UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

ÁREA ACADÉMICA DE DERECHO Y JURISPRUDENCIA

Los Delitos Informáticos e Internet en el Sistema Jurídico Penal Mexicano

PROYECTO TERMINAL DE CARÁCTER PROFESIONAL QUE, PARA OBTENER EL GRADO DE MAESTRA EN DERECHO PENAL Y CIENCIAS PENALES PRESENTA:

PRESENTA: ESTELA JUÁREZ MENDOZA.

DIRECTOR: DR. ROBERTO WESLEY ZAPATA DURÁN.

PACHUCA, HIDALGO OCTUBRE 2014

A Dios por permitirme llegar a estas Instancias de la vida.

A mi madre y a mi padre, quienes hicieron de mí

Lo que ahora soy, mujer de trabajo y perseverancia.

A ti José Manuel, que eres el motor de mi vida y por

quien día a día lucho por ser mejor para ti y por ti.

A esta gloriosa Universidad Autónoma del Estado de Hidalgo

y que en su aulas me forme como profesionista.

¿Por qué esta magnifica tecnología científica, que ahorra trabajo y nos hace la vida más fácil nos aporta tan poca felicidad? La respuesta es esta, simplemente: porque aún no hemos aprendido a usarla con tino.

(Albert Einstein)

ÍNDICE

RESUMEN

La presente investigación se concreta en analizar los delitos informáticos tanto en la legislación nacional como internacional, las cuales tienen relación o contemplan tipos penales susceptibles de ser cometidos por medios informáticos, establecer y analizas la falta de regulación de todas y cada una de las conductas llevadas acabo dentro de nuestra sociedad.

Es necesario en la actualidad estudiar, analizar y solucionar los problemas que la sociedad presenta, pues las misma se ha visto rebasada por el avance tecnológico y los delitos que a través de este se llevan a cabo, sin lograr empatar, a la tecnología y la regulación de la diversas conductas llictas que pudieran llevarse a cabo de la misma, toda vez que segundo a segundo se crea nuevos delitos, programas e instrumentos con los cuales delinquir, mismos que quedan en el olvido debido a la falta de legislación para ser castigados por las leyes.

El internet resulta ser la vía más rápida, eficiente y eficaz para cometer delitos informáticos, sin que estos seas castigados, pues evidentemente segundo a segundo se crean nuevos programas para el avance en la tecnología, sin embargo son malamente empleados para generar daños a la sociedad.

En resumen en la actualidad ha resultado materialmente imposible regular todas y cada una de las conductas llictas, que fenecen en delitos informáticos y la imposibilidad a la que se enfrentan las legislaciones nacionales como internaciones para castigar dichos delitos, debido a que el internet resulta se una interconexión transfronteriza, sin embargo dentro del presente proyecto se realiza un análisis de la legislación mexicana y su forma de regular dichas conductas.

ABSTRACT

This research is only an analysis of the computing crimes in both national and international legislations, which are related or consider penal types subject to be committed by computing means, as well as establishing and analyzing the lack of regulation of all and every conduct carried out by our society.

It is necessary nowadays to study, analyze and find a solution to problems of our society, because they have been surpassed by the technological advancements, and the crimes being made thru them, which exceed the technology and the regulation of several illegal conducts, which could be carried out about them, but every second a new crime is produced, even under delinquent programs and instruments, and that they are forgotten for lack of legislation under which to be punished.

Internet is the fastest and efficient way to commit computing crimes, and not be punished, because every second there are new programs invented for technology advancement, however they may be used to create damages for society.

In summary, up to date, it has been almost impossible to regulate every and all illegal conducts which constitute computing crimes, and the impossibility of national and international legislations to confront them, because internet is only an interconnection among nations. However, within this project an analysis is made of the Mexican Legislation and how it can regulate such conducts.

INTRODUCCIÓN

En la actualidad la Informática está alcanzando una enorme influencia en la vida diaria de las personas, junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, (Internet, comunicación, transacciones electrónicas, etc.) han surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos informáticos, electrónicos, cibernéticos. Los delitos informáticos, electrónicos, cibernéticos son: "como método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito; como medio: conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo y como fin: conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla." [1]

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas (virus, gusanos, troyanos, etc.), han creado nuevas posibilidades del uso indebido por parte de la delincuencia, de las computadoras e internet, lo que ha creado la necesidad de regulación por parte del derecho. De acuerdo al principio de exacta aplicación de le ley penal "En los juicios del orden criminal queda prohibido imponer, por simple analogía, y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata."[2]

[1] Lima de la luz María*, Delitos Electrónicos*, Ed. Porrúa, México 1994, pág., 123.

[2] Constitución Política de los Estados Unidos Mexicanos, *Articulo 14 Tercer Párrafo*, www.diputados.gov.mx, Consultado 22 Abril 2014.

El presente trabajo tiene como objetivo, analizar las conductas delictivas que pueden generar las tecnologías informáticas y su uso a través del internet, con el objeto de encuadrar dichos ilícitos en el Sistema Jurídico Mexicano, sin embargo debemos de tener en cuenta que las conductas delictivas (delitos informáticos, electrónicos, cibernéticos), no son cometidas por la computadoras, si no que es el ser humano quien las comete con ayuda de las aquellas e internet, 3"las computadoras son utilizadas como una herramienta que ofrece oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales."[3] También es importante señalar que el sujeto activo de los delitos informáticos, son personas de cierto estatus intelectual, o con conocimientos avanzados en informática.

Ante el esquema de globalización y la dependencia de las tecnologías informáticas, así como el uso masivo y universal de Internet, los países cada vez se ven más afectados, por parte de las personas que utilizan para delinquir el Internet a través de las computadoras o medios electrónicos para cometer delitos como fraude, sabotaje, robo, con el propósito de obtener un lucro indebido, y también atrae a otros tipos de delincuentes, como los terroristas cibernéticos cuyos esfuerzos se orientan a afectar la economía, paz social, gobierno y estabilidad, con el propósito simplemente de causar daño, y terror. "Los futuros ataques terroristas a gran escala los realizará una persona sentada detrás de una computadora, y no necesariamente con un coche bomba o mediante el secuestro de un avión".[4]

Según estadísticas existen más de mil quinientos millones de usuarios de Internet en el mundo; quizás el número llegue una séptima parte de la población del planeta. Por otra parte el 10% de la población global está formada por criminales profesionales que utilizan la computadora y los medios electrónicos para delinquir.

[3] Ricardo Levene, Alicia Chiaravalloti, *Introducción a los Delitos Informáticos Tipos y Legislación*, http://www.chiaravalloti_ asociados.dtj.com, Consultado 10 Septiembre de 2012.
[4] Davis, Tom, Legislador de Estados Unidos, *Terrorismo Cibernético,* Director Grupo de Trabajo de Información Tecnológica del gobierno de los Estados Unidos www.alfaredi.org/revista.com. consultado el 22 de Septiembre de 2013.

Esto indica, que puede haber unos 50 millones de usuarios de Internet que son criminales en informática profesionales. “En los Estados Unidos se arresta y condena al 5% de los criminales informáticos; el riesgo que corren, es mínimo y la recompensa potencial es alta pues, por ejemplo, en Canadá y los Estados Unidos el comercio electrónico al menudeo en 2012 fue de 150 mil millones de dólares. El comercio electrónico entre empresas sumo 2 billones de dólares. En los Estados Unidos las perdidas financieras ascendieron a 265, 589,940 millones de dólares por causa de delincuentes informáticos en 2012.” [5]

En las ultimas reformas que ha sufrido el Código Penal Federal, así como la creación de nuevas leyes federales, como la ley de seguridad nacional que entró en vigor el primero de febrero de 2005, se encuentran enfocadas a ciertas conductas delictivas, relacionadas estrechamente con el desarrollo de las nuevas tecnologías de información y comunicación.

Dicho trabajo aborda el tema de los delitos Informáticos, cibernético, electrónicos y pone en relieve que la problemática no es nueva; si no que nos enfrentamos a solo nuevas formas o modalidades de comisión de delitos que actualmente se encuentran tipificados como los que alguna vez el derecho tuvo que afrontar en similares situaciones, como por ejemplo: la aparición en su tiempo del cine y la televisión y sus respectivos contenidos, solo que en este delito su comisión es a través de tecnología informática.

La mayoría de los autores que abordan estos temas como los delitos cibernéticos, electrónicos o informáticos, e incluso en el Tercer Congreso Nacional Cultura de la Legalidad e Informática Jurídica,[6] y las tendencias de los países que abordan estas

[5] McAfee Virtual Criminology Report, *McAfee North America Criminology Report Organized crime and the Internet 2007 Real time Publishers*, http://www.realtime-websecurity.com, consultado el 22 de Septiembre de 2010.

[6] Tercer Congreso Nacional Cultura de la Legalidad e Informática Jurídica, http://www.ordenjuridico.gob.mx.congreso/congreso, consultado 8 Septiembre de 2007.

situaciones indican que se debe de legislar sobre este tema, por el problema de territorialidad de la ley antes expuesto.

Es de suma importancia que si se realizan reformas legislativas, estás no se orienten por la creación de nuevos tipos penales, sino por la de considerar la posibilidad de incluir el uso de las nuevas tecnologías informáticas, como el uso de Internet a través de la computadora, como un medio para realizar el delito.

Entre las modalidades de delitos informáticos encontramos terrorismo cibernético, crimen organizado, tráfico de drogas, personas, armas, piratería, pornografía Infantil, estafas electrónicas, delitos tradicionales cometidos a través de medios electrónicos.

Los delitos informáticos, electrónicos, cibernéticos son nuevos tipos de delitos ? o son delitos clásicos? (robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes), ya previstos en leyes penales en México, que se presentan en una nueva forma de comisión a través del uso de los avances tecnológicos informáticos exteriorizados con el auxilio de la Internet a través de una computadora.

De lo anterior expuesto, los objetivos de la investigación son los siguientes:

1 Analizar si los delitos informáticos son nuevos tipos de delitos o si los tipos penales existentes en los que se pueden encuadrar este tipo de delitos son suficientes para acreditar los elementos del tipo penal, analizando; el marco normativo y la jurisprudencia en materia de los delitos informáticos, así como la legislación penal federal y de las diversas entidades federativas que han legislado sobre este tema, y los organismos encargados de la prevención de estos tipos de delitos como la policía cibernética de la Secretaria de Seguridad Publica Federal.

2 Proponer reformas a las leyes penales federales materia de este delito, no

orientadas a la creación de nuevos tipos penales, sino a considerar la posibilidad de incluir el uso de las tecnologías informáticas como medio para cometer este tipo de delitos.

JUSTIFICACIÓN DEL TEMA.

La libertad con la que se desenvuelve cualquier persona dentro del llamado ciberespacio, propicia una seria discusión sobre el tema: hasta donde llega la libertad y hasta donde se puede dañar con esa libertad?

El uso de tecnologías informáticas nos lleva al ámbito del derecho y continua con otro problema, que es válido para todas las ramas que conforman a esté, el sentido del presente trabajo se enfoca a prestar atención a los aspectos más gravosos, como lo son los fraudes Informáticos y demás delitos informáticos, para el individuo derivados del uso de las tecnologías informáticas, tan gravoso que forman parte del catálogo de actos a la que la ley vincula la aplicación de una sanción penal o incluso debido a la novedad de estos comportamientos, se plantea si deben de tener cabida en la misma legislación penal federal o si en realidad han estado en está, pero su forma de comisión se presenta a través de situaciones diferentes, esta es la base de nuestro estudio desde un punto de vista académico ya que, en estos momentos el tratamiento y la consideración, desde el punto de vista del derecho penal, de aquellas conductas que emergen de la realidad social vinculadas a la tecnología de la información y que plantean serias interrogantes sobre su trascendencia penal.

METODOLOGÍA.

La investigación a realizar es mayoritariamente de naturaleza jurídica dogmática y normativa, por lo tanto, se sujetará a la aplicación de las técnicas de investigación documentales, fuentes normativas, informáticas y bibliográficas.

Por lo que se refiere a las fuentes normativas, haremos referencia a las disposiciones contenidas en la Constitución Política de los Estados Unidos Mexicanos que se refieren a los principios o garantías penales en las leyes y en el procedimiento como por ejemplo el principio de audiencia, exacta aplicación de la ley penal etc. Código Penal Federal, Código Nacional de Procedimientos Penales, y los códigos penales de algunas entidades federativas que han legislado sobre los delitos informáticos como lo son el Código Penal para el Distrito Federal y Código Penal para el Estado de Sinaloa y la jurisprudencia establecida por la Suprema Corte de Justicia de la Nación.

Al ir desarrollando esta investigación determinaremos cual es la naturaleza jurídica de los delitos informáticos analizando los elementos del tipo penal de esta clase de delitos, las legislación penal federal que emana de esta clase de delitos para determinar si se trata de delitos que ya se encuentran establecidos y que lo que varia es su forma de comisión de los mismos o si se encuentra ante una nueva clase de delitos según los elementos del tipo penal y de la informática jurídica.

Analizaremos el marco normativo y la jurisprudencia en materia de los delitos informáticos así como la legislación que se refiere a estos delitos en materia penal o no penal, para darnos una idea de lo que se ha avanzado en la actualidad en México en esta clase de delitos, en materia penal federal y de las diversas entidades federativas que han legislado sobre este tema, y los organismos encargados de la prevención de estos tipos de delitos concluyendo y dando la opinión derivado de nuestro estudio sobre esta clase de delitos enfocándolos a la ciencia penal, tomando en cuenta las leyes federales y locales.

CAPITULO I

INTRODUCCIÓN DEL DERECHO INFORMÁTICO PARA CONOCER, Y ENTENDER EL LENGUAJE INFORMÁTICO, ASÍ COMO LOS ANTECEDENTES HISTÓRICOS Y NOCIONES BÁSICAS DEL DERECHO INFORMÁTICO

1.1. La computación en general.

Los principales instrumentos en los que se basa esta tesis son las computadoras por lo que es necesario exponer los rasgos de esta, debido a que la computadora se ha considerado como la herramienta por excelencia y de rápida respuesta y eficiencia, toda vez que resulta ser el principal vehículo para la comisión de delitos informáticos.

Debido a que los medios electrónicos se han convertido en un instrumento de comunicación, obtención, análisis, intercambio de datos y documentos electrónicos. Los mismos son una herramienta indispensable en los distintos sectores sociales, económicos, jurídicos y culturales.

Con el uso de la computadora es posible la interconexión, en el ámbito mundial de todos los que se encuentren dispuestos a sumergirse en el Océano de la información en el cual no se encuentran límites, hablando de educación y de cultura, sin embargo también puede atraer aspectos negativos.

Las nuevas generaciones de hoy, encuentran a los ordenadores, ya no como un instrumento de aprendizaje y método de instrucción personal, sino como una necesidad en la vida del estudiante y de las nuevas generaciones.

El uso de la instrumentos electrónicos, no solo atrae aspectos educativos, sino también recreacionales al poder bajar programas, juegos, música y almacenar

datos e información que se podría utilizar en el futuro, sin duda la computadora ha venido a mejorar, optimizar y eficientizar el trabajo, así como la rapidez, mejoramiento en los tramites que en un pasado significaba la perdida de tiempo. Es por hoy la computadora no solo un instrumento sino una necesidad para las generaciones futuras y mas en el aspecto que nos interesa, hablando de derecho, leyes, abogados, tribunales y juzgados en los cuales la misma ha venido a realizar un papel importante en una justicia pronta y expedita, de lo que habla nuestra Constitución Política de los Estados Unidos Mexicanos.

La computadora es considerada como una máquina capaz de efectuar, una secuencia de operaciones mediante un programa, de tal manera, que se realice un procesamiento sobre un conjunto de datos de entrada, obteniéndose otro conjunto de datos de salida.

Por otro lado tenemos que el multicitado instrumento, es el equipo informático, de tratamiento automático de datos que contienen los órganos (o elementos) necesarios, para su funcionamiento autónomo.[7]

Como otro concepto tenemos, "que la computadora, es un maquina que computa o calcula".[8]

Jorge Vasconcelos para definir a la computadora señala "Maquina que sigue un estricto programa de instrucciones para procesar gran cantidad de datos muy rápidamente".[9]

A) Tipos de computadora.

I. Se clasifican de acuerdo al principio de operación de Analógicas y Digitales**.**

[7] Téllez Valdez Julio, *Derecho informático,* Ed. Mc Graw Hill, México 2004, Pág. 438.
[8] *Gran Diccionario Enciclopédico Visual, Programa visual*, Ed. Encas, México 1998, Pág. 301.
[9] Vascocelos Santillán Jorge. *Sistemas de Información, Informática II*, Ed. Publicaciones Cultural, México 2002, Pág. 141.

a) Computadora Analógica.

Aprovechando el hecho de que diferentes fenómenos físicos se describen por relaciones matemáticas similares (v.g. Exponenciales, Logarítmicas, etc.) pueden entregar la solución muy rápidamente. Pero tienen el inconveniente que al cambiar el problema a resolver, hay que realambrar la circuitería (cambiar el Hardware).

b) Computadora Digitales.

Están basadas en dispositivos bi-estables, i.e., que sólo pueden tomar uno de dos valores posibles: **'1'** ó **'0'**. Tienen como ventaja, el poder ejecutar diferentes programas para diferentes problemas, sin tener que la necesidad de modificar físicamente la máquina.

1.1.1 Orígenes históricos.

Uno de los primeros dispositivos mecánicos para contar fue el ábaco, cuya historia se remonta a las antiguas civilizaciones griega y romana. Este dispositivo es muy sencillo, consta de cuentas ensartadas en varillas que a su vez están montadas en un marco rectangular. Al desplazar las cuentas sobre varillas, sus posiciones representan valores almacenados, y es mediante dichas posiciones que este representa y almacena datos. A este dispositivo no se le puede llamar computadora por carecer del elemento fundamental llamado programa.

Otro de los inventos mecánicos fue la Pascalina inventada por Blaise Pascal (1623 - 1662) de Francia y la de Gottfried Wilhelm von Leibniz (1646 - 1716) de Alemania. Con estas máquinas, los datos se representaban mediante las posiciones de los engranajes, y los datos se introducían manualmente estableciendo dichas posiciones finales de las ruedas, de manera similar a como leemos los números en el cuentakilómetros de un automóvil.

La primera computadora fue la máquina analítica creada por Charles Babbage, profesor matemático de la Universidad de Cambridge en el siglo XIX. La idea que tuvo Charles Babbage sobre un computador nació debido a que la elaboración de las tablas matemáticas era un proceso tedioso y propenso a errores. En 1823 el gobierno Británico lo apoyo para crear el proyecto de una máquina de diferencias, un dispositivo mecánico para efectuar sumas repetidas.

Mientras tanto Charles Jacquard (francés), fabricante de tejidos, había creado un telar que podía reproducir automáticamente patrones de tejidos leyendo la información codificada en patrones de agujeros perforados en tarjetas de papel rígido. Al enterarse de este método Babbage abandonó la máquina de diferencias y se dedico al proyecto de la máquina analítica que se pudiera programar con tarjetas perforadas para efectuar cualquier cálculo con una precisión de 20 dígitos. La tecnología de la época no bastaba para hacer realidad sus ideas.

El mundo no estaba listo, y no lo estaría por cien años más.

En 1944 se construyó en la Universidad de Harvard, la Mark I, diseñada por un equipo encabezado por Howard H. Aiken. Esta máquina no está considerada como computadora electrónica debido a que no era de propósito general y su funcionamiento estaba basado en dispositivos electromecánicos llamados relevadores.

En 1947 se construyó en la Universidad de Pennsylvania la ENIAC (Electronic Numerical Integrator And Calculator) que fue la primera computadora electrónica, el equipo de diseño lo encabezaron los ingenieros John Mauchly y John Eckert. Esta máquina ocupaba todo un sótano de la Universidad, tenía más de 18 000 tubos de vacío, consumía 200 KW de energía eléctrica y requería todo un sistema de aire acondicionado, pero tenía la capacidad de realizar cinco mil operaciones aritméticas en un segundo.

El proyecto, auspiciado por el departamento de Defensa de los Estados Unidos, culminó dos años después, cuando se integró a ese equipo el ingeniero y

matemático húngaro John von Neumann (1903 - 1957). Las ideas de von Neumann resultaron tan fundamentales para su desarrollo posterior, que es considerado el padre de las computadoras.

La EDVAC (Electronic Discrete Variable Automatic Computer) fue diseñada por este nuevo equipo. Tenía aproximadamente cuatro mil bulbos y usaba un tipo de memoria basado en tubos llenos de mercurio por donde circulaban señales eléctricas sujetas a retardos.

La idea fundamental de von Neumann fue: permitir que en la memoria coexistan datos con instrucciones, para que entonces la computadora pueda ser programada en un lenguaje, y no por medio de alambres que eléctricamente interconectaban varias secciones de control, como en la ENIAC.

Todo este desarrollo de las computadoras suele divisarse por generaciones y el criterio que se determinó para determinar el cambio de generación no está muy bien definido, pero resulta aparente que deben cumplirse al menos los siguientes requisitos:

I) La forma en que están construidas.
II) Forma en que el ser humano se comunica con ellas.

A) Primera Generación.

En esta generación había un gran desconocimiento de las capacidades de las computadoras, puesto que se realizó un estudio en esta época que determinó que con veinte computadoras se saturaría el mercado de los Estados Unidos en el campo de procesamiento de datos.

Esta generación abarco la década de los cincuenta. Y se conoce como la primera generación. Estas máquinas tenían las siguientes características:

I) Estas máquinas estaban construidas por medio de tubos de vacío.
II) Eran programadas en lenguaje de máquina.

En esta generación las máquinas son grandes y costosas (de un costo aproximado de ciento de miles de dólares).

En 1951 aparece la UNIVAC (universal Computer), fue la primera computadora comercial, que disponía de mil palabras de memoria central y podían leer cintas magnéticas, se utilizó para procesar el censo de 1950 en los Estados Unidos.

En las dos primeras generaciones, las unidades de entrada utilizaban tarjetas perforadas, retomadas por Herman Hollerith (1860 - 1929), quien además fundó una compañía que con el paso del tiempo se conocería como IBM (International Bussines Machines).

Después se desarrolló por IBM la IBM 701 de la cual se entregaron 18 unidades entre 1953 y 1957.

Posteriormente, la compañía Remington Rand fabricó el modelo 1103, que competía con la 701 en el campo científico, por lo que la IBM desarrollo la 702, la cual presentó problemas en memoria, debido a esto no duró en el mercado.

La computadora más exitosa de la primera generación fue la IBM 650, de la cual se produjeron varios cientos. Esta computadora que usaba un esquema de memoria secundaria llamado tambor magnético, que es el antecesor de los discos actuales.

Otros modelos de computadora que se pueden situar en los inicios de la segunda generación son: la UNIVAC 80 y 90, las IBM 704 y 709, Burroughs 220 y UNIVAC 1105.[10]

B) Segunda Generación.

Cerca de la década de 1960, las computadoras seguían evolucionando, se reducía su tamaño y crecía su capacidad de procesamiento. También en esta época se empezó a definir la forma de comunicarse con las computadoras, que recibía el nombre de programación de sistemas.

Las características de la segunda generación son las siguientes:

I) Están construidas con circuitos de transistores.
II) Se programan en nuevos lenguajes llamados lenguajes de alto nivel.

En esta generación las computadoras se reducen de tamaño y son de menor costo. Aparecen muchas compañías y las computadoras eran bastante avanzadas para su época como la serie 5000 de Burroughs y la ATLAS de la Universidad de Manchester.

Algunas de estas computadoras se programaban con cintas perforadas y otras más por medio de cableado en un tablero. Los programas eran hechos a la medida por un equipo de expertos: analistas, diseñadores, programadores y operadores que se manejaban como una orquesta para resolver los problemas y cálculos solicitados por la administración. El usuario final de la información no tenía contacto directo con las computadoras. Esta situación en un principio se produjo en las primeras computadoras personales, pues se requería saberlas "programar" (alimentarle instrucciones) para obtener resultados; por lo tanto su uso estaba limitado a aquellos audaces pioneros que gustaran de pasar un buen número de horas escribiendo instrucciones, "corriendo" el programa resultante y verificando y

[10] Huerta Miranda Marcelo, *Delitos Informáticos, segunda edición, complementada y actualizada*, Chile 1998, Pág. 5.

corrigiendo los errores o bugs que aparecieran. Además, para no perder el "programa" resultante había que "guardarlo" (almacenarlo) en una grabadora de astte, pues en esa época no había discos flexibles y mucho menos discos duros para las PC; este procedimiento podía tomar de 10 a 45 minutos, según el programa. El panorama se modificó totalmente con la aparición de las computadoras personales con mejores circuitos, más memoria, unidades de disco flexible y sobre todo con la aparición de programas de aplicación general en donde el usuario compra el programa y se pone a trabajar. Aparecen los programas procesadores de palabras como el célebre Word Star, la impresionante hoja de cálculo (spreadsheet) Visicalc y otros más que de la noche a la mañana cambian la imagen de la PC. El sortware empieza a tratar de alcanzar el paso del hardware. Pero aquí aparece un nuevo elemento: el usuario.

El usuario de las computadoras va cambiando y evolucionando con el tiempo. De estar totalmente desconectado a ellas en las máquinas grandes pasa la PC a ser pieza clave en el diseño tanto del hardware como del software. Aparece el concepto de human interface que es la relación entre el usuario y su computadora. Se habla entonces de hardware ergonómico (adaptado a las dimensiones humanas para reducir el cansancio), diseños de pantallas antirreflejos y teclados que descansen la muñeca. Con respecto al software se inicia una verdadera carrera para encontrar la manera en que el usuario pase menos tiempo capacitándose y entrenándose y más tiempo produciendo. Se ponen al alcance programas con menús (listas de opciones) que orientan en todo momento al usuario (con el consiguiente aburrimiento de los usuarios expertos); otros programas ofrecen toda una artillería de teclas de control y teclas de funciones (atajos) para efectuar toda suerte de efectos en el trabajo (con la consiguiente desorientación de los usuarios novatos). Se ofrecen un sinnúmero de cursos prometiendo que en pocas semanas hacen de cualquier persona un experto en los programas comerciales. Pero el problema constante es que ninguna solución para el uso de los programas es constante. Cada nuevo programa requiere aprender nuevos controles, nuevos trucos, nuevos menús. Se empieza a sentir que la relación usuario PC no está

acorde con los desarrollos del equipo y de la potencia de los programas. Hace falta una relación amistosa entre el usuario y la PC.

Las computadoras de esta generación fueron: la Philco 212 (esta compañía se retiró del mercado en 1964) y la UNIVAC M460, la Control Data Corporation modelo 1604, seguida por la serie 3000, la IBM mejoró la 709 y sacó al mercado la 7090, la National Cash Register empezó a producir máquinas para proceso de datos de tipo comercial, introdujo el modelo NCR 315.

La Radio Corporation of América introdujo el modelo 501, que manejaba el lenguaje COBOL, para procesos administrativos y comerciales. Después salió al mercado la RCA 601.[11]

C) Tercera generación.

Con los progresos de la electrónica y los avances de comunicación con las computadoras en la década de los 1960, surge la tercera generacion de las computadoras. Se inaugura con la IBM 360 en abril de 1964.

Las características de esta generación fueron las siguientes:

I) Su fabricación electrónica esta basada en circuitos integrados.
II) Su manejo es por medio de los lenguajes de control de los sistemas operativos.

La IBM produce la serie 360 con los modelos 20, 22, 30, 40, 50, 65, 67, 75, 85, 90, 195 que utilizaban técnicas especiales del procesador, unidades de cinta de nueve canales, paquetes de discos magnéticos y otras características que ahora son estándares (no todos los modelos usaban estas técnicas, sino que estaba dividido por aplicaciones).

[11] *Ibid*.

El sistema operativo de la serie 360, se llamó OS que contaba con varias configuraciones, incluía un conjunto de técnicas de manejo de memoria y del procesador que pronto se convirtieron en estándares.

En 1964 CDC introdujo la serie 6000 con la computadora 6600 que se consideró durante algunos años como la más rápida.

En la década de 1970, la IBM produce la serie 370 (modelos 115, 125, 135, 145, 158, 168). UNIVAC compite son los modelos 1108 y 1110, máquinas en gran escala; mientras que CDC produce su serie 7000 con el modelo 7600. Estas computadoras se caracterizan por ser muy potentes y veloces.

A finales de esta década la IBM de su serie 370 produce los modelos 3031, 3033, 4341. Burroughs con su serie 6000 produce los modelos 6500 y 6700 de avanzado diseño, que se reemplazaron por su serie 7000. Honey - Well participa con su computadora DPS con varios modelos.

A mediados de la década de 1970, aparecen en el mercado las computadoras de tamaño mediano, o minicomputadoras que no son tan costosas como las grandes (llamadas también como mainframes que significa también, gran sistema), pero disponen de gran capacidad de procesamiento. Algunas minicomputadoras fueron las siguientes: la PDP - 8 y la PDP - 11 de Digital Equipment Corporation, la VAX (Virtual Address eXtended) de la misma compañía, los modelos NOVA y ECLIPSE de Data General, la serie 3000 y 9000 de Hewlett - Packard con varios modelos el 36 y el 34, la Wang y Honey - Well -Bull, Siemens de origen alemán, la ICL fabricada en Inglaterra. En la Unión Soviética se utilizó la US (Sistema Unificado, Ryad) que ha pasado por varias generaciones.[12]

D) Cuarta Generación.

[12] *Ibidem*, Pág. 9.

Aquí aparecen los microprocesadores que es un gran adelanto de la microelectrónica, son circuitos integrados de alta densidad y con una velocidad impresionante. Las microcomputadoras con base en estos circuitos son extremadamente pequeñas y baratas, por lo que su uso se extiende al mercado industrial. Aquí nacen las computadoras personales que han adquirido proporciones enormes y que han influido en la sociedad en general sobre la llamada *"revolución informática"*.

En 1976 Steve Wozniak y Steve Jobs inventan la primera microcomputadora de uso masivo y más tarde forman la compañía conocida como la Apple que fue la segunda compañía más grande del mundo, antecedida tan solo por IBM; y esta por su parte es aún de las cinco compañías más grandes del mundo.

En 1981 se vendieron 800 00 computadoras personales, al siguiente subió a 1 400 000. Entre 1984 y 1987 se vendieron alrededor de 60 millones de computadoras personales, por lo que no queda duda que su impacto y penetración han sido enormes.

Con el surgimiento de las computadoras personales, el software y los sistemas que con ellas de manejan han tenido un considerable avance, porque han hecho más interactiva la comunicación con el usuario. Surgen otras aplicaciones como los procesadores de palabra, las hojas electrónicas de cálculo, paquetes gráficos, etc. También las industrias del Software de las computadoras personales crece con gran rapidez, Gary Kildall y William Gates se dedicaron durante años a la creación de sistemas operativos y métodos para lograr una utilización sencilla de las microcomputadoras (son los creadores de CP/M y de los productos de Microsoft).

No todo son microcomputadoras, por su puesto, las mini computadoras y los grandes sistemas continúan en desarrollo. De hecho las máquinas pequeñas rebasaban por mucho la capacidad de los grandes sistemas de 10 o 15 años antes, que requerían de instalaciones costosas y especiales, pero sería equivocado suponer que las grandes computadoras han desaparecido; por el contrario, su

presencia era ya ineludible en prácticamente todas las esferas de control gubernamental, militar y de la gran industria. Las enormes computadoras de las series CDC, CRAY, Hitachi o IBM por ejemplo, eran capaces de atender a varios cientos de millones de operaciones por segundo.[13]

E) Quinta Generación.

En vista de la acelerada marcha de la microelectrónica, la sociedad industrial se ha dado a la tarea de poner también a esa altura el desarrollo del software y los sistemas con que se manejan las computadoras. Surge la competencia internacional por el dominio del mercado de la computación, en la que se perfilan dos líderes que, sin embargo, no han podido alcanzar el nivel que se desea: la capacidad de comunicarse con la computadora en un lenguaje más cotidiano y no a través de códigos o lenguajes de control especializados.

"Japón lanzó en 1983 el llamado programa de la quinta generación de computadoras"[14], con los objetivos explícitos de producir máquinas con innovaciones reales en los criterios mencionados. Y en los Estados Unidos ya está en actividad un programa en desarrollo que persigue objetivos semejantes, que pueden resumirse de la siguiente manera:

I) Procesamiento en paralelo mediante arquitecturas y diseños especiales y circuitos de gran velocidad.
II) Manejo de lenguaje natural y sistemas de inteligencia artificial.

El futuro previsible de la computación es muy interesante, y se puede esperar que esta ciencia siga siendo objeto de atención prioritaria de gobiernos y de la sociedad en conjunto.[15]

1.1.3. Concepto y estructuración.

[13] Huerta Miranda Marcelo, Op Cit, Pág. 11.
[14] Nava Garcés Alberto Enrique, Análisis de los Delitos Informáticos, Ed. Porrua, México 2005, Pág. 14.
[15] Huerta Miranda Marcelo, Op Cit, Pág. 14.

En el presente análisis he estado observando que la computadora es de gran utilidad para la vida diaria, sin embargo diversos autores que han hablado de aspectos de informática en sus libros o escritos no se ha llegado a un concepto en el que coincidan.

La computadora es el equipo informático, de tratamiento automático de datos que contienen los órganos (o elementos) necesarios, para su funcionamiento autónomo.[16]

Como otro concepto tenemos, "que la computadora, es un maquina que computa o calcula".[17]

Jorge Vasconcelos para definir a la computadora señala "Maquina que sigue un estricto programa de instrucciones para procesar gran cantidad de datos muy rapidamente".[18]

Estructuración de la computadora.

Principalmente la computadora se divide en dos partes el Hardware y Software.

A) Definición de Hardware.

Hardware son todos aquellos componentes físicos de una computadora, todo lo visible y tangible. El Hardware realiza las 4 actividades fundamentales: entrada, procesamiento, salida y almacenamiento secundario. Entrada Para ingresar los datos a la computadora, se utilizan diferentes dispositivos, por ejemplo: Teclado Dispositivo de entrada más comúnmente utilizado que encontramos en todos los equipos computacionales. El teclado se encuentra compuesto de 3 partes: teclas de función, teclas alfanuméricas y teclas numéricas.

[16] Téllez Valdez Julio, *Op Cit*, Pág. 438.
[17] *Gran Diccionario Enciclopédico Visual, Op Cit,* Pág. 301.
[18] Vascocelos Santillan Jorge. *Op Cit*, pag. 141.

I) Mouse.

Es el segundo dispositivo de entrada más utilizado. El Mouse o ratón es arrastrado a lo largo de una superficie para maniobrar un apuntador en la pantalla del monitor. Fue inventado por Douglas Engelbart y su nombre se deriva por su forma la cual se asemeja a la de un ratón.

II) Procesamiento.

El CPU (Central Proccesor Unit) es el responsable de controlar el flujo de datos (Actividades de Entrada y Salida E/S) y de la ejecución de las instrucciones de los programas sobre los datos. Realiza todos los cálculos (suma, resta, multiplicación, división y compara números y caracteres). Es el "cerebro" de la computadora.

Se divide en 3 Componentes

a) 1.Unidad de Control (UC)
b) 2.Unidad Aritmético/Lógica (UAL)
c) 3.Área de almacenamiento primario (memoria)

a) Unidad de control.

Es en esencia la que gobierna todas las actividades de la computadora, así como el CPU es el cerebro de la computadora, se puede decir que la UC es el núcleo del CPU. Supervisa la ejecución de los programas Coordina y controla al sistema de cómputo, es decir, coordina actividades de E/S Determina que instrucción se debe ejecutar y pone a disposición los datos pedidos por la instrucción. Determina donde se almacenan los datos y los transfiere desde las posiciones donde están almacenados. Una vez ejecutada la instrucción la Unidad de Control debe determinar donde pondrá el resultado para salida ó para su uso posterior.

b) Unidad Aritmético/Lógica.

Esta unidad realiza cálculos (suma, resta, multiplicación y división) y operaciones lógicas (comparaciones). Transfiere los datos entre las posiciones de almacenamiento. Tiene un registro muy importante conocido como: Acumulador ACC Al realizar operaciones aritméticas y lógicas, la UAL mueve datos entre ella y el almacenamiento. Los datos usados en el procesamiento se transfieren de su posición en el almacenamiento a la UAL. Los datos se manipulan de acuerdo con las instrucciones del programa y regresan al almacenamiento. Debido a que el procesamiento no puede efectuarse en el área de almacenamiento, los datos deben transferirse a la UAL. Para terminar una operación puede suceder que los datos pasen de la UAL al área de almacenamiento o varias veces.

c) Área de almacenamiento Primario.

La memoria da al procesador almacenamiento temporal para programas y datos. Todos los programas y datos deben transferirse a la memoria desde un dispositivo de entrada o desde el almacenamiento secundario (disquete), antes de que los programas puedan ejecutarse o procesarse los datos. Las computadoras usan 2 tipos de memoria primaria: ROM (read only memory), memoria de sólo lectura, en la cual se almacena ciertos programas e información que necesita la computadora las cuales están grabadas permanentemente y no pueden ser modificadas por el programador.

Las instrucciones básicas para arrancar una computadora están grabadas aquí y en algunas notebooks han grabado hojas de calculo, basic, etc. RAM (Random access memory), memoria de acceso aleatorio, la utiliza el usuario mediante sus programas, y es volátil. La memoria del equipo permite almacenar datos de entrada, instrucciones de los programas que se están ejecutando en ese momento, los dato s resultados del procesamiento y los datos que se preparan para la salida. Los datos proporcionados a la computadora permanecen en el almacenamiento primario hasta que se utilizan en el procesamiento. Durante el procesamiento, el almacenamiento primario almacena los datos intermedios y finales de todas las operaciones a aritméticas y lógicas. El almacenamiento primario debe guardar

también las instrucciones de los programas usados en el procesamiento. La memoria está subdividida en celdas individuales cada una de las cuales tiene una capacidad similar para almacenar datos.

III) Almacenamiento Secundario.

El almacenamiento secundario es un medio de almacenamiento definitivo (no volátil como el de la memoria RAM). El proceso de transferencia de datos a un equipo de cómputo se le llama procedimiento de lectura. El proceso de transferencia de datos desde la computadora hacia el almacenamiento se denomina procedimiento de escritura. En la actualidad se pueden usar principalmente dos tecnologías para almacenar información:

a) El almacenamiento Magnético.

b) El almacenamiento Óptico. Algunos dispositivos combinan ambas tecnologías.

a) Almacenamiento Magnético.

1) Discos Flexibles.

2) Discos Duros.

3) Cintas Magnéticas o Cartuchos.

b) Almacenamiento Óptico.

La necesidad de mayores capacidades de almacenamiento han llevado a los fabricantes de hardware a una búsqueda continua de medios de almacenamiento alternativos y cuando no hay opciones, a mejorar tecnologías disponibles y desarrollar nuevas. Las técnicas de almacenamiento óptico hacen posible el uso de la localización precisa mediante rayos láser.

Leer información de un medio óptico es una tarea relativamente fácil, escribirla es otro asunto. El problema es la dificultad para modificar la superficie de un medio óptico, ya que los medios ópticos perforan físicamente la superficie para reflejar o dispersar la luz del láser.

Los principales dispositivos de almacenamiento óptico son:

a) CD ROM.- CD Read Only Memory.

b) WORM.- Write Once, Read Many.

IV) Medios Magnético – Ópticos.

Estos medios combinan algunas de las mejores características de las tecnologías de grabación magnética y óptica. Un disco MO tiene la capacidad de un disco óptico, pero puede ser re-gravable con la facilidad de un disco magnético. Actualmente están disponibles en varios tamaños y capacidades.

V) Salida.

Los dispositivos de salida de una computadora es el hardware que se encarga de mandar una respuesta hacia el exterior de la computadora, como pueden ser: los monitores, impresoras, sistemas de sonido, módem. etc.

VI) Monitores.

El monitor ó pantalla de vídeo, es el dispositivo de salida más común. Hay algunos que forman parte del cuerpo de la computadora y otros están separados de la misma. Existen muchas formas de clasificar los monitores, la básica es en término de sus capacidades de color, pueden ser: Monocromáticos, despliegan sólo 2 colores, uno para el fondo y otro para la superficie. Los colores pueden ser blanco y negro, verde y negro ó ámbar y negro. Escala de Grises, un monitor a escala de grises es un tipo especial de monitor monocromático capaz de desplegar diferentes

tonos de grises. Color: Los monitores de color pueden desplegar de 4 hasta 1 millón de colores diferentes.

Conforme ha avanzado la tecnología han surgido los diferentes modelos: TTL, Monocromático, muy pobre resolución, los primeros no tenían capacidad de graficar. CGA, Color Graphics Adapter, desplegaba 4 colores, con muy pobre resolución a comparación de los monitores actuales, hoy en día fuera del mercado. EGA, Enhanced Graphics Adapter, manejaba una mejor resolución que el CGA, de 640x350 píxeles. (Los píxeles son los puntos de luz con los que se forman los caracteres y gráficas en el monitor, mientras más píxeles mejor resolución). D desplegaban 64 colores. VGA, Vídeo Graphics Array, los hay monocromáticos y de color. Adecuados para ambiente gráfico por su alta resolución (640x480 píxeles). Pueden llegar hasta 256,000 colores ó 64 tonalidades de gris dependiendo de la memoria destinada al dispositivo. PVGA, Súper Vídeo Graphics Array, maneja una resolución más alta (1,024x768), el número de colores desplegables varía dependiendo de la memoria, pero puede ser mayor que 1 millón de colores. UVGA, Ultra Vídeo Graphics Array, Resolución de 1280 x 1024.

La calidad de las imágenes que un monitor puede desplegar se define más por las capacidades de la Tarjeta controladora de vídeo, que por las del monitor mismo. El controlador de vídeo es un dispositivo intermediario entre el CPU y el monitor. El controlador contiene la memoria y otros circuitos electrónicos necesarios para enviar la información al monitor para que la despliegue en la pantalla.

B) Software.

Definición de Software.

El software es el conjunto de instrucciones que las computadoras emplean para manipular datos. Sin el software, la computadora sería un conjunto de medios sin utilizar. Al cargar los programas en una computadora, la máquina actuará como si recibiera a una educación instantánea; de pronto "sabe" cómo pensar y cómo operar. El Software es un conjunto de programas, documentos, procedimientos, y

rutinas asociados con la operación de un sistema de cómputo. Distinguiéndose de los componentes físicos llamados hardware. Comúnmente a los programas de computación se les llama software; el software asegura que el programa o sistema cumpla por completo con sus objetivos, opera con eficiencia, esta adecuadamente documentado, y suficientemente sencillo de operar. Es simplemente el conjunto de instrucciones individuales que se le proporciona al microprocesador para que pueda procesar los datos y generar los resultados esperados. El hardware por si solo no puede hacer nada, pues es necesario que exista el software, que es el conjunto de instrucciones que hacen funcionar al hardware.

1.2. ¿ Qué es la cibernética?

Parte importante del idioma de la computación, o informática es la cibernética, es importante para entender, de lo que estamos hablando, o de lo que vamos a hablar, o de lo que trata esta investigación, antes de conocer lo que son los delitos informáticos y lo que implica la informática, es importante conocer lo que es la cibernética, la cual es conocida como una ciencia que se encarga de estudiar la comunicación y el control entre el hombre y la maquina. La cibernética enlaza a la teoría general con el derecho

1.2.1. Orígenes históricos.

En 1948, un matemático Estadounidense, Nordert Wiener, escribió un libro titulado cibernética (*Cybernetics, or control and communication in the animal and machine*)[19] en el cual empleo este termino para designar a la nueva ciencia de la comunicación y control entre el hombre y la maquina.

[19] Guibourg Ricardo A., *Informática Jurídica Decisoria*, Ed. Astrea, Argentina, Pág. 16.

Ya un siglo antes Federico Engels en su libro titulado dialéctica de la naturaleza que en los puntos de unión o de contacto entre las distintas ciencias, fue donde se pueden esperar los mejores resultados, es decir, resaltar la importancia de las uniones interdisciplinarias.

1.2.2. Concepto y estructuración.

Si atendemos a la etimología de la palabra, el vocablo cibernética tiene su origen en la voz griega *kybernetes*, que significa piloto y *kybernes,* concepto referido al arte de gobernar esta palabra alude a la función del cerebro con respecto de las máquinas.

La cibernética es la ciencia de la comunicación y el control. [20] Los aspectos aplicados a estas disciplinas se encuentran relacionados con cualquier campo de estudio. Sus aspectos formales estudian una teoría general del control, la cual tiene aplicación en diversos campos y se adaptan a todos ellos.

1.3. ¿Qué es la Internet.?

Internet es un conjunto de redes locales conectadas entre si a través de una computadora especial por cada red, conocida como gateway. Las interconexiones entre gateways se efectúan a través de diversas guías de comunicación, entre las que figuran líneas telefónicas, fibras ópticas y enlaces por radio. Pueden añadirse redes adicionales conectando nuevas puertas. La información que debe enviarse a una máquina remota se etiquetan con una dirección computarizada de dicha máquina.

Los distintos tipos de servicios proporcionados por Internet utilizan diferentes formatos de dirección (dirección de Internet). Uno de los formatos se conoce decimal con puntos, otro formato describe el nombre del ordenador de destino y otras informaciones. Las redes situadas fuera de Estados Unidos utilizan sufijos

[20] Beer, Estanfford, *Cibernética y administración,* México 1967, Pág. 27.

que indican el país, por ejemplo (.es) para España. Dentro de los Estados Unidos, el sufijo anterior especifica el tipo de organización a que pertenece la red informática en cuestión, por ejemplo puede ser una institución educativa (edu).

1.3.1. Concepto.

Se podría definir al Internet como la interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales. También existen sistemas de redes llamados Internet generalmente para el uso de una única organización.

Aquí podemos destacar la llamada *red de redes o Internet* y definirla como un conjunto de elementos tecnológicos que permite enlazar masivamente redes de diferentes tipos, para que los datos puedan ser transportados de una a otra red.[21]

1.3.2. ¿Cómo funciona el Internet.?

La topología de Internet consiste en que varias computadoras individuales conectadas entre si forman una red de área local (LAN). Internet consiste en una serie de redes (LAN) interconectadas. Las computadoras personales y las estaciones de trabajo pueden estar conectadas a una red de área local mediante un MODEM a través de una conexión (RDSI o RTS), o directamente a la LAN. También hay otras formas de conexión a redes como la conexión T1.[22]

---

[21] Vascocelos Santillán Jorge. *Sistemas de Información, Informática II*, Ed. Publicaciones Cultural, México 2002, Pág. 142.

[22] Hernández Montoya escribe: *"Internet es la primera anárquica exitosa de la Historia. Esta red mundial de redes de computadoras no tiene gobierno. No se puede, además. Basta que dos computadoras se conecten para que armen una red incontrolable. Y en Internet hay cintos de miles mas cada mes. Paradójicamente Internet surgió como un proyecto del Ministerio de la Defensa de los Estados Unidos para el caso de un ataque nuclear: necesitaban una red comunicaciónal sin centro, modo de seguir operando desde varios puntos a la vez luego de destruido el comando central. Una institución anárquica originada en los cuarteles". Consultable en http://www.analitica.com/bitblioteca/roberto/teoria.asp#superautopista.*

1.4. ¿Qué es la informática.?

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

"Esta disciplina tiene en nuestros días un enorme desarrollo gracias a las computadoras pues tienen gran capacidad de memoria, y el acceso a los datos, y a la información se realiza de manera sencilla y rápida".[23]

1.4.1 Orígenes históricos.

Surge de la inquietud racional del hombre, el cual, ante la continua y creciente necesidad de información para una adecuada toma de decisiones, es impulsada a formular nuevos postulados y desarrollar nuevas técnicas que satisfagan dichos propósitos.

1.4.2 Concepto y estructuración.

La palabra informática es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en el año de 1962. En sentido general la informática se define como un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información para una adecuada toma de decisiones. Cabe aclarar que es más una técnica que una ciencia, debido a su carácter eminentemente pragmático.[24]

1.5 ¿Qué es la informática jurídica.?

[23] Guibourg, Op Cit, Pág. 19.
[24] Téllez Valdez Julio, *Op Cit*, Pág. 4.

La informática jurídica se presento en los términos de una informática documentaria de carácter jurídico, es decir, creación y recuperación e información que contenía datos jurídicos (leyes, jurisprudencia, doctrina) o al menos de interés jurídico. Poco a poco empezó a evolucionar la idea de que en estos bancos de datos jurídicos se podían obtener no solo información sino también, mediante programas estudiados expresamente, verdaderos actos jurídicos como certificaciones, atribuciones, de juez competente y sentencias premodeladas, por lo que nació así a fines de los años 60" la llamada informática jurídica.

También se le denomina Derecho Informático, "se refiere a la reglamentación, racional y científica, de la comunicación. Comprende por ende, lo vinculado con la computación. Su aspiración consiste en lograr una mejor convivencia; debiéndose respetar, escrupulosamente la libertad de expresión.[25]

1.5.1 Origen y evolución.

En sentido general, la informática jurídica es el conjunto de aplicaciones de la informática en el ámbito del derecho. Esta área surgió en 1959 en Estados unidos. La informática jurídica ha sufrido cambios a fines a la evolución general de la misma informática.

Las primeras investigaciones en materia de recuperación de documentos jurídicos en forma automatizada se remonta a los años 50", época en la se comienza a utilizar las computadoras no solo con fines matemáticos, sino también lingüísticos. Estos esfuerzos fueron realizados en el Health Law Center de la Universidad de Pittsburg, Pensylvania. El entonces director del centro, John Horty, estaba convencido de la necesidad de encontrar medios satisfactorios para tener acceso a la información legal. Para 1959, el centro colocó los ordenamientos legales de Pensylvania en cintas magnéticas, wl sistema fue demostrado posteriormente en 1960 ante la Amerycan Association Boreau Of Lawyers en la reunión anual en

[25] Vasconcelos Aguilar Mario, *El derecho y la sociología*, Ed. Porrua, México 2000, Pág. 30.

Washington, D.C. esta fue la primera demostración de un sistema legal automatizado de búsqueda de información.

1.5.2 Concepto y clasificación.

Si bien resulta difícil pretender dar una definición de la informática jurídica, como sucede en las disciplinas recientes, podemos decir que se trata, en última instancia del empleo de las computadoras en el ámbito jurídico.

En términos generales, podemos definir a la informática jurídica como la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de la información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación. [26]

[26]. Téllez Valdez Julio, *Op Cit*, pag. 18.

CAPITULO II.

DELITOS INFORMÁTICOS

2. ANTECEDENTES DE LOS DELITOS INFORMATICOS

2.1. Características de los delitos informáticos.

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho.

2.1.1. Concepto de delitos informáticos.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que Julio Téllez Valdés señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de ‘delitos’ en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere

que la expresión ‘delitos informáticos’ esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos, no ha sido objeto de tipificación aún".[27]

Para Carlos Sarzana, en su obra “Criminalita e Tecnología”, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".[28]

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".[29]

Rafael Fernández Calvo define al delito informático como: "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el Título 1 de la Constitución Española".[30]

María de la Luz Lima dice que: el delito electrónico "en un sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, y en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[31]

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que

---

[27]Téllez Valdez Julio, *Op Cit*, Pág. 103.
[28] Sarzana Carlo, *Criminalita e tecnología en computers crime*. Italia, Ed. Nos, Pág. 53.
[29]Callegari Lidia, *Delitos informáticos y legislación*. Colombia 1985, Revista dela Facultad de Derecho y Ciencias Política de la Universidad Pontificia Bolivariana, Edición # 70, Pág. 115.
[30] Fernández Calvo Rafael, *El tratamiento del llamado Delito Informático en el proyecto de la Ley orgánica del Código Penal, Reflexión y propuestas de la Comisión de Libertades e informática y Derecho*. España 1984, Pág. 1150.
[31] Lima de la Luz Maria, *Delitos electrónicos en Criminalistica*, México 1984, Ed. Porrua, Pág. 100.

se tienen a las computadoras como instrumento o fin", y por las segundas, "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

En este orden de ideas, en el presente trabajo se entenderán como delitos informáticos todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático.
Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes en México debido a que la legislación se refiere a derecho de autor y propiedad intelectual sin embargo, deberá tenerse presente que la propuesta final de este trabajo tiene por objeto la regulación penal de aquellas actitudes antijurídicas que estimamos más graves como último recurso para evitar su impunidad.

2.1.2. Características.

Según Téllez Valdés: “este tipo de acciones (Delitos Electrónicos) presentan las siguientes características principales

A) Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
B) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
C) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
D) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
E) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

F) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
G) Son muy sofisticados y relativamente frecuentes en el ámbito militar.
H) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
I) En su mayoría son imprudenciales y no necesariamente se cometen con intención.
J) Ofrecen facilidades para su comisión a los menores de edad.
K) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
L) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.[32]

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

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades encargadas de las investigaciones y los funcionarios judiciales.

2.1.3 Clasificación.

[32] Téllez Valdez Julio, *Op Cit*, Pág. 163.

A continuación analizaremos las respectivas clasificaciones de diversos autores. Estos se centran en la actividad del sujeto y no en el ámbito espacial en que ocurre dicha conducta.

Julio Téllez Valdez clasifica a los delitos informáticos con base en dos criterios, como instrumentó o medio, como fin u objetivo.[33]

Maria de la Luz Lima clasifica lo que llama “Delitos Electrónicos” en tres categorías.

A) Los que utilizan la tecnología electrónica como método.

Conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

B) Los que utilizan la tecnología electrónica como medio.

Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

C) Los que utilizan la tecnología electrónica como fin.

Conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

En esta clasificación no se distingue una diferencia, sustancial entre el método y el medio.

Pablo A. Palazi se apega mas a la dogmática penal, realiza una clasificación acorde con el bien jurídico tutelado.[34]

A) Delitos contra el patrimonio.
B) Delitos contra la intimidad.

[33] *Ibidem*, Pág. 165.

C) Delitos contra la seguridad publica y las comunicaciones
D) Falsificaciones Informáticas.
E) Contenidos ilegales en Internet.

Este autor se apega a distintos géneros de bienes jurídicamente tutelados, ahora bien, se refiere eminentemente en el medio que se utiliza para vulnerar los bienes jurídicamente tutelados.

2.1.3.1. Como instrumento o medio.

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

A) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
B) Variación de los activos y pasivos en la situación contable de las empresas.
C) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
D) Lectura, sustracción o copiado de información confidencial.
E) Modificación de datos tanto en la entrada como en la salida.
F) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
G) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
H) Uso no autorizado de programas de cómputo.
I) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
J) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

K) Obtención de información residual impresa en papel luego de la ejecución de trabajos.
L) Acceso a áreas informatizadas en forma no autorizada.
M) Intervención en las líneas de comunicación de datos o teleproceso.

2.1.3.2. Como fin u objeto.

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

A) Programación de instrucciones que producen un bloqueo total al sistema.
B) Destrucción de programas por cualquier método.
C) Daño a la memoria.
D) Atentado físico contra la máquina o sus accesorios.
E) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
F) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

2.1.3.3 Tipos de ataques contra los sistemas de información.

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

A) Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
B) Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
C) Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.

D) Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
E) Estafas electrónicas: A través de compras realizadas haciendo uso de la red.
F) Transferencias de fondos: Engaños en la realización de este tipo de transacciones.
G) Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:
H) Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
I) Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
J) Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

2.1.3.4. Clasificación de las Naciones Unidas (ONU).

A) Fraudes cometidos mediante manipulación de computadoras.

I) Manipulación de los datos de entrada

Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

II) La manipulación de programas

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

III) Manipulación de los datos de salida

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

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

B) Falsificaciones informáticas.

I) Como objeto.

Cuando se alteran datos de los documentos almacenados en forma computarizada.

II) Como instrumentos.

Las computadoras 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.

C) Daños o modificaciones de programas o datos computarizados.

I) 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:

II) Virus.

Es 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".[35]

III) 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.

IV) 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.

D) Acceso no autorizado a servicios y sistemas informáticos.

[35] Nava Garcés, *Análisis de los delitos informáticos,* 1ra ed., México 2005, p. 32.

I) 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.

II) 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.

E) 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. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.[36]

2.1.3.5. Otras clasificaciones.

A) Otros delitos.

[36] Hidalgo Ballina, Antonio, *Derecho Informático*, 4a. ed. México D.F. Flores Editor y Distribuidor, 2014, p.267.

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

2.2. Formas de control de los delitos informáticos.

2.2.1. Preventiva.

Como podemos inferir, este tipo de ilícitos requieren de un necesario control, y este, al no encontrar en la actualidad un adecuado entorno jurídico ha tenido que manifestarse, en su función preventiva, a través de diversas formas de carácter administrativo, normativo y técnico, de las que se encuentran las siguientes:

A) Elaboración de un examen psicometrico previo al ingreso al área de sistemas en las empresas.
B) Introducción, de cláusulas especiales en los contratos de trabajo, con el personal informático, que por el tipo de labores a realizar así lo requiera.
C) Establecimiento de un código ético de carácter interno en las empresas.
D) Adoptar estrictas medidas en el acceso y control de las áreas informáticas de trabajo.
E) Capacitación adecuada del personal informático, a efecto de evitar actitudes negligentes.
F) Identificación, yen su caso segregación, de personal informático descontento.
G) Rotación en el uso de clave de acceso al sistema (passwords).[37]

2.2.2 Correctiva.

[37] Téllez Valdez, Julio, *Derecho Informático, 4a.* ed., Mc Graw Hill, México 2009, p. 175.

Esto podrá darse en la medida en que se introduzca un conjunto de disposiciones jurídicas específicas en los códigos penales sustantivos, ya que en caso de considerar este tipo de ilícitos como figuras análogas "existentes", se corre el riesgo de alterar flagrantemente el principio de legalidad de las penas. (*nulla pena sine legem*).

Cabe hacer mención que una adecuada legislación al respecto traería consigo efectos no solo correctivos sino eventualmente preventivos, de forma que se reducirían en buen numero este tipote acciones que tanto daño causan a los intereses individuales y sociales, inhibiendo la eventual comisión de estos ilícitos.

El objetivo de la creación de un espacio de libertad, seguridad y justicia debe ser alcanzado mediante la prevención y la lucha contra la delincuencia, organizada o no, incluido el terrorismo, mediante la cooperación mas estrecha entre los servicios represivos y las autoridades judiciales de los distintos Estados interesados, al informar las legislaciones y las normas en materia de cooperación policial y judicial penal, la reciente entrada en funciones de la Corte Penal Internacional (Estatuto de Roma), pone de relieve la necesidad de pensar cada vez mas, en una "universalización" del derecho.[38]

2.3. Sujetos que intervienen en delitos informáticos.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos, el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada.[39] Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

[38] Téllez Valdez, Julio, *Derecho Informático, 4a.* ed., Mc Graw Hill, México 2009, p. 205.
[39]Manual de las Naciones Unidas, para la prevención y control de delitos informáticos.

Este nivel de criminalidad se puede explicar, porque existe una dificultad para reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien, los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas, de las dificultades ocasionadas por los delitos informáticos, y sus posibilidades son limitadas.

2.3.1. Sujeto activo.

Las personas que cometen los "Delitos electrónicos" 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 los delitos electrónicos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que, lo que los diferencia entre sí, es la naturaleza de los actos cometidos. De esta forma, la persona que "entra" en un sistema informático, sin intenciones delictivas es muy diferente, del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente es tema de controversia ya que para algunos en el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos, son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminológico norteamericano Edwin Sutherland en el año de 1943.[40]

Efectivamente, este conocido criminólogo señala un sin número de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios entre otros.

Así mismo, este criminológico estadounidense dice que tanto la definición de los "delitos informáticos" como las de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que el “sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional”.[41]

Hay dificultad para elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta, hay dificultades para descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos, existe una gran indiferencia de la opinión pública, sobre los daños ocasionados a la comunidad, la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables"

[40] Nava Garcés, Alberto E, *Delitos Informáticos*, 2a. ed., Porrúa, México, 2007, p. 150.
[41] *Ibid.*

otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Por nuestra parte, consideramos que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudios más profundos, que dada la naturaleza de nuestro objeto de estudio, nos vemos en la necesidad de limitar.

2.3.2 Sujeto pasivo.

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

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

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática, el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las

estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, una análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, debemos destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

2.3.3. Bien Jurídico protegido.

Pedagógicamente y para fines meramente didácticos y con afán expositivo, y si ser estrictamente precisos, podemos decir que los bienes jurídicos protegidos en los

delitos electrónicos, con la incorporación de estos en los tipos penales de los delitos electrónicos son fundamentalmente.

A) El patrimonio.

En el caso de la amplia gama de fraudes electrónicos, y las manipulaciones de datos a que da lugar.

B) La privacidad, Intimidad, y la confidencialidad de los datos.

En el caso de las agresiones, en forma general, especialmente en los casos de los bancos de datos, y en el espionaje de datos.

C) La seguridad y fiabilidad del tráfico jurídico y probatorio.

En el caso de las falsificaciones de datos probatorios vía medios informáticos.[42]

2.3.4. Conductas ilegales más comunes.

2.4.1 Hackers.

Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas.[43]

El término de hacker en castellano significa "cortador". Las incursiones de los piratas son muy diferentes y responden a motivaciones diferentes, desde el lucro económico a la simple diversión. Los "hackers", son fanáticos de la informática,

[42] Huerta Miranda Marcelo, *Op Cit,* Pág. 118.
[43] Pfaffenberger Bryan, *Diccionario de términos de computación*, Ed. Prentice Hall, México 1999. Pág. 560.

generalmente jóvenes, que tan sólo con una computadora personal, un modem, gran paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, saltándose todas las medidas de seguridad, y leer información, copiarla, modificarla, preparando las condiciones idóneas para realizar un fraude, o bien destruirla. Se pueden considerar que hay dos tipos.

A) Los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad.

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

Un hacker es un Apasionado de la tecnología, de todo tipo, quiere investigar cuanta cosa sale en el mercado. Experto en SO, sistemas de seguridad, programación avanzada, criptología, conocimiento de phreaking.

El hacker puede actuar solo o en grupo, pero generalmente, si se reúnen, es para intercambiar información, no para que los demás miembros le enseñen a hackear.

La rutina para ellos es bajar todo lo que puedan de Internet sobre vulnerabilidad, sistemas operativos, ingeniería social, phreaking, programación), Inventan un nick (sobrenombre), para que los demás los reconozcan, y generalmente no transmiten desde su casa.

2.4.2 Crackers.

Aquel que rompe con la seguridad de un sistema. El término fue acuñado por hacker en 1985, oponiéndose al mal uso de la palabra hacker por parte de la prensa.[44]

[44] *Ibidem*, Pág. 63.

Para las acciones nocivas existe la más contundente expresión, "cracker" o "rompedor", sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender; es decir, presenta dos vertientes.

A) El que se infiltra en un sistema informático y roba información o produce destrozos en el mismo.

B) El que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anti copia.

El cracker tiene como intención destruir. El cracker comete fraudes con tarjetas de crédito, por ejemplo, una persona posee una empresa que vende productos, esos productos pueden ser adquiridos vía web con el uso de una tarjeta de crédito, supongamos que entra un cracker y se apodera de los números de tarjetas de todas las personas que han comprado en ese sitio, el cracker usa la valiosa información que encontró en ese sitio, y piensa en cuanto puede vender esos números.

2.4.3. Phreckers.

Arte y ciencia de Crackear la red telefónica para obtener beneficios personales (por ejemplo llamadas gratis de larga distancia).[45]

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

2.4.4 Viruckers.

[45] *Ibidem*, Pág. 601.

Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o inutilizar la información contenida.[46] Existen dos tipos de virus.

A) Los benignos que molestan pero no dañan.
B) Los malignos que destruyen información o impiden trabajar.

Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

2.4.5. Pirata informático.

Es quien reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor.[47]

Hay que considerar también la piratería como descargar música de Internet, y grabarla en un CD para escucharla, resulta pues que estamos inmersos entre una juventud de "corsarios negros" y cada día hay programas donde se puede descargar gratuitamente el software para descargar la música gratuitamente.

2.4. Conductas que se utilizan para cometer los delitos informáticos.

Podemos decir que son conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física

2.4.1. Cazadores de contraseñas.

Un cazador de contraseñas es un programa que desencripta las contraseñas o elimina su protección.[48] Aunque estos programas no han de desencriptar nada, y

[46] *Ibidem*, Pág. 750.
[47] *Ibidem*, Pág. 599.

además con determinados sistemas de encriptación es imposible invertir el proceso, si no es de forma autorizada. El funcionamiento es el siguiente, escogemos una palabra de una lista, la encriptamos con el protocolo que han sido encriptadas las claves, y el programa compara las claves encriptadas con la palabra encriptada que le hemos dado, si no coincide pasa a otra clave encriptada, si coincide la palabra en texto legible se almacena en un registro para su posterior visualización. Los cazadores de contraseñas que podemos encontrar son: Crack, CrackerJack, PaceCrak95, Qcrack, Pcrack, Hades, Star Cracker, etc. Hay cazadores de contraseñas para todos los sistemas operativos.

2.4.2. Caballos de Troya o Troyanos.

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.[49] Por ejemplo, formatear el disco duro, modificar un fichero, sacar un mensaje, obtener información privilegiada del sistema, etc. Los troyanos, los crean los programadores, ya sea creando, ellos un programa original, e introduciendo el código maligno, o cogiendo el código fuente de otro programa e introduciendo el código maligno, y luego distribuirlo como el original.

2.4.3. Superzapping.

Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de una computadora.[50] El nombre proviene de una utilidad llamada SUPERZAP diseñada para Mainframes y que permite acceder a cualquier parte del ordenador y modificarlo, su equivalente en un PC serían las Pctools o el Norton Disk Editor.

---

[48] *Ibidem*, Pág. 52.
[49] *Ibidem*, Pág. 51.
[50] *Ibidem*, Pág. 722.

2.4.4 Puertas falsas.

Es una práctica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc. con objeto de producir un atajo para ir corrigiendo los posibles errores.[51]

Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas.

2.4.5. Herramientas de destrucción.

Este suele ser el procedimiento de sabotaje mas utilizado por empleados descontentos.

Consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificará la información, o provocará el cuelgue del sistema.[52]

Podemos distinguir cuatro métodos de destrucción: mailbombing, flash bomb, aplicaciones especiales de negación de servicio, y virus.

2.4.6. Mailbombing.

Este método se basa en enviar muchos mensajes de correo electrónico, al mismo usuario, lo cual provoca una gran molestia a dicho usuario.[53]

Las herramientas que existen para estos ataques son: Up Yours, KaBoom, Avalanche, Unabomber, extreme mail, Homicide, Bombtrack, etc. La mayoría de estas aplicaciones suelen ser gratuitas, y tenemos para todas las plataformas.

---

[51] *Ibidem*, Pág. 609.
[52] *Ibidem*, Pág. 565.
[53] *Ibidem*, Pág. 580.

2.4.7. Flash bomb.

Son herramientas que se utilizan en el IRC. Cuando nos conectamos a un IRC, hay varios canales o chats, y cada chat tiene su operador que es la autoridad en ese chat, y decide la persona que ha de marcharse del chat. Las personas expulsadas del chat toman represalias, y apareció el flash bomb. Las aplicaciones de flahs bomb que existen atacan en el IRC de una forma diferente, pero básicamente lo que hacen puede ser es expulsar a otros usuarios del chat, dejar colgado el chat, o llenar de basura (flooding) un canal. Las herramientas que tenemos a nuestra disposición son: crash.irc, botkill2.irc, ACME, Saga, THUGS, o The 7th Sphere.

2.4.8. Aplicaciones de negación de servicio.

Este tipo de ataques trata de dejar colgado o desactivar un servicio de la red saturándolo de información y dejándolo bloqueado, e incluso se obligará a reiniciar la máquina.[54] Las utilidades que podemos encontrar para realizar este tipo de ataques son: Syn_floder, DNSKiller, arnudp100.c, cbcb.c, o win95ping.c.

2.4.9. Ataques asincrónicos.

Este es quizá el procedimiento más complicado y del que menos casos se ha tenido conocimiento. Se basa en las características de los grandes sistemas informáticos para recuperarse de las caídas, para ello periódicamente se graban los datos como volcado de memoria, valor de los registros, etc. de una forma periódica. Si alguien consiguiera hacer caer el sistema y modificar dichos ficheros en el momento en que se ponga de nuevo en funcionamiento el sistema, éste continuará con la información facilitada y por tanto la información podría ser modificada o cuando menos provocar errores.

2.4.10. Ingeniería social.

[54] *Ibidem*, Pág. 15.

Básicamente es convencer a la gente de que haga lo que en realidad no debería, por ejemplo, llamar a un usuario haciéndose pasar por administrador del sistema y requerirle el password con alguna excusa convincente.

2.4.11. Simulación de identidad.

Básicamente es usar un terminal de un sistema en nombre de otro usuario, bien porque se conoce su clave, o bien porque abandonó el terminal pero no lo desconectó y ocupamos su lugar.[55] El término también es aplicable al uso de tarjetas de crédito o documentos falsos a nombre de otra persona

2.4.12. Reciclaje de basura.

Este procedimiento consiste en aprovechar la información abandonada en forma de residuo. Existen dos tipos.

A) El físico.

Se basa principalmente en los papeles abandonados en papeleras y que posteriormente van a la basura, por ejemplo el papel donde un operario apuntó su password y que tiró al memorizarla, listados de pruebas de programas, listados de errores que se desechan una vez corregidos, etc.

B) El electrónico.

Se basa en la exploración de zonas de memoria o disco en las que queda información residual que no fue realmente borrada, por ejemplo ficheros de swapping, ficheros borrados recuperables (por ejemplo, undelete), ficheros de spooting de impresora, etc.

2.4.13. Spooting.

[55] *Ibidem*, Pág. 701.

Mediante este sistema se utiliza una máquina con la identidad de otra persona, es decir, se puede acceder a un servidor remoto sin utilizar ninguna contraseña. ¿Cómo se hace esto? Pues utilizando la dirección IP de otro usuario, y así hacemos creer al servidor que somos un usuario autorizado. En máquinas UNIX se suelen utilizar para estos ataques los servicios "r", es decir, el rlogin y rsh; el primero facilita el procedimiento de registro en un ordenador remoto, y el segundo permite iniciar un shell en el ordenador remoto.

2.4.14. Sniffer.

Un sniffer es un dispositivo que captura la información que viaja a través de una red, y su objetivo es comprometer la seguridad de dicha red y capturar todo su tráfico.[56]

Este tráfico se compone de paquetes de datos, que se intercambian entre ordenadores, y estos paquetes a veces contienen información muy importante, y el sniffer está diseñado para capturar y guardar esos datos, y poder analizarlos con posterioridad. Un ataque mediante un sniffer se considera un riesgo muy alto, ¿por qué?, pues porque se pueden utilizar los sniffers para algo más que para capturar contraseñas, también pueden obtener números de tarjetas de crédito, información confidencial y privada, etc. Actualmente existen sniffers para todas las plataformas, ya que los sniffers se dedican a capturar datos, no computadoras, y por ello es igual la plataforma que se utilice. Algunos sniffers son los siguientes: Gobbler, ETHLOAD, Netman, Esniff. (se distribuye en código fuente), Sunsniff, linux_sniffer.c, etc.

No se si algún día llegaremos a decir "será penado…. con... el que hackea...? ¿Cuándo un hacker llega a configurar una acción delictiva del verbo hackear?..... Hasta ahora no creo que nadie de la respuesta, ya que al momento de elaboración del presente, la Real Academia aún no lo había incorporado.

[56] *Ibidem*, Pág. 708.

CAPITULO III.

DIVERSOS MEDIOS DE PRUEBA EN LOS DOCUMENTOS ELECTRÓNICOS

Entre los principales medios de prueba que se presentan en los juzgados y tribunales se destacan los siguientes: la prueba confesional, documental, pericial, testimonial, de inspección judicial, de fama pública, presuncional.

La prueba documental en particular es la prueba que en última instancia guarda un vínculo mas estrecho con los medios de prueba que tienen que ver con la computadora debido a que los soportes magnéticos pueden constar al igual que un documento.

Documento es el diploma carta o escrito que ilustra acerca de un hecho, en especial de lo sistólicos, o también como escrito, en la que se constan datos fidedignos o susceptibles de ser empleados para probar algo.[57]

En materia jurídica documento es todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica. [58]

De acuerdo con este concepto, son documentos además de los escritos en papel, los planos gráficos, dibujos, fotografías, videos, películas, cintas magnetofónicas, discos informáticos, etc.

El documento, en sentido amplio, es toda representación material destinada e idónea para reproducir una cierta manifestación del pensamiento.[59] De esta manera

[57] *Diccionario De La Real Academia Española*, Barcelona España, 2009 Pág. 76.
[58] Téllez Valdez Julio, *Op cit*, Pág. 243.

los documentos escritos no son, por lo tanto, la única manifestación de prueba documental, por lo que las fotografías, copias fotostáticas, registros, etc. Pueden constituir en última instancia, variedades de prueba documental.

3.1 El documento electrónico.

La evolución tecnológica de los últimos tiempos ha provocado una verdadera conmoción que afecta a todos los ámbitos de la actividad jurídica y comercial, lo que origina nuevas modalidades de contratación y de actos jurídicos. En este sentido, es necesario en la ciencia del derecho hallar las formas y maneras de optimizar las oportunidades que presenta la tecnología, de cara a los medios tradicionales como la del documento en soporte de papel o la firma que pierden utilidad práctica y vigencia. Hoy existe la tecnología suficiente para realizar todo tipo de transacciones por medios electrónicos, por lo que correspondería preguntarse si el sistema jurídico se encuentra capacitado para responder a las nuevas exigencias generadas por la tecnología de la información.[60]

Técnicamente el documento electrónico es un conjunto de impulsos electrónicos que recaen en un soporte de la computadora y que sometidos a un adecuado proceso permiten su traducción al lenguaje natural a través de un pantalla o una impresora. Cabe aclarar que lo que se lee en la pantalla o lo impreso no son los documentos electrónicos originales, sino copias, ya que el original no se podrá utilizar directamente, debido a que su contenido no puede ser percibido por nuestros sentidos.

Sobre este concepto hay una gran discusión en la denominación. Unos los llaman documento electrónico, otro documento digital y finalmente hay quienes, hablan del documento informático.[61]

---

[59]Hidalgo Ballina, Antonio, *Derecho Informático*, 4a. ed. México D.F. Flores Editor y Distribuidor, 2014, p. 334.
[60] Téllez Valdez Julio, *Op cit.* Pág. 246.
[61] *Ibidem* Pág. 247.

3.1.1 Concepto de documento electrónico.

Se puede definir al documento electrónico a aquel lenguaje magnético que constituye la acreditación, materialización o documentación de una voluntad ya expresada en las formas tradicionales, y en que la actividad de una computadora o una red solo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regularización de intereses preexistentes. Se caracteriza porque solo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales.

En pocas palabras el documento electrónico se puede definir como un conjunto de impulso electrónico que recaen en un soporte de computadora y permiten su traducción al lenguaje natural.[62]

Otros opinan que es el dato simplemente, y para otros, "es aquel que se concibe como soporte, vale decir, en cuanto que es la representación pero bajo un criterio material. Representación en forma electrónica de hechos jurídicamente relevantes, susceptibles de ser presentados en forma humanamente comprensible."[63]

3.1.2. Características.

3.1.2.1. Inalterabilidad.

El principal obstáculo para la admisibilidad y eficacia probatoria de los nuevos soportes de información se plantea con relación al carácter de permanente que se menciona como esencial de la definición de documento. El temor sobre la

[62] *Ibid*
[63] Nava Garcés, Alberto E, *Delitos Informáticos*, 2a. ed., Porrúa, México, 2007, p. 187.

posibilidad de reinscripción o reutilización de los soportes informáticos, se dice, disminuye su seguridad y confiabilidad. [64]

3.1.2.2 Autenticidad.

Un documento es auténtico cuando no ha sufrido alteraciones que varíen su contenido, lo que implica decir que la autenticidad esta íntimamente vinculada a la inalterabilidad. Un documento será más seguro cuando mas difícil sea alterallo y sea más fácil de verificarse la alteración que podría haberse producido o reconstruir el texto originario.

3.1.2.3 Durabilidad.

Durable seria toda reproducción indeleble del original que importe una modificación reversible del soporte. Se entiende por modificación irreversible del soporte la imposibilidad de reinscripción del mismo; por indeleble la inscripción o imagen estable en el tiempo y que no puede ser alterada por una intervención externa sin dejar huella. Se dice que el papel es un razonable soporte físico porque no es fácil de alterar, lo que es relativo, ya que no es inalterable y es posible la falsificación de instrumentos. El papel se deteriora e incluso su conservación es problemática por la capacidad de absorción de partículas de polvo.[65]

3.1.2.4 Seguridad.

También se cuestionan los documentos no escritos, con relación a la autenticidad de la representación. Con el desarrollo de claves descifrado y otras medidas criptográficas, el documento electrónico es al menos equivalente al instrumento escrito y firmado sobre el soporte del papel en cuanto a su seguridad.

---

[64] Téllez Valdez Julio, *Op cit.* Pág. 248.
[65] *Ibid.*

El requisito de la firma de las partes es requerido como una condición esencial para la existencia de todo acto bajo forma privada. La firma es un signo personal autógrafo, trazado por la mano del autor que sirve para informar sobre la identidad del autor de la declaración de voluntad, así como del acuerdo de este con el contenido del acto y que luego sirve para probar la autoría. La impresión digitó pulgar, y aunque asimilado con la firma, no la suple legalmente.

Creemos qué en materia de prueba de los actos jurídicos esta noción de autoría por medio de la firma debe ampliarse, incorporando otro medio técnico que asegure la verificación de la autoría atribuida y de la autenticidad de la declaración de voluntad contenida en el documento. Las técnicas de seguridad de los datos basadas en la biometría o las técnicas criptográficas (sistemas de registro y sistema de descifrado literal), brindan similares seguridades. [66]

3.1.3 Clasificación.

Los documentos electrónicos en sentido estricto se encuentran contenidos o escritos en soportes de naturaleza magnética o interna o trasmitidos vía redes telemáticas. Existe una segunda especie de documento electrónico que surge cuando los impresos en forma automatizada provienen de un sistema informatizado, es decir, que ha sido plasmado al papel o llevado a la pantalla de la computadora con información proveniente de un documento electrónico en sentido estricto.[67]

El Documento electrónico es el que esta en la memoria de la máquina y cuyo contenido o texto esta en el lenguaje de la maquina, el que puede ser pasado a lenguaje natural y eventualmente ser impreso para facilitar su utilización y lectura por parte de los usuarios.

De acuerdo con Giannantonio, los documentos electrónicos se clasifican en.

---

[66] *Ibid.*
[67] *Ibidem*, Pág. 250.

A) documento formado por la computadora.

Es cuando la computadora no se limita a materializar una voluntad, una decisión, una regulación de intereses ya formada, sino conforme a una serie de parámetros y datos y a un adecuado programa, decide en el caso concreto el contenido de una regulación de intereses. La computadora no se va limitar a documentar una voluntad externa, si no que determinara el contenido de tal voluntad.

B) Documento formado mediante la computadora.

Este es un caso distinto, pues la computadora documenta una regulación de intereses ya expresados en otras instancias o en otras formas. Aquí su actividad se dirige solo a comprobar y no a constituir.

Son estos últimos los llamados documentos electrónicos en sentido estricto, ya que se encuentra contenido en la memoria central de la computadora, o en la memoria de masa (es decir, en soportes distintos a el y, generalmente externos, como cintas floppy disk, CD rom, etc) y cuya característica común es que no pueden ser leídos por el hombre sino a través de la actuación de una maquina que haga perceptible y comprensible la señal digital de que están constituidos.
También los documentos electrónicos pueden ser distinguidos al grado de su conservación.

I) De carácter volátil.

Como los datos contenidos en las memorias de circuitos RAM (Random Access memory), los cuales se pierden inmediatamente al cortar la energía de la computadora.

II) Permanentes.

Son aquellos contenidos en algunas memorias de masa como discos compactos, cintas, USB y floppy disk de la anterior categoría los datos allí almacenados desaparecen solo al ser borrados, o en caso contrario se mantienen en el tiempo.

III) Inalterables.

Son aquellos que una vez grabados no pueden ser alterados, solo leídos. Dentro de estos encontramos las memorias Ram (read only memory), que consiten en un circuito o chip integrado a la computadora o que se le puede incorporar a la voluntad y los CD rom que son una memoria de masa, contenido en un disco láser.[68]

3.2.3.1. Tipos de soporte informáticos.

Los principales soportes informáticos son.

A) Los soportes magnéticos que almacenan la información digitalmente.

I) El disco duro (hard disk) que viene en el Hardware de la computadora.

II) El disco móvil (disquete), que es intercambiable y fácil de transportar.

B) Los soporte ópticos de lectura láser.

Conocidos como discos compactos y que tienen la ventaja sobre los disquetes que son durables y tienen mayos capacidad de almacenamiento.

C) Los códigos ópticos impresos.

[68] Giannantonio Etore, *El valor jurídico del documento electrónico en informática y derecho,* Ed. Depalma, 1987, Pág. 100.

Los códigos que se conocen como códigos de barras, que se utilizan básicamente en el comercio para leer el precio e identificar el producto.

D) Nuevos dispositivos electrónicos portátiles, como el (USB).

3.2.3.2 Desventajas únicamente de documentos con soporte electrónico.

Las principales desventajas del documento electrónico son.

A) esta escrito en un lenguaje solo comprensible por la computadora.
B) Es descifrable y utilizable solo con el auxilio de la computadora.
C) no se distingue de una eventual copia suya.
D) es fácilmente alterable.
E) Esta desprovisto de toda certeza en orden a su autoría y datación.
F) Se archiva en formatos soportes concretos que no son siempre compatibles con otra computadora [69]

3.2.3.3 Naturaleza del documento electrónico.

El documento se diferencia del soporte o del contenido, en el que el soporte informático es un disco magnético, cinta magnética, disco óptico o tarjeta perforada, es como ya vimos en la composición del documento, el continente, la materialidad.

En cambio, el contenido es aquella información de que da cuenta el soporte, el continente. Cuando los datos ingresan a la máquina quedan registrados y el documento ya ha sido creado. La computadora no forma sino que documenta una regulación de intereses ya expresados de otras formas, la computadora no constituye sino comprueba.

[69] Téllez Valdez Julio *Op Cit* Pág. 252.

Para tener una idea clara de la naturaleza del documento electrónico, es necesario determinar algunos conceptos técnicos que devienen el uso de la computadora, estos son el programa o software, datos o información o dato elaborado.

El programa hace funcionar a la computadora, es el cerebro de la misma, y se puede definir como un conjunto ordenado de instrucciones que actúan entre si para llegar a un resultado final. Estas instrucciones son establecidas previamente por el ser humano en su calidad de programador con el fin de llegar a un resultado. Este objetivo puede ser información o una decisión, aquí es donde debemos tener presente que es el ser humano es quien toma la decisión ya que la máquina por si misma nada hace sino cumplir ordenes explícitas y claras.

Los datos son aquellos elementos que llegan a la computadora por diversos medios y que no son más que la base por medio de la cual llegan a trabajar los diversos programas, convirtiéndolos en información útil. Estos datos pueden tener su origen en la misma o en otra computadora, pero siempre debe tenerse en cuenta que a mano del hombre es la que esta detrás la información es el dato elaborado, es el producto final de la interacción del hombre con la máquina y dicha información puede llegar a plasmarse en una decisión, pero esta siempre tendrá por origen el intelecto humano.[70]

3.2.3.4 Contenido del documento electrónico.

Los documentos electrónicos poseen los mismo elementos que un documento escrito es soporte papel.

A) Constan en un soporte material (cintas, disquetes, circuitos, chips de memorias, redes) sobre el cual se graba el documento electrónico.

[70] *Ibidem* Pág. 253.

B) Contienen un mensaje que esta escrito en el lenguaje convencional de los dígitos binarios o bits, entidades magnéticas que los sentidos humanos no pueden percibir.

C) Están escritos en un idioma o código determinado.

D) Pueden ser atribuidos a una persona determinada en calidad de autor mediante firma digital, clave o llave electrónica.

En conclusión, puede afirmarse que el documento electrónico es información, producto de una interacción hombre-maquina, cuyo origen es el hombre, y que tiene el valor descrito ya que es un mensaje (texto alfanumérico o gráfico) el lenguaje convencional (bits) sobre un soporte material mueble (Cintas o discos magnéticos, discos ópticos, o memorias de circuito.[71]

3.2.3.5 Implicaciones probatorias de los soportes informáticos.

En la actualidad los sectores esenciales de la actividad tanto en el ámbito público como privado están sujetos, en la práctica de sus asuntos y en razón de su clientela o naturaleza de sus actividades, a las reglas judiciales de prueba, (independientemente de la jurisprudencia de que se trata, como sería las redacciones y firma de escritos.

Los soporte informáticos que figuran actualmente a través de documentos como facturas, cheques, letras de cambio, pagarés, etc., realizados por medios computarizados los cuales no obstante ser cada vez mas comunes, enfrentas serias dificultades ya no solo para ser valorados por los jueces, sino siquiera acordados actos los órganos jurisdiccionales respectivos, discutiendo su originalidad en donde radicar dicho elemento) la estabilidad del contenido de

[71] Ruiz Fernando, *El documento electrónico frente al derecho civil y financiero,* publicado en Internet en al sección doctrinal del Derecho. Org.

compromisos que supone un soporte inalterable y aun la misma identificación del autor por medio de la firma, ya que muchos documentos al venir ya impresos con la firma permiten dudar ya no tanto de su identidad sino de su voluntad de compromiso.

Bajo estas consideraciones, no podemos soslayar que el fenómeno de informatización ha provocado un giro en cuanto a los escritos bajo su forma tradicional lo cual altera el funcionamiento normal de las reglas formales del derecho de la prueba.

La redacción de un escrito firmado es una regla de prudencia para todos los convenios importante: una prueba literal esta aquí preparada para toda impugnación eventual. Sin embargo, este tipo de prueba no tiene cabida dentro de la lógica de informatización que tiende a simplificar los compromisos repetitivos que no dan lugar a la redacción de un escrito, (por ejemplo ordenes de giro transmitidos por computadora) así como fijar la información sobre tipos de soportes mas o menos alejados de los escritos tradicionales y difícilmente asimilables por la derecho clásico de la prueba como es el caso de listados, bandas magnéticas, cintas magnéticas, microfichas entre otras.

La manifestación de actos no existentes o no, guarda conformidad a los ordenamientos jurídicos. El derecho de prueba se haya frente a un enorme desafío generado por el desarrollo informático, superior a cualquier otro presentado hasta estos momentos por la tecnología moderna.[72]

3.2.3.6 El documento y la firma electrónica.

El documento electrónico en sentido estricto no tiene firma autógrafa del autor, es un documento que tiene una nueva forma jurídica que no admite la firma de la manera habitual.[73]

[72] Téllez Valdez Julio, *Op Cit* Pág. 255.
[73] Nava Garcés, Alberto E, *Delitos Informáticos*, 2a. ed., Porrúa, México, 2007, p. 98.

Al ser la firma el único requisito esencial para la generalidad de los casos, en principio el sistema del Código Civil permitiría amplia libertad de registro que incluiría los medios electrónicos, siempre que los mismos pudieran ser reproducidos. El mismo principio aplicado al idioma que se utilice, conforme a la total libertad de elección permitida, autoriza el empleo de los idiomas informáticos pero la amplia libertad que tienen las partes en los instrumentos privados respecto del soporte material, queda limitado por la necesidad de que sea firmado por ellas.

3.2 Situación internacional.

En los países en que el nivel de información a arribado a niveles considerables, el problema del valor probatorio de los soportes informáticos a adquirido matices importantes; sin embargo, cabe mencionar que en países como Estados Unidos, Gran Bretaña, Alemania y los países nórdicos, en los que predomina el principio de libertad de prueba, que consiste en otorgar libertad a los juzgadores para determinar los medios de prueba, su eficacia probatoria y la manera de producirlos, el problema no llega a ser tan profundo en aquéllos países como Francia, Bélgica e Italia, fieles al principio de la exigencia legal de la prueba escrita. A pesar de ello, en Gran Bretaña, Australia, Alemania, Austria, Suiza, Suecia y Francia se ha dado lugar a modificaciones que atribuyen en buena acogida a otro tipo de medios de prueba fundamentalmente derivados por la aparición de nuevas técnicas.

Nuevas reglas han permitido a compañías de seguros, bancos, sociedades de crédito y todas aquellas instituciones que requieren archivar numerosos documentos contractuales poderlos remplazar por copias las calidades de durabilidad y de fidelidad al original, por ejemplo el uso de microfichas siempre que no sean susceptibles de modificaciones a nivel de borraduras o enmendaduras. Otra regla versa sobre la no convalidación de soportes magnéticos como pruebas, esto es, que al igual de las copias de calidad insuficiente los soportes magnéticos no se veían reconocidos en cuanto a su valor probatorio; sin embargo, estos pueden valer hasta ahora como si se tratara de elementos de prueba escrita, esto

mas que nada les atribuye un carácter complementario, aunque ello este sujeto a las valoraciones propiamente realizadas por el juez, quien sin un apoyo técnico no permitiría pensar en una ponderación pertinente.

También se menciona la aceptación de nuevos modos de firma, así como la tele transmisión de documentos por digitalización y criptografía, a nivel mundial hay coincidencia respecto de la importancia y necesidad de reconocimiento de validez jurídica al soporte electrónico para que la firma digital adquiera operatividad. La tendencia general sea reconocida por la ley.[74]

3.2.1 Estados Unidos.

En un principio adoptó un sistema menos reglamentarista, regulándose con base a la jurisprudencia emanada de los tribunales, surgiendo así normas federales, como la Uniform Business Records as Ebidence Act y la Uniform Rules of Ebidence, que nos constituían una excepción para la producción en juicio de la prueba con documento electrónico que fue conocida como la Business Records Exception.

El primera el legislar sobre la materia fue el Estado de Utah que el primero de mayo de 1995 sanciono la Utah Digital Signatura Act, implementando un nuevo uso en la autopista informática, ante la ausencia de una ley modelo, esta ley se ha convertido en la referencia obligada para los demás Estados, conformando un sistema regulatorio que brinda efectos legales a la firma digital, un sistema de doble clave que brinda protección, verificación y autenticación a transacciones en línea y decide la intervención de una tercer parte que es la autoridad certificante, la encargada de emitir los certificados indispensables para utilizar el sistema.

Dicha iniciativa fue seguida por la mayoría de los Estados de Estados Unidos que tomaron como modelo tanto esa normativa como la digital Signatura Guidelines,

[74] Tellez Valdez, *Op Cit.* pag, 256.

publicada en octubre de 1995 por The American Bar Association ´s Information Security Committee.

El primero de octubre de 2000 entro en vigor en Estados Unidos, la primera ley nacional sobre firmas digitales. Esta ley concede a la firma digital la misma validez que a la tradicional escrita sobre el papel. [75]

3.2.2 Naciones Unidas (ONU).

Por las dificultades por llegar a un acuerdo internacional respecto de la negociación mediante medios electrónicos, las naciones unidas (a través de la UNCITRAL) se han proclamado a favor de la rápida adecuación de las legislaciones de cada país como medida de carácter más pragmático. Por ello dicho organismo a emitido un valioso documento titulado Legal Value of Computer Records, en el que expresa que las normas concernientes a las pruebas relativas a documentos electrónicos (si bien dicen registros de la computadora) no deben suponer un obstáculo para el uso de las tecnologías emergentes tanto a nivel doméstico como internacional. Señala que las normas redactadas por algunos países deben superar los problemas que genera el lenguaje empleado debido a que incorpora referencias culturales que todavía suponen un freno al desarrollo.[76]

3.2.3 Italia.

La legislación Italiana en esta materia esta conformada por el reglamento de actos, documentos y contratos en forma electrónica, aprobado el 5 de agosto de 1997.

El capítulo primero hace referencia a los principios generales, dando en su artículo primero un conjunto de definiciones de lo que debe de entenderse por documento informático, que es la representación informática de actos hechos o datos

[75] *Ibidem,* Pág. 257.
[76] *Ibid.*

jurídicamente relevantes, por firma digital, el resultado del proceso informático basado en sistema de claves o llaves asimétricas, una pública y otra privada, que permite al firmante a través de la llave privada, y al destinatario, a través de la llave píblica, respectivamente, hacer manifiesta y verificar la proveniencia y la integridad de un documento informático o de un conjunto de documentos informáticos.

Así mismo, define lo que debe entenderse por llave privada llave publica, certificación, mediante la cual se garantiza la correspondencia biunívoca entre la llave publica y el sujeto titular a la que esta pertenecen, se identifica a este ultimo y se declara el periodo de validez de la citada llave; por certificación, el sujeto público privado que efectúa la certificación.

El artículo 5to de este reglamento es acerca de la eficacia probatoria del documento informático, en el sentido de que este con fiemas digitales tiene la eficacia de documento privado y que el documento informático revestido de requisitos previstos en el presente reglamento tiene la eficacia prevista en el articulo 2712 del Código Civil de dicho país.[77]

3.2.4 España.

La legislación española ha prevista en distintas normas la validez del documento electrónico y de las comunicaciones telemáticas como prueba documental.

Asimismo, la jurisprudencia ha reconocido que para los efectos probatorios ha de entenderse por documento escrito, en sentido tradicional, o aquella otra cosa que sin serlo pueda asimilarse al mismo, por ejemplo un disquette, un documento de computadora, un video, una película, etc., con un criterio moderno de interacción de las nuevas realidades tecnológicas, en el sentido de que la palabra documento figura en algunos diccionarios como cualquier cosa que sirve para ilustrar o comprobar algo siempre que el documento tenga un soporte material, que es lo que

[77] *Ibídem, pag*. 258.

sin duda exige la norma penal en la actualidad dicha formula jurisprudencial tiene adecuada correspondencia en la norma contenida en el articulo 26 del nuevo Código Penal según el cual: a los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

En lo que respecta a la firma electrónica, el Real Decreto Ley 14/1999, de 17 de septiembre establece un régimen especifico aplicable a las relaciones telemática. Este régimen persigue básicamente, dotar de seguridad a estas relaciones.[78]

3.3. Situación nacional.

3.3.1. Ley de Mercado de Valores (Diario Oficial de la Federación del 2 de Enero de 1975).

A mediados de los 80 se introdujo un capítulo VIII, referido a la contratación bursátil, introduciéndose por primera ocasión el llamado contrato de intermediación bursátil, por virtud del cual, la casa de bolsa en el desempeño de su encargo actuará conforme a las instrucciones del cliente que reciba el apoderado para celebrar operaciones con el público designado por la propia casa de bolsa, o el que en su ausencia temporal la misma casa de bolsa designe. Se incluyó también la fracción segunda del articulo 91 que señala que a menos que en el contrato se pacte el manejo discrecional de la cuenta, las instrucciones del cliente para la ejecución de operaciones concretas con movimientos de la cuenta del mismo, podrán hacerse de manera escrita, verbal o telefónica, debiéndose precisar en todo caso el tipo de operación o movimiento, así como el genero, especie, clase, emisor, cantidad, precio y cualquier otra característica necesaria para identificar los valores materia de cada operación o movimiento en la cuenta.

[78] *Ibídem, pag 259.*

Lo mas importante para el problema que nos ocupa esta plasmado en la fracción V del artículo 91 en el que se establecen y se consignan lo siguiente. “En caso de que las partes convengan el uso de los medios electrónicos, de computo o de telecomunicaciones para el envio, intercambio y en su caso confirmación de las ordenes y demás avisos que deban darse, habrán de precisar las claves de identificación recíproca y las responsabilidades que conlleve su utilización”.

Las claves de identificación que se convenga utilizar conforme a este artículo sustituirá a la firma autógrafa, por lo que las constancias documentales o técnicas donde aparezcan producirán los mismos efectos que las leyes otorguen a los documentos suscritos por las partes y en consecuencia, tendrán igual valor probatorio.

En los años 90 se introdujo el capitulo X, referido a la automatización, que establece, entre otros, que las casas de bolsa, especialistas bursátiles, bolsas de valores instituciones para el deposito de valores, instituciones calificadores de valores y contrapartes centrales deberán llevarse su contabilidad y el registro de las operaciones en que intervenga, mediante sistemas automatizados (art. 112).
Dichos sistemas deberá reunir de acuerdo con el artículo 113, una serie de características, entre las que se destacan.

A) la compatibilidad técnica de los equipos y programas de Comisión Nacional Bancaria y de los valores.
B) Los asientos contables y registros de operaciones que emanen de dichos sistemas, expresados en lenguaje natural o informático, se emitirán de conformidad a las disposiciones legales en materia probatoria, a fin de garantizar la autenticidad e inalterabilidad de la información respecto a la seguridad del sistema ampliado.
C) El uso de claves de identificación en los términos y loe efectos señalados en el articulo 91, fracción V de dicha ley.

Por ultimo el articulo 116 establece que la información contenida en soportes materiales, o bien proveniente de procesos telemático, siempre que este validada por la autoridad receptora y la entidad emisora, de acuerdo con las características y dentro de los plazos que determine la autoridad, así como la información que cumpliendo con dicho procedimiento se integre a las bases de datos producirán los mismos efectos que las leyes que otorgan a los documentos originales y, en consecuencia, tendrán el mismo valor probatorio.[79]

3.3.2. Reformas legislativas en materia de comercio electrónico.

Cabe destacar las modificaciones al Código Federal de Procedimientos Civiles, que en su artículo 210-A reconoce como prueba "de información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología".

Continua el artículo "para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la confiabilidad del método en que haya sida 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" a su vez el Código de Comercio, en su articulo 1205, establece que.

" Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el animo del juzgador acerca de los hechos controvertidos o dudosos y en su consecuencia serán tomados como prueba las declaraciones de las partes, terceros, peritos, documentos públicos o privados inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, *mensajes de datos* (en donde se incluyen los soportes magnéticos), reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad".

[79] *Ibidem,* Pág., 260.

Finalmente, el artículo 1298-A establece que:

"se reconoce como prueba los mensajes de datos. Para valor la fuerza probatoria de dichos mensajes, se estimará primordialmente la confiabilidad del método en que haya sido generada, archivada, comunicada o conservada".[80]

[80] *Ibidem,* Pág., 261.

CAPITULO IV.

LEGISLACIÓN DE OTROS PAÍSES, EN COMPARACIÓN A NUESTRA LEGISLACIÓN EN MATERIA DE LOS DELITOS ELECTRÓNICOS.

4.1. Tipos de delitos informáticos reconocidos por la Organización de Naciones Unidas (ONU).

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

A) Los Fraudes cometidos mediante manipulación de computadoras.

Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común.

B) La manipulación de programas.

Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas que tienen conocimiento especializados en programación informática.

C) La Manipulación de datos de salida.

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

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

E) Falsificaciones informáticas.

Cuando se alteran datos de los documentos almacenados en forma computarizada.

F) Como instrumentos.

Las computadoras pueden utilizarse también para efectuar falsificación de documentos de uso comercial.

G) 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.

H) Los Virus.

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.

I) Los Gusanos.

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

J) La Bomba lógica o cronológica.

La cual exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

K) Acceso no autorizado a servicios u sistemas informáticos.

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

L) Piratas Informáticos o hackers.

Este acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones.

M) Reproducción no autorizadas de programas informáticos de protección legal.

La cual trae una pérdida económica sustancial para los propietarios legítimos. Los delitos informáticos constituyen una gran laguna en nuestras leyes penales, así pues, el derecho comparado nos permite hacer una lista de los delitos que no están contemplados en el Código Penal y que requieren análisis urgente por parte de nuestros académicos, penalistas y legisladores. Por lo tanto, en este apartado se verá que países disponen de una legislación adecuada para enfrentarse con el problema sobre el particular.[81]

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con este problema.

4.2 Legislación de otros países relacionado con los delitos electrónicos.

[81]Naciones Unidas, *Revista internacional de de Política Criminal. Manual de las Naciones Unidas sobre Prevención del Delito y Control de Delitos Informáticos*., 2008, p 43.

4.2.1 Alemania.

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan las siguientes formas típicas del delito.

Espionaje de datos (202 a);

Estafa informática (263 a);

Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).

Alteración de datos (303 a) es ilícito, cancelar, inutilizar o alterar datos inclusive la tentativa es punible.

Sabotaje informático (303 b). Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

Utilización abusiva de cheques o tarjetas de crédito (266 b).

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial , en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos

incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.[82]

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los Países Escandinavos y en Austria.

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma calificada.

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

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

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

[82] Téllez Valdez, Julio, *Derecho Informático, 4a. ed.* McGraw-Hill, México 2009, p. 282 .

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

4.2.2 Estados Unidos.

En el marco Federal Estados Unidos desde por lo menos 1986 contaba con la *Federal Abuse and Fraud Act (Acta Federal de Fraude y Abuso),* que brindaba un marco legal para defenderse de los delitos informáticos. Sin embargo en 1994 adopto la *Fraud and Related Activity in Connection With Computers (Acta Federal de Fraude y Actividades relativas a las Conexiones con la Computadora*), (18 U.S.C. Sec.1030) que modificó al Acta Federal de Fraude y Abuso de 1986.[83]

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

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

[83] Soto Alberto, Argentina: Delitos informáticos, consultable en: http//www.alfaredi.org/revista/data/52-3.asp.

Me llama la atención que el Acta de 1994 aclara que el creador de un virus no debe escudarse, en el hecho que no conocía, que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

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

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

Consideramos importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10, 000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos, etcétera.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Así mismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas usualmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

4.2.3 Francia.

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

Acceso fraudulento a un sistema de elaboración de datos(462-2).- En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

Sabotaje informático (462-3).- En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos (462-4).- En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados (462-5).- En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

4.2.4 Italia.

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

A) Acceso Abusivo.

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

B) Abuso de la calidad de operador de sistemas.

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

C) Introducción de virus informáticos.

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

D) Fraude Informático.

Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un injusto beneficio, ocasionando daño a otro. También se entiende como tal la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en

ellos contenidos o pertenecientes a ellos, cuando se procure una ventaja injusta, causando daño a otro. La punibilidad de este tipo de delito es de meses a tres años de prisión, más una multa considerable.

E) Intercepción abusiva.

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

F) Falsificación informática.

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

G) Espionaje Informático.

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

H) Violencia sobre bienes informáticos.

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

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

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

4.2.5 España.

Dentro del Código Penal Español de 1995, se contiene un catalogo de delitos informáticos muy amplio para sancionar aquellas conductas que atentan diversos bienes jurídicos.

A) Ataques que se producen contra el derecho a la intimidad.

Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o sopotes informáticos. (Artículos del 197 al 201 del Código Penal).

B) Infracciones a la propiedad intelectual a través de la protección de los derechos de autor.

Especialmente la copia y distribución de la copia no autorizada de programas de computadora y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (articulo 270).

C) Falsedades.

Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de la moneda a las tarjetas de débito y crédito.

Fabricación o tenencia de programas de computadora para la comunicación de delitos de falsedad. (Artículos 386 y ss. Del código Penal).

Sobre el particular debemos recalcar que el código penal español es aplicable en todo su territorio, por lo que la persecución del delito en comento es más efectiva para los delitos como el señalado con anterioridad.

D) sabotajes informáticos.

Delitos de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Articulo 263).

El delito anterior en nuestro concepto, no es sino una variante o modalidad del daño en propiedad ajena.

E) Fraudes informáticos.

Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (articulo 248 y ss. Del código penal).

F) Amenazas.

Realizadas por cualquier medio de comunicación. (articulo 169 y ss. Del código penal).

G) Calumnias e injurias.

Cuando se propaguen por cualquier medio de eficacia semejante a la impresión o la radiodifusión. (artículo 205 y ss. Del código penal).

H) Pornografía infantil.

Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.
La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. Articulo 187.[84]

4.2.6 Argentina.

El tratadista Gabriel Andrés Campoli, la legislación Argentina sobre los delitos informáticos se detuvo esencialmente en el debate conceptual: “por medio de “ y “en contra de “. Y en efecto, esta discusión se repite desde que se realiza una clasificación.

Campoli escribe: se observa que solo los equipos dotados de la capacidad de procesar dotados pueden ser por regla general ser utilizados como medios comisivos de acciones que afecten bienes jurídicos que a la sociedad le puede interesar brindarle mayor protección (la penal).

¿Entonces que es lo que nos separa de una correcta aplicación de las leyes penales preestablecidas?

Solo la pretendida falta de legislación en materia de delitos informáticos, y digo pretendida porque esto no es así, ya que al perpetrarse el delito a través del uso de medios informáticos no se están sino en presencia de un nuevo método comisivo del delito y no como erróneamente se piensa de un nuevo delito que para lo que

[84] Nava Garcés Alberto Enrique, *Op Cit*, Pág. 92.

sea debe de estar correctamente tipificado, en resumen, los delitos informáticos, en su gran mayoría dependen para su persecución penal de la correcta interpretación de la ley penal y de la toma de conciencia por parte de los jueces de que solo nos encontramos ante nuevos métodos para estafar o para injuriar, pero en ningún caso ante nuevos delitos, ya que una postura semejante nos llevaría al absurdo de pensar, por ejemplo que si mañana se pudiese quitar la vida a alguien por medio de Internet habría de establecer una nueva figura penal ya que el homicidio no estaría cubriendo esta posibilidad; cuando el derecho, si se lesiona el bien jurídico protegido no importa cual sea el medio utilizado, corresponde la aplicación de la ley penal vigente y no se requiere una nueva y específica.[85]

La urgente necesidad de combatir a la delincuencia informática hizo que algunos tratadistas como Campoli, desestimaran las características de las conductas que ahora tratamos, tomando o recomendado medidas radicales, pero, nuevamente insuficientes. Etéreo de la prueba la extraterritorialidad del acto y la posibilidad de dilatar o programar la lesión jurídica.[86]

4.3 Legislación Nacional.

Para el desarrollo de este capítulo se analizará la legislación que regula, administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos en este entendido, consideramos pertinente recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte en virtud de que el artículo 133 constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

4.3.1 Tratado de libre comercio de América del Norte (TLC).

[85] Campoli Gabriel Andrés, Argentina: *Hacia una correcta hermenéutica penal delitos informáticos vs. Delitos electrónicos,* consultable en: http://www.alfa-redi.org/revista/data/50-10.asp.
[86] Nava Garcés, *Op Cit*, Pág. 87.

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la 6ª parte capítulo XVII.[87] En el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

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

De esta forma, debe mencionarse que los tres Estados, Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714)[88]. A fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta, que se incluye en el presente trabajo, debe destacarse el contenido del párrafo 1 del artículo 1717.[89] Titulado: Procedimientos y sanciones penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

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

---

[87] Tratado de Libre Comercio de América del Norte, I Texto Oficial, Ed. grupo editorial Miguel Ángel Porrua, México 2002, Pág. 483.
[88] *Ibídem*, Pág. 502.
[89] *Ibídem*, Pág. 508.

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

Llama la atención que en su párrafo 2 habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que éstos consten en medios electrónicos o magnéticos.

4.3.2 Ley Federal Del Derecho de Autor y Código Penal Federal.

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

Sobre el particular, y por considerar de interés el contenido de la exposición de motivos cuando esta ley se presentó ante la Cámara de Diputados, a continuación se presentan algunos comentarios pertinentes respecto a los elementos que deben contemplarse en la atención a la problemática de los derechos de autor en nuestro país.

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

Además, se consideró que debido a que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de Decreto de Reforma al Código Penal Federal, proponiendo la adición de un título Vigésimo Sexto denominado "De los delitos en materia de derechos de autor".

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

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

En este sentido, consideramos importante detenernos en los artículos 102 y 231 de la Ley Federal de Derechos de Autor. El primero de ellos, regula la protección de los programas de computación y señala además que los programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos. El segundo en su fracción V sanciona el comercio de programas de dispositivos o sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo.

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

Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, Artículo 424 bis, fracción II del Código Penal Federal del que se infiere la sanción al uso de programas de virus.

Por otra parte, el artículo 104 de dicha ley se refiere a la facultad del titular de los derechos de autor sobre un programa de computación o sobre una base de datos, de conservar aún después de la venta de ejemplares de los mismos el derecho de autorizar o prohibir el arrendamiento de dichos programas.

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

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

Además, la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su artículo 215 al Título Vigésimo Sexto del Código Penal citado, donde se sanciona con multa de 300 a 3 mil días o pena de prisión de seis meses hasta seis años al que incurra en este tipo de delitos, específicamente en el articulo 426. Sin embargo, la regulación existente no ha llegado a contemplar el delito informático como tal, sino que se ha concretado a la protección de los derechos autorales y de propiedad industrial, principalmente.

Tal y como hemos sostenido, México no está exento de formar parte de los países que se enfrentan a la proliferación de estas conductas ilícitas. En ocasiones, la prensa a publicado notas en las que se ha informado sobre las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que se

remontan a un valor de mil millones de dólares por concepto de piratería de estos programas.

Esto, a la larga podría traer implicaciones muy desventajosas para México, entre las que podemos citar, la pérdida de prestigio a nivel internacional por el actuar ilícito de empresas cuyo radio de acción no está reducido al ámbito nacional y la pérdida de credibilidad por parte de las compañías proveedoras de programas informáticos, lo que se traduciría en un mercado poco atractivo para ellas, que pondrían al país en una situación marginada del desarrollo tecnológico.

En este entendido, consideramos que por la gravedad de la conducta ilícita en sí, y las implicaciones que traería aparejadas, justifica su regulación penal.

En otro orden, el Artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que los individuos inescrupulosos pueden hacer con esta información. Así, el acceso no autorizado a una base de datos de carácter personal de un Hospital de enfermos de SIDA puede ser utilizado contra estas personas quienes a causa de su enfermedad, se encuentran marginados socialmente, en la mayoría de los casos.

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

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

Por otra parte, debe mencionarse que en abril de 1997 se presentó una reforma a la fracción III del artículo 231 de la Ley Federal del Derecho de Autor así como a la fracción III del artículo 424 del Código Penal Federal.

De esta forma, las modificaciones a la ley autoral permitieron incluir en su enunciado la expresión "fonogramas, videogramas o libros", además del verbo "reproducir", quedando.

Art.231 fracción III Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta Ley".

Con las reformas al Código Penal se especifica que:

"Art.424 BIS fracción.- I A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende, copias de obras, fonogramas, viedogramas o libros protegidas por la Ley Federal del Derecho de Autor en forma dolosa, a escala comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos"

Sobre el particular, debe mencionarse que durante la modificación a la Ley en diciembre de 1996 se contempló parcialmente lo que se había acordado en el TLC y que por tal razón fue necesaria una segunda modificación, en abril del año en curso 2008, para incluir la acción de "reproducción".

De igual forma el artículo 424 que había sufrido una modificación en diciembre de 1996, fue reformado en su fracción tercera en abril del 2008, pasado para incluir la reproducción y su comisión en una forma dolosa.

Quedando el Código Penal Federal, actual de la siguiente manera:

Artículo 167.- Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:

VI.- Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos;

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.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad

pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

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.

CÓDIGO PENAL FEDERAL

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN

Secretaría General

Secretaría de Servicios Parlamentarios

Última Reforma DOF 14-03-2014

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

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, sele 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 delas 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.

Los tipos penales anteriormente citados concuerdan con los planteados en países como España, Italia, Alemania, entre otros, mismos que hemos analizado en capítulos anteriores, respecto a ciertos elementos comunes aplicados a la protección de los sistemas de información de uso del Gobierno.

Por ultimo un avance significativo en materia de Propiedad Intelectual. Se encuentran tipificadas conductas como producción, reproducción, a través de sistemas de información, conductas llevabas a acabo mediante delitos como la piratería, entre otros.

4.3.3 Código Penal y de Procedimientos Penales del Estado de Sinaloa.

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo

"Delitos contra el patrimonio"

Capítulo V

Delito Informático.

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

Use o entre a una base de datos, sistemas 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 Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte

lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

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

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

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

4.3.4 JURISPRUDENCIA Y TESIS AISLADAS

Debido al avance constante y sobre todo veloz de la tecnología, así como las consecuencias que con ello conlleva para la aparición de nuevas formas de cometer delitos a través de esta, es necesario crear instrumentos legales para la defensa de estas conductas o medios que de manera general que permitan la protección del daño o menoscabo en nuestro patrimonio o persona, mientras esto no suceda seguirán emitiéndose jurisprudencias y tesis aisladas que ayuden a ocultar las deficiencias de la legislación en materia de delitos informáticos.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL CUARTO CIRCUITO.[90] FRAUDE COMETIDO MEDIANTE EL USO DE

COMPUTADORAS. Si el inculpado asentó en la computadora instalada en el banco un depósito ficticio para ser abonado en la cuenta de ahorros que abrió a nombre de su coacusado, es evidente que el empleo de la computadora por el inculpado resultó un medio de comisión del fraude en esta época de la electrónica, pues al crear una falsa concepción de la realidad, con el propósito de alcanzar un beneficio económico, determinó la existencia del engaño constitutivo de dicho delito.

TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO.[91] PRUEBA DE INSPECCIÓN. DEBE DESECHARSE CUANDO LOS PUNTOS PROPUESTOS PARA SU DESAHOGO PUEDAN SER COMPROBADOS A TRAVÉS DE LA DOCUMENTAL, ENTENDIDA COMO LA INFORMACIÓN GENERADA O COMUNICADA QUE CONSTE EN MEDIOS ELECTRÓNICOS O EN CUALQUIER OTRA TECNOLOGÍA, QUE PUEDE SER REPRODUCIDA, NO SOLAMENTE EN PAPEL SINO TAMBIÉN EN ALGÚN DISQUETE O DISCO
ÓPTICO. La base de datos existente en el sistema de cómputo de alguna dependencia oficial, constituye, en sentido amplio, una documental, atendiendo a que el artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, por disposición de su artículo 2o., segundo párrafo, señala que se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIAS PENAL Y ADMINISTRATIVA DEL VIGÉSIMO PRIMER CIRCUITO.[92] INFORMACIÓN PROVENIENTE DE INTERNET. VALOR PROBATORIO. El artículo 188 del
Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, en términos de lo previsto en el diverso artículo 2o. de este ordenamiento legal, dispone: "… reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en

cualquiera otra tecnología; ahora bien, entre los medios de comunicación electrónicos se encuentra "internet", que constituye un sistema mundial de diseminación y obtención de información en diversos ámbitos y, dependiendo de esto último, puede determinarse el carácter oficial o extraoficial de la noticia que al efecto se recabe, y como constituye un adelanto de la ciencia, procede, en el aspecto normativo, otorgarle valor probatorio idóneo.

TERCER TRIBUNAL COLEGIADO DEL QUINTO CIRCUITO.[93] INTERNET. ES UNA MEDIDA PERTINENTE PARA INVESTIGAR EL DOMICILIO DE LA TERCERA PERJUDICADA SI SE TRATA DE UNA EMPRESA CUYOS DATOS

SE LOCALICEN POR ESE MEDIO. Según la fracción II del artículo 30 de la Ley de Amparo, si no consta en autos el domicilio del tercero perjudicado, la autoridad que conozca del amparo dictará las medidas que estime pertinentes para investigar su domicilio. "…Por su parte, el artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, reconoce como prueba la información generada o comunicada a través de medios electrónicos.." Por lo tanto, una de las medidas pertinentes que puede dictar la autoridad federal para localizar el domicilio de la parte tercera perjudicada, si se trata de una empresa cuya localización no conste en autos, es la de efectuar su búsqueda por internet a través de las diversas páginas que ofrecen dicho servicio, donde basta introducir el nombre de la empresa que se pretende localizar y en breve se despliega información de la que puede obtenerse la forma para contactar con dichas empresas y en algunos casos también proporcionan sus domicilios.

SÉPTIMO TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO.[93] REVELACIÓN DE SECRETOS. EL DELITO PREVISTO EN EL ARTÍCULO 211 BIS DEL CÓDIGO PENAL FEDERAL, ES DE PELIGRO Y DE

RESULTADO. Del citado precepto se advierte que el delito de revelación de secretos corresponde a una mezcla de la categoría de los denominados delitos de peligro, en una parte, y en otra, se inscribe dentro de la clase de los de resultado, ya que el elemento normativo "o en perjuicio de otro", se establece como disyuntiva del también elemento normativo "indebidamente"; lo cual significa que a falta de éste, para que se configure el delito, debe darse aquel requisito de perjuicio como necesaria existencia de un daño, de un menoscabo o detrimento en los bienes morales o materiales del ofendido, por revelación, divulgación o utilización de la información o imágenes obtenidas en una intervención de comunicación privada. Es decir, se considerará conducta ilícita el solo hecho de revelar, difundir o utilizar indebidamente la información, pero también se admite como ilícito una forma de comisión material, al prever el posible perjuicio a alguien por dicha conducta.[94]

REVELACIÓN DE SECRETOS. EL ARTÍCULO 211 BIS DEL CÓDIGO PENAL FEDERAL QUE TIPIFICA ESE DELITO, NO VIOLA LA GARANTÍA DE EXACTA APLICACIÓN DE LA LEY PENAL CONTENIDA EN EL TERCER PÁRRAFO DEL ARTÍCULO 14 DE LA CONSTITUCIÓN FEDERAL. Conforme a la garantía de exacta aplicación de la Ley Penal prevista en el citado precepto constitucional. "… En congruencia con lo anterior, el artículo 211 bis del Código Penal Federal, al tipificar el delito de revelación de secretos señalando que a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada … no viola la citada garantía constitucional en virtud de que el vocablo "indebidamente", empleado en dicho precepto legal, no provoca confusión; en primer lugar, porque es posible precisar su significado a través de su concepto gramatical y, en segundo, porque su sentido puede fijarse desde el punto de vista jurídico y determinar cuándo la conducta es indebida para poder considerarse delictuosa…"[95] .

El material resulta insuficiente, si bien en cuanto a criterios

jurisprudenciales ha existido un avance vertiginoso, la legislación de la materia aplicable no cuenta con tal denominación respecto al tema.

[90]Queja 39/2005. Cervezas Cuauhtémoc Moctezuma, S.A. de C.V.. Ponente: José Carlos Rodríguez Navarro. Secretaria: Rebeca del Carmen Gómez Garza. 4 de mayo de 2005. Unanimidad de votos.

[91]Amparo directo 344/78. Rogelio Mendoza Reséndiz. . Ponente: Víctor Manuel Franco. La publicación no menciona la fecha de resolución del asunto. Unanimidad de votos.

[92] Queja 39/2006. Inversiones Raf, S.A. de C.V Ponente: Martiniano Bautista Espinosa. Secretario: Mario Alejandro Nogueda Radilla. . 29 de junio de 2006. Unanimidad de votos.

[93]Queja 19/2009 Disidente: Manuel Ernesto Saloma Vera. Ponente: Julio César Vázquez-Mellado García. Secretario: Benjamín Garcilazo Ruiz. 21 de mayo de 2009. Mayoría de votos.

[94]Amparo en revisión 534/2005. Ponente: Juan N. Silva Meza. Secretario: Manuel González Díaz. 22 de junio de 2005. Cinco votos.

[95] Amparo en revisión 534/2005. Ponente: Juan N. Silva Meza. Secretario: Manuel González Díaz. 22 de junio de 2005. Cinco votos.

Situación alarmante toda vez que, atendiendo a los principios generales del derecho *“Nullum crimen sine lege”, “Nulla poena sine crimine”* estas conductas ilícitas se llevan a cabo al margen de la ley, y no pueden ser penalizadas en su totalidad como un conjunto de acciones tendientes a la producción del delito mediante conductas dolosas creadas por agentes que cuentan con un conocimiento especializado del tema.

Es indispensable dar al tema la importancia jurídica correspondiente, ya que con los insuficientes criterios jurisprudenciales anteriormente citados, no es posible cubrir la totalidad de los casos que a diario se presentan y de los cuales existe una casi nula incidencia de denuncia, porque no pueden ser formalmente punibles, toda vez, que la ley no los contempla, aunado al desconocimiento de la gente en la materia y la poca denuncia de estos delitos realizados a través de los medios informáticos en mención.

CONCLUSIÓN.

Las nuevas tecnologías cada vez se van implantando más en nuestra sociedad, hasta el punto de que se ha hecho indispensable para determinadas tareas de vital importancia el uso de la informática y las telecomunicaciones, y además proporcionan un gran servicio a toda la sociedad.

Las redes de telecomunicaciones como Internet han generado un submundo, en el que los delitos son difíciles de perseguir, debido a la propia naturaleza del entorno y a la falta de tipificación de las modalidades de comisión y de los medios empleados. Entre los delitos, infracciones administrativas y malos usos, que se pueden llevar a cabo en la infraestructura de la información, en estos momento es casi imposible y tal como están dadas las cosas, llegar a una descripción cerrada de estas conductas delictivas, por cuanto Internet es algo absolutamente dinámico, (es uno de los hechos más importantes de los últimos tiempos), en que su progreso debe contarse por horas ya que sufre cada segundo una modificación continua que el avance tecnológico le imprime a sus mecanismos.

No es fácil formular un catálogo de conductas, por cuanto las mismas continuamente se van perfeccionado, o se van modificando surgiendo otras nuevas. Por eso en Internet, las técnicas para llegar a realizar este tipo de conductas son prácticamente inagotables.

El único hacedor de la ley penal, entiéndase el legislador, conforme con nuestro principio de legalidad, podría llegar a expresar concreta concisa y lo más claramente posible conductas que sean penalizadas.

Se requiere un arduo esfuerzo, que para emprenderlo es necesaria una previa y exhaustiva investigación de los hechos que componen la mayoría de casos, donde ya se habla de millonarios perjuicios de orden económico y de delitos de "guante virtual" terminología que se ha manejado en Seminarios de España, y destaco, que Europa está mucho más adelantado, respecto de este tema, que América y por ende nuestro país.

El dinamismo, que comprende el tráfico en la red se torna sumamente difícil aunque casi imposible delimitar conductas penales para lo cual, se requeriría de crear una policía o una fuerza altamente especializada en la detección de este tipo de conductas criminales.

PROPUESTA.

Consiste en la inclusión en el Código Penal Federal, los delitos electrónicos que observamos en nuestro trabajo.

Cabe señalar que esta propuesta propone incluir los delitos electrónicos, en el Código Penal Federal debido a que estos tienen que ver con ataques a las vías de comunicación, considerados estos como delitos Federales.

Esta propuesta tiene como objeto solo incluir los delitos electrónicos, sin el afán de abrogar, ni derogar, ningún artículo mencionado en dicha legislación. Solo incluir o complementar, en base al estudio reflejado en el presente trabajo, y a las legislaciones comparadas en nuestro estudio, y diferentes propuestas, que se han realizado, en nuestro país.

Añadir al código penal federal las siguientes propuestas:

TITULO QUINTO

Delitos en Materia de Vías de Comunicación y Correspondencia

CAPITULO I

Ataques a las vías de comunicación y violación de correspondencia

Capitulo II Violación a la correspondencia.

III Al que abra indebidamente una comunicación escrita, o la ejerce a través de medios electrónicos, electromagnéticos u ópticos, que no este dirigida a el.

TITULO VIGESIMO SEGUNDO
Delitos en Contra de las Personas en su Patrimonio

CAPITULO III
Fraude

Capitulo III Fraude.

Articulo 389 ter. Comete el delito de fraude y se sancionará con prisión de tres meses a diez años y multa de treinta a doscientos cincuenta días multa, al que en calidad de usuario, intermediario, empresa proveedora de información, banco, o cualquier empresa comercializadora, utilice el intercambio electrónico de datos para obtener con engaños ganancias indebidas d, como dinero, valores, o cualquier otra cosa aprovechándose de su acceso a los sistemas de redes computacionales, adquiriendo, enajenando, trasfiriendo depositando, o dando en garantía productos y servicios de toda índole.

Capitulo VIII Delitos Informáticos.

Articulo 390. Se aplicara la pena de prisión de dos a cinco años, y de cien a trescientos días de multa al que:

I. Sin estar autorizado, se apodere, altere, utilice o modifique, en perjuicio de un tercero, datos reservados de carácter personal, familiar o de negocios que se hallen registrados en ficheros, programas, códigos, comandos, soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro publico o privado.

II. Difunda, revele o ceda a terceros los datos o hechos descubiertos o las imágenes captadas a que se refiere el apartado anterior.

III. Con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realice la conducta descrita en el párrafo anterior.

IV. **Teniendo la calidad de encargado o responsable de los ficheros, programas, códigos, comandos o soportes informáticos, electrónicos o telemáticos archivos o registros, incurra en lo descrito en los apartados I y II, se le impondrá la pena de prisión de tres a seis años de prisión.**

V. **Afecte con los hechos descritos en los apartados anteriores datos de carácter personal, que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la victima fuere un menor de edad o una persona con discapacidad, se impondrán las penas de cuatro a siete años de prisión.**

VI. **Realice los hechos descritos de la fracción primera a la tercera con fines lucrativos, se impondrán penas de cinco a diez años de prisión.**

VII. **Siendo proveedor de acceso al Internet, que proporcione servicios informativos que contengan material apto sólo para mayores de edad, o que puedan afectar la integridad de la familia, o herir la sensibilidad de algún sector de la población, omita identificarse totalmente, influyendo nombre o razón social, domicilio, y numero telefónico, y no especifique claramente en su pagina de entrada la siguiente advertencia: "esta página contienen materiales aptos solo para adultos, si usted tiene menos de dieciocho años deberá salir de esta página, si usted es un adulto que esta interesado en evitar que menores de edad que manejen su equipo de cómputo tengan acceso a estas páginas, póngase en contacto con el proveedor de la información para su cancelación".**

VIII. **Siendo proveedor de acceso a Internet, solicite de los usuarios el derecho de uso de sus datos personales para determinados fines como inscripción para obtener un servicio, o comprar o vender un producto, los utilice para fines.**

FUENTES DE CONSULTA.

DOCTRINA.

NAVA GARCES. ALBERTO E. *Delitos informáticos, 2a* edición, México*.,* Porrúa.

NAVA GARCES. ALBERTO E. *Análisis de los delitos informáticos, 1a* edición, México*.,* Porrúa.

MOLINA SALGADO, Jesús Antonio Delitos y otros ilícitos informáticos en el derecho de la propieda industrial, 1a. edición, Porrúa, México.

HIDALGO BALLINA, Antonio, *Derecho Informático,* 2a edición, Flores Editor, México.

AMUCHATEGUI REQUENA, Griselda, *Derecho Penal*, 3ª Edición, México, Oxford University Press, 2010.

ANDRÉS CÁMPOLI, Gabriel, *Derecho penal informático en México*, México, INACIPE, 2004.

TÉLLEZ VALDÉS, Julio, *Derecho Informático*, 3ª. Edición, México, McGraw-Hill, 2004.

CASTELLANOS Tena, Fernando, *Lineamientos Elementales de Derecho Penal*, Cuadragésima edición, México, Editorial Porrúa, 2003.

DÍAZ-ARANDA, Enrique, *Derecho Penal Parte General*, 2ª Edición, México, Editorial Porrúa, 2004.

PALAZZI PABLO, Andrés, *Delito Informático*, Buenos Aires Argentina, Editorial Ad Hoc S.R.L. 2000.

LEGISLACION.

Exposición de Motivos de la Comisión de Justicia de la Cámara de Diputados Doc,184/LVI/96(I.P.O. Año III) DICT. Durante el Análisis de la Ley Federal del Derecho de Autor.

Ley Federal del Derecho de Autor, Diario Oficial de la Federación, Martes 24 de Diciembre de 1996.

Leyes Federales de México, Cámara de Senadores del H. Congreso de la Unión, Ley Federal del Derecho de Autor, México 2007.

Tratado de Libre comercio (TLC). Diario oficial de la Federación, Lunes 20 de Diciembre de 1993.

Delitos informáticos Legislación y capacidad de ejecución de proyectos de construcción 3 ª Conferencia de Expertos y el Seminario de Capacitación, APEC de Telecomunicaciones y el Grupo de Trabajo de Información, 32 ª reunión, 5-9 de septiembre de 2005, Seúl, Corea.

FUENTES ELECTRONICAS.

http//www. aba.org.ar/bi151303.htm.

http://www.alfa-redi.org/revista/data/50-10.asp.

http//www.alfaredi.org/revista/data/52-3.asp.

http://www.analitica.com/bitblioteca/roberto/teoria.asp#superautopista.

http://www.bma.org.mx

http://www.camaradesenadores.gob.mx

Hernández Montoya consultable en http://www.analitica.com/bitblioteca/roberto/teoria.asp#superautopista.

http://www.librado.50megs.com/Delito_Intimidad.htm.

http://www.juridicasunam.mx

http://www.ordenjuridico.gob.mx

http://www.scjn.gob.mx

http://www.todoelderecho.com

http://www.unam.mx

http://www.wto.org