés jurídico, a solicitud del coordinador de sector correspondiente. El Procurador General de la República acordará lo pertinente tomando en cuenta la importancia que el asunto revista para el interés público.

Los coordinadores de sector y, por acuerdo de éstos las entidades paraestatales, conforme a lo que establezca la ley respectiva, por conducto de los órganos que determine su régimen de gobierno, deberán hacer del conocimiento de la Institución los casos en que dichas entidades figuren como partes o como coadyuvantes, o de cualquier otra forma que comprometa sus funciones o su patrimonio ante órganos extranjeros dotados de atribuciones jurisdiccionales. En estos casos la Institución se mantendrá al tanto de los procedimientos respectivos y requerirá la información correspondiente. Si a juicio del Procurador General de la República el asunto reviste importancia para el interés público, formulará las observaciones o sugerencias que estime convenientes, y

d) Intervenir en las controversias en que sean parte los diplomáticos y los cónsules generales, precisamente en virtud de esta calidad. Cuando se trate de un procedimiento penal y no aparezcan inmunidades que respetar, el Ministerio Público de la Federación procederá en cumplimiento estricto de sus obligaciones legales, observando las disposiciones contenidas en los tratados internacionales en que los Estados Unidos Mexicanos sea parte.

III. Intervenir en la extradición o entrega de indiciados, procesados, sentenciados, en los términos de las disposiciones aplicables, así como en el cumplimiento de los tratados internacionales en que los Estados Unidos Mexicanos sea parte;

IV. Requerir informes, documentos, opiniones y elementos de prueba en general a las dependencias y entidades de la Administración Pública Federal, a las correspondientes al Distrito Federal y a los Estados integrantes de la Federación, y a otras autoridades y personas que puedan suministrar elementos para el debido ejercicio de dichas atribuciones.

Es obligatorio proporcionar los informes que solicite el Ministerio Público de la Federación en ejercicio de sus funciones. El incumplimiento a los requerimientos que formule el Ministerio Público de la Federación será causa de responsabilidad en términos de la legislación aplicable;

V. Promover la pronta, expedita y debida procuración e impartición de justicia, y

VI. Las demás que las leyes determinen.

II. Conocer de los asuntos que tengan a su cargo las delegaciones, relacionados con los delitos materia de su competencia, de conformidad con las normas aplicables y políticas institucionales o cuando así lo determinen el Procurador o el Subprocurador respectivo;

III. Ejercer la facultad de atracción para la investigación y persecución de delitos del fuero común que tengan conexidad con delitos federales materia de su competencia;

IV. Remitir a las delegaciones por conducto de la Dirección General de Control de Averiguaciones Previas las indagatorias relacionadas con delitos materia de su competencia, para su prosecución, de conformidad con las normas y políticas institucionales, o cuando así lo determinen el Procurador o el Subprocurador respectivo;

V. Autorizar los acuerdos de reserva, incompetencia, acumulación y separación de las averiguaciones previas a su cargo;

VI. Establecer mecanismos de coordinación con las unidades administrativas que tengan a su cargo el control y seguimiento de las averiguaciones previas y de los procesos penales federales, a fin de perfeccionar el ejercicio de la acción penal, y facilitar las actuaciones procesales que deban desahogarse ante los órganos jurisdiccionales;

VII. Coordinarse con las delegaciones en las investigaciones y diligencias que practique en el ámbito territorial de la Delegación respectiva, relacionadas con aquellos delitos materia de su competencia, de conformidad con las normas aplicables y políticas institucionales o cuando así lo determinen el Procurador o el Subprocurador respectivo, así como brindar asesoría y apoyo a las delegaciones;

VIII. Proponer, en coordinación con las unidades administrativas competentes de la Institución, políticas, estrategias y líneas de acción para combatir los delitos materia de su competencia;

IX. Participar, en coordinación con las unidades administrativas competentes de la Institución, en los organismos y grupos internacionales encargados o que tengan relación con la investigación y represión de los delitos materia de sus respectivas competencias;

X. Proporcionar a las unidades administrativas competentes de la Institución la información y estadística de los delitos materia de su competencia;

XI. Ejercer el mando directo e inmediato sobre el personal que le esté adscrito, y

XII. Las demás que les confieran otras disposiciones aplicables o el Procurador.

De conformidad con lo antes referido el artículo 29 del Reglamento de la Ley Orgánica de la Procuraduría General de la República quedaría de la siguiente forma con la creación de la Unidad Especializada en cuestión:

Las unidades especializadas en delitos que no se consideren cometidos por la delincuencia organizada serán competentes para conocer los asuntos siguientes:

I. Unidad Especializada en Investigación de Delitos contra los Derechos de Autor y la Propiedad Industrial, conocerá de los delitos en materia de derechos de autor y propiedad industrial previstos en el Código Penal Federal y en la Ley de la Propiedad Industrial, respectivamente;

II. Unidad Especializada en Investigación de Delitos Fiscales y Financieros conocerá de los delitos que a continuación se indican:

a) Fraude previsto en el Código Penal Federal;

b) Los comprendidos en el Código Fiscal de la Federación, y

c) Los previstos en la Ley del Seguro Social, y en las leyes especiales relativas a las instituciones del sistema financiero.

III. Unidad Especializada en Investigación de Delitos Cometidos por Servidores Públicos y contra la Administración de Justicia, conocerá de los delitos cometidos por servidores públicos ajenos a la Procuraduría y contra la administración de justicia previstos en el Código Penal Federal, y

IV. Unidad Especializada en Investigación de Delitos contra el Ambiente y previstos en Leyes *E*speciales, conocerá de los delitos ambientales previstos en el Código Penal Federal y los delitos de otros géneros que se encuentren contenidos en leyes especiales y que no sean de competencia de otra unidad especializada, de conformidad con las disposiciones que al efecto emita el Procurador.

Lo anterior sin perjuicio de que el Procurador emita los criterios mediante los cuales las Delegaciones de la Institución en las entidades federativas queden facultadas para el conocimiento de los ilícitos de esta naturaleza.

A nuestro parecer a continuación se transcribe la necesidad de la unidad en cuestión, se debe adicionar:

V. "*Unidad Especializada en Investigación de Delitos Informáticos,* *conocerá de los delitos previstos en los artículos 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6 y 211 bis 7 del Código Penal Federal en relación al acceso ilícito a sistemas y equipos de informática, artículo 13 de la Ley Federal del Derecho de Autor en cuanto a la regulación legal en materia de derecho de autor a los Programas de Computación y las Bases de Datos, artículo 21 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación a la prohibición que tienen los sujetos obligados de hacer mal uso de los datos personales o en las disposiciones correspondientes de las legislaciones penales de las entidades* federativas.

Y por último de acuerdo al artículo 27 del Reglamento de la Ley Orgánica de la Procuraduría General de la República, el titular de la unidad tendrá las facultades siguientes:

I. Ejercer las atribuciones previstas en el artículo 4 de la Ley Orgánica, respecto de los delitos materia de su competencia, en coordinación con las unidades administrativas y órganos competentes;

II. Conocer de los asuntos que tengan a su cargo las delegaciones, relacionados con los delitos materia de su competencia, de conformidad con las normas aplicables y políticas institucionales o cuando así lo determinen el Procurador o el Subprocurador respectivo;

III. Ejercer la facultad de atracción para la investigación y persecución de delitos del fuero común que tengan conexidad con delitos federales materia de su competencia;

IV. Remitir a las delegaciones por conducto de la Dirección General de Control de Averiguaciones Previas las indagatorias relacionadas con delitos materia de su competencia, para su prosecución, de conformidad con las normas y políticas institucionales, o cuando así lo determinen el Procurador o el Subprocurador respectivo;

V. Autorizar los acuerdos de reserva, incompetencia, acumulación y separación de las averiguaciones previas a su cargo;

VI. Establecer mecanismos de coordinación con las unidades administrativas que tengan a su cargo el control y seguimiento de las averiguaciones previas y de los procesos penales federales, a fin de perfeccionar el ejercicio de la acción penal, y facilitar las actuaciones procesales que deban desahogarse ante los órganos jurisdiccionales;

VII. Coordinarse con las delegaciones en las investigaciones y diligencias que practique en el ámbito territorial de la Delegación respectiva, relacionadas con aquellos delitos materia de su competencia, de conformidad con las normas aplicables y políticas institucionales o cuando así lo determinen el Procurador o el Subprocurador respectivo, así como brindar asesoría y apoyo a las delegaciones;

VIII. Proponer, en coordinación con las unidades administrativas competentes de la Institución, políticas, estrategias y líneas de acción para combatir los delitos materia de su competencia;

IX. Participar, en coordinación con las unidades administrativas competentes de la Institución, en los organismos y grupos internacionales encargados o que tengan relación con la investigación y represión de los delitos materia de sus respectivas competencias;

X. Proporcionar a las unidades administrativas competentes de la Institución la información y estadística de los delitos materia de su competencia;

XI. Ejercer el mando directo e inmediato sobre el personal que le esté adscrito, y

XII. Las demás que les confieran otras disposiciones aplicables o el Procurador.

Así mismo de conformidad con el artículo 79 del Reglamento de la Ley Organica de la Procuraduría General de la República dentro de las facultades del Delegado deberá coordinarse con las unidades especializadas en las investigaciones y práctica de diligencias en el ámbito territorial de la Delegación, relacionadas con aquellos delitos materia de su competencia, para efectos de su trámite, seguimiento y vigilancia e Informar a las unidades especializadas sobre asuntos de su competencia y, en su caso, remitir las actuaciones correspondientes cuando así lo requieran.

Alcances Legales y Limitaciones de la Unidad Especializada en Investigación de Delitos Informáticos

Lamentablemente con la creación de la Unidad Especializada en Investigación de delitos informáticos no terminan estas acciones; se requiere de reformas a la legislación federal y estatal debido a que no coinciden en sus tipos penales o simplemente las entidades federativas no cuentan con la legislación en la materia. Por ende, la policía cibernética no resulta eficiente debido a la falta de cuerpos especializados para el tratamientos de delitos informáticos, de tal forma no pueden manejar las cuestiones probatorias y de procedimiento y lo más grave es la falta de jurisdicción y la conformación del tipo delictivo como federal u ordinario.

En el Ámbito Internacional, los tratados internacionales de derechos humanos reconocen la extradición; sin embrago, nos presentamos ante un problema en el proceso, es decir, para el sujeto activo es fácil realizar la acción delictiva ya que la mayoría de los delitos en comento no se encuentran legislados casi en ningún país, lo cual implica una falta de aplicabilidad.

El Domingo 1 de Abril de 2007 en el diario *La Crónica de Hoy*, cita: *"Está en pañales la legislación mexicana contra ciberdelitos: PGR; los cometen a la velocidad de la luz y los investigan al ritmo de un* elefante.

La llamada red de redes del ciberespacio se ha convertido en el caldo de cultivo para cometer múltiples delitos que aumentan vertiginosamente, mientras la comunidad mundial parece correr con la rapidez de un tractor para combatirlos. La cibercriminalidad lo hace a la velocidad de la luz, sin dejar rastros. Un método de seguridad que hoy tiene éxito, mañana quizá, habrá sido superado por los "piratas informáticos". Para cometer un ilícito como el lavado de dinero a través de la informática sólo se necesita de un minuto, pero para investigarlo se necesita, en el mejor de los casos, ocho meses. Mientras las grandes compañías piensan que invierten lo adecuado para asegurar sus sistemas, el incremento dramático de estos delitos indica lo contrario. Así, las reglas técnicas de la red evolucionan tan aprisa que las legislaciones mundiales bruscamente se quedan obsoletas. ***La legislación para combatir los delitos cibernéticos en México, dijo la PGR, "está en pañales" y sus principales debilidades son la definición de las figuras delictivas y el ámbito de competencia que limita las acciones en contra de las bandas organizadas que operan en varios países.*** *Apuntó que esta gran movilidad que hoy tienen los delincuentes creció al amparo de la globalización y de las nuevas tecnologías, por lo que "los gobiernos y los servidores públicos están llamados a actualizarse y trabajar unidos, compartir los avances científicos y tecnológicos con aquellas naciones que hoy atraviesan por dificultades económicas, sin poder acceder a las herramientas de la investigación moderna". Indicó que los delitos cibernéticos más reportados en México son: fraudes,*

introducción de virus, pirateo de páginas oficiales, tráfico de menores, terrorismo, sabotaje, clonación de tarjetas de crédito y señales satelitales, usurpación de identidad, robo y alteración de información. Alertó que utilizar microchips en lectores de tarjetas de crédito ha permitido conocer las claves de acceso de los usuarios para llevar a cabo fraudes financieros. El ciberdelito es muy alarmante, indicó, cuando se utilizan las redes de informática para el tráfico de drogas o lavar dinero o cuando una computadora se usa para destruir a cientos de personas al mismo tiempo, es decir, terroristas cibernéticos. Y advirtió: "Si la sociedad no es consciente de que las redes y todo este tipo de delitos cibernéticos están generando impactos reales en la seguridad pública y en todos los individuos, usen o no internet". De acuerdo a un análisis de la Procuraduría General de la República, "phishing" se le llama a la práctica en la que los delincuentes se apropian de la clave de los usuarios de servicios bancarios para estafar o robarlos. En esta práctica es común que clonen o incluso interfieran páginas bancarias en la que se pide al usuario dar su clave. Por clonación de tarjetas de crédito los bancos registran pérdidas de aproximadamente 400 millones de pesos anualmente. A partir de esta información, advirtió, los delincuentes cibernéticos saben todo sobre uno, los gustos que tiene uno, así como sus aficiones. Y la meta es vender algo o llevar a cabo una estafa. Hizo notar que sólo basta el registro que queda en las tiendas donde se aceptan tarjetas de crédito o débito, para que estas bandas cometan todo tipo de delitos. Por su parte, los analistas del FBI, Inez M. Miyamoto y Daniel R. Broker, mencionaron que la tendencia del crecimiento de la cibercriminalidad es casi exponencial. La evolución de las tecnologías y la diversidad de los medios de acceso a la red conllevan un aumento de la criminalidad electrónica. Durante su participación en el Congreso Internacional La Cibercriminalidad Hoy" que organizó la PGR, advirtieron que la delincuencia,

organizada o no, se ha apropiado ampliamente de las tecnologías de la informática, con consecuencias perjudiciales para las personas, las organizaciones y los Estados. En el mundo de policías y delincuentes, dijeron, la pesquisa cibernética se ha vuelto una parte esencial del trabajo de investigación. Mencionaron que la dimensión virtual de internet, en su aspecto lúdico (juego), puede ocultar para el usuario joven y con pocos conocimientos de informática, graves peligros relacionados con prostitución, pornografía o con la venta ilegal de drogas y armas. Joel Gómez Treviño, presidente fundador de la Academia Mexicana de Derecho Informático, advirtió que es complicado descubrir los delitos en los que se usa internet por lo difícil que resulta seguir las pistas, porque lo mismo se puede hacer un fraude en Lituania desde una computadora en Chile que uno desde Rusia en contra de un usuario en México. Y ejemplificó: "Para cometer un ilícito como el lavado de dinero se necesita un minuto, pero para investigarlo se necesitan, en el mejor de *los casos, ocho meses".* (1)

Operación de la Unidad Especializada en Investigación de delitos informáticos con la Policía Cibernética

Como bien sabemos unas de las atribuciones de la Secretaría de Seguridad Pública es la prevención del delito; y por lo tanto con el crecimiento de los delitos informáticos se crea la Policía Cibernética, la cual tiene como fin vigilar o patrullar las páginas Web que existan y la comisión de delitos por medios informáticos como nos referimos en el Código Penal Federal (en los artículos 211 bis 1- 211 bis 7)

La Policía Cibernética junto con las personas que integran la Unidad Especializada en delitos informáticos deberán trabajar en paralelo, es decir en el caso

de que la policía cibernética detectara por medio de la vigilancia de las páginas Web o reciban una denuncia de cualquier ciudadano de carácter en delitos informáticos, ésta le informe a la Unidad Especializada para intervenir con el fin de que la tarea de prevención del delito sea más efectiva o en su caso que surjan de la acción directa de la Policía Cibernética.

3.1.1. Ley Orgánica de la Procuraduría General de la República

La presente Ley fue publicada en el Diario Oficial de la Federación el 27 de diciembre de 2002, con una Fe de erratas del 11 de febrero de 2003.

Esta Ley tiene por objeto organizar la Procuraduría General de la República, ubicada en el ámbito del Poder Ejecutivo Federal para el despacho de los asuntos que al Ministerio Público de la Federación y al Procurador General de la República le atribuyen la Constitución Política de los Estados Unidos Mexicanos, este ordenamiento y demás disposiciones aplicables.

El citado ordenamiento consta de 10 Capítulos; distribuidos en Disposiciones Generales; Bases de Organización; De los Auxiliares del Ministerio Público de la Federación; De la Suplencia y Representación del Procurador General de la República; Del Servicio de Carrera de Procuración de Justicia Federal; De los procesos de Evaluación de los Servidores Públicos; De los derechos de los Agentes del Ministerio Público de la Federación, de la Policía Federal Investigadora y Peritos; De las Causas de Responsabilidad de los Agentes del Ministerio Público de la Federación, Agentes de la Policía Federal Investigadora y Peritos; De las Sanciones de los Agentes del

Ministerio Publico de la Federación, Agentes de la Policía Federal Investigadora y Peritos; y Disposiciones Finales; Así como de 9 transitorios.

3. 2. Estructura Orgánica de la Procuraduría General de la República

Ámbito de Competencia

La Procuraduría General de la República es una Institución ubicada en el ámbito del poder Ejecutivo Federal, a cargo de un Procurador General de la República, quien preside al Ministerio Público de la Federación.

Por lo tanto es la encargada del despacho de los asuntos que la Constitución Política de los Estados Unidos Mexicanos, la Ley Orgánica de la Procuraduría General de la República, su Reglamento y otros ordenamientos, le encomiendan al Procurador General de la República y al Ministerio Público de la Federación. (2)

Misión y Visión

La misión de la Procuraduría General de la República es representar a la sociedad y a la federación en la investigación y persecución de delitos del fuero federal, con apego a los principios de legalidad, certeza y seguridad jurídica, con respeto a los derechos humanos, que garanticen el Estado de Derecho. Así mismo la visión institucional es fortalecer la estructura funcional de procuración de justicia y un sistema saneado; para que en el año 2025 las instituciones que participen en la procuración de justicia sean de excelencia, cuenten con personal con vocación de servicio y sólida formación que contribuya a que los ciudadanos vivan en condiciones que promuevan el desarrollo integral dentro del Estado de Derecho. (3)

Marco Jurídico

La Legislación Jurídica que rige la actuación del Procurador General de la República, de los Agentes del Ministerio Público de la Federación, de la policía investigadora y de los peritos se encuentra en la Constitución Política de los Estados Unidos Mexicanos, en la Ley Orgánica de la Procuraduría General de la República y en su Reglamento, así como en otros ordenamientos tales como:

- Reglamento del Servicio de Carrera de Procuración de Justicia Federal
- Lineamientos para el Ejercicio Presupuestal 2006
- Manual de Organización General
- Legislación Secundaria (Acuerdos) (4)

3. 3. Competencia jurisdiccional.

Al frente de cada Subprocuraduría habrá un Subprocurador, que será nombrado en términos del artículo 17 de la Ley Orgánica y tendrá las facultades siguientes conforme al artículo 13 del Reglamento Interior de la Ley Orgánica de la Procuraduría General de la República.

ARTÍCULO 13. Al frente de cada Subprocuraduría habrá un Subprocurador, que será nombrado en términos del artículo 17 de la Ley Orgánica y tendrá las facultades siguientes:

I. Organizar, coordinar, dirigir y evaluar las unidades administrativas que le estén adscritas;

II. Acordar con el Procurador el despacho de los asuntos de su competencia;

III. En el ámbito de su competencia, fortalecer los mecanismos de cooperación y colaboración con autoridades federales, de las entidades federativas y municipales, atendiendo a las normas aplicables y políticas institucionales conforme a los lineamientos que emita el Procurador;

IV. Emitir o suscribir los instrumentos jurídicos a que se refiere el artículo 7 de la Ley Orgánica;

V. Autorizar en definitiva el no ejercicio de la acción penal, previo dictamen del Agente del Ministerio Público de la Federación auxiliar del Procurador, salvo la atribución conferida a los Delegados de la Institución en las entidades federativas; resolver la formulación de conclusiones no acusatorias; desahogar las prevenciones que la autoridad judicial acuerde en los términos de la ley, respecto de la omisión de formular conclusiones en el término legal o de conclusiones presentadas en un proceso penal cuya consecuencia sea el sobreseimiento del mismo; o de cualquier incidente procesal que tuviere como resultado la libertad absoluta del inculpado antes de que se pronuncie sentencia. Tratándose del no ejercicio de la acción penal deberá notificarse a la víctima u ofendido de conformidad con las disposiciones aplicables;

VI. Participar en coordinación con las unidades administrativas competentes de la Institución, en la formulación de anteproyectos de iniciativas de leyes, tratados, decretos, reglamentos y demás instrumentos normativos que se relacionen con los asuntos materia de su competencia;

VII. Ejercer y supervisar las facultades que correspondan a las unidades administrativas que le estén adscritas, sin perjuicio de que sean desempeñadas por sus respectivos titulares, y

VIII. Las demás que les confieran otras disposiciones o el Procurador.

3. 4. Ministerio público.

Conforme a su artículo 4 del Reglamento Interior de la Procuraduría General de la República, son Agentes del Ministerio público de la Federación:

I. El Procurador;

II. Los Subprocuradores;

III. El Fiscal Especializado para la Atención de Delitos Electorales;

IV. El Visitador General;

V. El Titular de la Coordinación de Asuntos Internacionales y Agregadurías;

VI. El Titular de la Coordinación General de Delegaciones;

VII. Los titulares de las Unidades Especializadas;

VIII. Los Directores Generales:

a) De Asuntos Jurídicos;

b) De Constitucionalidad;

c) De Normatividad;

d) De Extradiciones y Asistencia Jurídica;

e) De Control de Averiguaciones Previas;

f) De Control de Procesos Penales Federales;

g) De Amparo;

h) De Atención a Recomendaciones y Amigables Conciliaciones en Derechos Humanos;

i) Jurídico en Materia de Delitos Electorales;

j) De Averiguaciones Previas en Materia de Delitos Electorales;

k) De Control de Procesos y Amparo en Materia de Delitos Electorales;

l) De Visitaduría;

m) De Inspección Interna;

n) De Supervisión e Inspección Interna para la Agencia Federal de Investigación, y

ñ) De Delitos Cometidos por Servidores Públicos de la Institución,

IX. Los titulares de las Delegaciones, y

X. Aquellos servidores públicos a los que el Procurador confiera dicha calidad mediante Acuerdo.

Los servidores públicos que por esta disposición adquieren el carácter de agentes del Ministerio Público de la Federación deberán contar con título y cédula profesional de licenciado en Derecho, y cumplir los demás requisitos que exige este Reglamento.

3. 4. 1 Policía cibernética.

ORÍGENES

Ejerciendo sus atribuciones legales y para garantizar la presencia de la autoridad en la supercarretera de la información, la Policía Federal Preventiva desarrolló en México la primera Unidad de Policía Cibernética, que además de las acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en los países desarrollados.

Los crímenes cometidos en agravio de menores a través de una computadora y otros medios han tenido un incremento sin precedentes, tanto en México como en el mundo, derivado de la velocidad del desarrollo tecnológico y con las crecientes oportunidades de acceso a Internet. La red ha sido utilizada por organizaciones criminales de pedófilos que promueven y transmiten pornografía infantil; también, se sabe de las operaciones de bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento.

Otro tipo de crímenes que se han incrementado de manera considerable son el fraude cibernético, la piratería de software, la intrusión a sistemas de computo, el hackeo, la venta de armas y drogas por internet y el ciberterrorismo las cuales son amenazas para la sociedad.

Por lo tanto la Secretaría de Seguridad Pública mediante la Policía Federal Preventiva, contribuye con su granito de arena para proteger el entorno de la red Internet.

MISIÓN

- Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.
- Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos.

- Realización de operaciones de patrullaje anti hacker, utilizando internet como instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.
- Análisis y desarrollo de investigaciones en el campo sobre las actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

Como resultado del crecimiento de delitos informáticos, la Policía Cibernética de la PFP, asumió el cargo de la Secretaría Técnica del Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos en México, a través de la cual se promueve una cultura de legalidad, respeto y seguridad en la red.

Actividades

- Integrar un equipo especializado en delitos cibernéticos a fin de hacer de este medio electrónico un lugar seguro para el intercambio de información. Analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciber espacio, así como su modus operandi.
- Utilizar Internet como un instrumento para identificar a los delincuentes que cometen este tipo de delitos.
- Realizar patrullajes en la red a fin de localizar sitios que hayan podido ser vulnerados.
- Analizar y desarrollar estrategias para la identificación de los diversos delitos ocurridos en Internet.

- Ofrecer seguridad en la navegación en la Internet para los menores, ya que existen peligros en ella.
- Identificar los procedimientos mediante los cuales los niños son explotados por personas mayores.
- Identificar la naturaleza, extensión y causas de los delitos cometidos en contra de mujeres y menores como son la corrupción y explotación sexuales.
- Identificar y combatir el crimen organizado dedicado al tráfico de menores.
- Establecer técnicas adecuadas para la búsqueda y localización oportuna de niños extraviados, perdidos y/o robados.
- Crear estrategias para combatir a las redes de delincuentes que se dedican a dañar a los menores de edad.
- Desintegrar y poner a disposición del Agente del Ministerio Público a las bandas de pedófilos dedicadas a la explotación sexual de menores y a la pornografía infantil.
- Acciones de operación con autoridades locales, federales e internacionales. (5)

CONCLUSIONES

PRIMERA.- El avance tecnológico requiere de la especialización constante. No se puede tener progreso cuando no se cumple con la finalidad de capacitarse ante las exigencias que el mundo moderno demanda, de ahí la necesidad y el compromiso que tenemos los profesionistas de actualizarnos en la diversidad cognoscitiva tanto nacional como internacional que el derecho informático demanda.

SEGUNDA.- Existe legislación federal y estatal que regulan cuestiones de delitos informáticos, la cual no es suficiente y clara en sus definiciones y por tal resulta hasta confusa. Esto refleja la importancia que representa en la actualidad el fenómeno informático, ya que la existencia de normas jurídicas en la materia, es el resultado de la demanda que hace la sociedad de contar con un marco legal regulatorio de los diversos campos en el cual interviene el derecho informático.

TERCERA.- Se requiere contar con un mayor número de juristas en materia de derecho informático. Esto solo podrá realizarse siempre y cuando se de la apertura necesaria a esta disciplina empezando por las instituciones educativas, lo cual nos permitiría contar en un futuro no muy lejano con un buen número de estudiosos interesados y desarrolladores de temas en el cual el derecho informático sea la piedra angular. De igual forma, el gobierno mexicano deberá buscar la apertura de este tipo de temas que permitan interesar al publico en general y considerar la idea de contar con más de una dependencia del gobierno de estudios del Derecho Informático como la Secretaría de Gobernación, que

cuenta con la Dirección General de Consulta del Orden Jurídico Nacional y ésta a su vez, con el Registro Nacional de Avisos de Testamentos, el cual contribuye a dar certeza y seguridad jurídica a los gobernados, ya que ante la tramitación de un juicio sucesorio, es un instrumento jurídico valioso al ser el medio por el cual se confirma la inexistencia o existencia de uno o varios testamentos, a través de la consulta que se hace a su base de datos central.

CUARTA.- Se requiere de una reforma al Reglamento Interior de la Procuraduría General de la República, para crear una ***Unidad Especializada de Investigación en Delitos Informáticos*** en la Procuraduría General de la República, con el fin dar un seguimiento a las denuncias de los ciudadanos sobre hechos que constituyan delitos informáticos, o bien que se deriven de la Policía Cibernética y acudan con el titular de dicha Unidad o simplemente la indagación de dichos delitos. El ministerio público federal acreditará un curso de especialización en delitos Informáticos para la integración de la averiguación previa, todo lo anterior de conformidad con los artículos 8 y 27 del Reglamento de la Ley Orgánica de la Procuraduría General de la República.

QUINTA.-Se requiere de una mayor difusión en la tarea que realiza la Policía Cibernética, con el fin de prevenir el delito; está labor consiste en dar a conocer a través de los medios electrónicos las atribuciones y funciones de dicha policía.

CITAS CAPÍTULO UNO

1) Beer, Stafford, Cibernética y Administración, México, 1965, Pág. 27.

(2) El mundo de la Computación, Editorial Océano. Volumen 3 y 4.

(3) Internet, http://www.monografias.com/trabajos6/delin/delin.shtml, Universidad del Salvador, Octubre 2000.

(4) Campoli, Gabriel, Derecho Penal Informático en México, Ed. Instituto Nacional de Ciencias Penales, México, 2004, Pág. 10.

(5) Téllez, Valdés, Julio, Derecho Informático, 3era Edición, Ed. Mc Graw Hill, México, 2003, Pág. 5.

(6) Ibid. Pág.6.

(7) Internet, http://bine.org.mx/?q=node/1147 , La Comunidad Académica en línea Noviembre 2005.

(8) Téllez, Valdés, Julio, Op. Cit. Pág.17.

(9) Campoli, Gabriel, Op. Cit. Pág.13.

(10) Altmark, Daniel Ricardo. La etapa precontractual en los contratos informáticos. Vol. I, Editorial De Palma. Buenos Aires, 1987. Pág. 18.

(11) Peñaranda, Héctor. La informática jurídica y el derecho informático como ciencias. El derecho informático como rama autónoma del derecho. Revista Electrónica de Derecho Informático (REDI), No.3 1998.

(12) Téllez, Valdés, Julio, Op. Cit. Pág. 20.

(13) Héctor Peñaranda, La informática jurídica y el derecho informático como ciencias. El derecho informático como rama autónoma del derecho [en línea], Redi, octubre de 1998, [citado 12/03/2005], Revista Electrónica de Derecho Informático (Núm. 003).

(14) Campoli, Gabriel, Op. Cit. Pág.10.

(15) Ibid. Pág. 17.

(16) Téllez, Valdés, Julio, Op. Cit. Pág.163.

(17) Fernández, Calvo, Rafael, El tratamiento del llamado delito informático en el proyecto de ley orgánico del Código Penal de Argentina; Reflexiones y propuestas de la C. L. I. (Comisión de libertades e informática).

(18) Téllez, Valdés, Julio, Op. Cit. Pág.163.

(19) Ibid. Pág.164.

(20) Ibid. Pág. 165-166.

(21) Ibid. Págs. 167-174.

(22) Campoli, Gabriel, Op. Cit. Pág. 20.

(23) Idem.

(24) Ibid. Pág. 21.

(25) Ibid. Pág. 22.

(26) Ibid. Pág. 23.

(27) y (28) Internet, http://www.monografias.com/trabajos6/delin/delin.shtml, Universidad del Salvador, Octubre 2000.

CITAS CAPÍTULO DOS

(1) Téllez, Valdés, Julio, Op. Cit. Pág. 23.

(2) Idem.

(3) Idem.

(4) Secretaría de Gobernación, Dirección General de Compilación y Consulta del Orden Jurídico Nacional, Temas de Derecho Informático, 1era Edición, junio de 2006, Pág. 79.

(5) Campoli, Gabriel, Op. Cit. Págs. 85-86.

(6) Idem.

(7) Idem.

(8) Téllez, Valdés, Julio, Op. Cit. Pág. 170.

(9) Idem.

CITAS CAPÍTULO TRES

(1) Adolfo Sánchez Venegas, "Está en pañales la legislación mexicana contra ciberdelitos: PGR; los cometen a la velocidad de la luz y los investigan al ritmo de un elefante", Disponible en: http://www.cronica.com.mx/nota.php?id_nota=293553. Consultado el 1 de Abril de 2007.

(2) http://www.pgr.gob.mx/index.asp

(3) http://www.pgr.gob.mx/index.asp

(4) http://www.pgr.gob.mx/index.asp

(5)http://www.ssp.gob.mx/portalWebApp/appmanager/pcibernetica/desk?_nfls=false&_pageLabel=pcibernetica_page_1