UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES "ARAGÓN"

LA NECESIDAD DE REFORMAR EL CÓDIGO PENAL FEDERAL ANTE LOS DELINCUENTES INFORMÁTICOS.

T E S I S

PARA OBTENER EL TÍTULO DE :
LICENCIADO EN DERECHO
P R E S E N T A :

RAFAEL AUGUSTO HUERTA LARA

ASESOR:

MAESTRA MA. GRACIELA LEÓN LÓPEZ

BOSQUES DE ARAGÓN, ESTADO DE MÉXICO 2005

DEDICO LA PRESENTE TESIS
A MIS PADRES
RAFAEL AUGUSTO HUERTA GUZMÁN
Y TERESA LARA.

Por su gran apoyo y guía para la
culminación de mis estudios
profesionales.

A MI ESPOSA
PATRICIA AHUATZIN LÓPEZ

Por su cariño y apoyo que me ha servido
para la realización de todos
mis proyectos.

A MIS HERMANOS:
IVONNE, CARLOS Y TERESA

Deseando que sus proyectos personales
se hagan realidad.

A MI ASESORA
LA MAESTRA MARÍA
GRACIELA LEÓN LÓPEZ

Por ser una guía para cualquier
persona del concepto de
la superación personal, el empeño
y la constancia.

A MIS SUPERIORES
JERÁRQUICOS Y AMIGOS
JOAQUÍN VELÁZQUEZ GARCÍA DE
LEÓN Y LEOPOLDO MARTÍNEZ
BAUTISTA.

Por ser un gran ejemplo en la
Procuraduría General de Justicia
Del Distrito Federal.

A MIS AMIGOS:
FERNANDO RENÉ CASTILLO PATT,
GERMÁN ALEXANDER CENTENO,
ALEJANDRINA LUNA ORTEGA,
LEYVER RAMÍREZ SANDOVAL Y
GUADALUPE MORALES

Por su desinteresada amistad
y el apoyo moral que
me han brindado en la realización
de mis proyectos.

LA NECESIDAD DE REFORMAR EL CÓDIGO PENAL FEDERAL ANTE LOS DELINCUENTES INFORMÁTICOS.

ÍNDICE

CAPITULO IV
ANTECEDENTES DEL INTERNET Y LAS PRINCIPALES CONDUCTAS DELICTIVAS.

CAPÍTULO V
EL DELITO INFORMÁTICO EN EL DERECHO COMPARADO.

LA NECESIDAD DE REFORMAR EL CÓDIGO PENAL FEDERAL ANTE LOS DELINCUENTES INFORMÁTICOS.

INTRODUCCIÓN.

El avance tecnológico y el uso de las nuevas tecnologías, en específico el uso de las computadoras actuales trae consigo no solo la comodidad, la facilidad para realizar varias de las actividades humanas, desde la organización de las actividades, el trabajo y hasta la diversión, sino también trae consigo problemas de índole jurídico, surgidos por el uso de tales tecnologías, pues ya sea por curiosidad propia del ser humano de experimentar o descubrir mediante el uso de la computadora las actividades que cada usuario puede realizar que de cierta manera no son permitidas o por violar las normas de seguridad de un programa, o bien con la firme intención de causar un daño o un perjuicio, se ocasionan conductas que perjudican a alguna persona en específico, grupo de personas, corporaciones y hasta los órganos de Gobierno, sin ser en la actualidad algunas de éstas conductas contempladas en nuestros códigos penales, algunos locales y en el federal vigente como un delito, pues la definición que señalan los mismos es un tanto limitativa y no abarca todas las posibles conductas de éste tipo, aunado ello, que el afectado en éstas situaciones prefiere no poner en conocimiento las mismas, a fin de no dar a conocer la vulnerabilidad y fragilidad de sus sistemas informáticos.

La realización del presente trabajo de tesis tiene como objetivo dar a conocer los problemas que con el uso de las computadoras se pueden realizar, así como

poner de manifiesto la ausencia de una normatividad adecuada a fin de que éstas conductas sean consideradas como delito, originando así la impunidad de las personas que realizan éstos actos, y a quienes se les denomina de diversas maneras, tales como delincuente informático, Hacker, Cracker, peacker, blue hacker, etcétera o múltiples nombres que han sido adoptados mediante el uso de los sistemas informáticos, sin que en la normatividad mexicana exista una correcta definición de tales términos.

Se pretende de igual manera mediante éste trabajo, dar a conocer las diversas conductas, a través de las cuales una persona común con ciertos conocimientos de cómputo puede llegar a ocasionar, dañando el sistema operativo de un sistema o bien, en aquellos casos del denominado delincuente informático, el cual al tener los conocimientos suficientes y hasta especializados en la materia realiza éstos actos violando la intimidad de cada usuario de computadora, de una empresa, realizando transferencia de archivos o documentos que por su carácter de confidenciales no pueden ser dados a conocer a ninguna otra persona o hasta la obtención de un lucro, sin el consentimiento, en todos éstos casos del titular de tales derechos.

Proponiéndose en éste trabajo de tesis la creación y delimitación del concepto del "*delito informático*", así como el adecuar conductas nuevas para realizar delitos ya conocidos los cuales al no estar correctamente adecuados al uso de los avances de la ciencia, resultan inservibles para la adecuación de una conducta de éste tipo, o en el mayor de los casos, el encuadrar las nuevas conductas en actos nuevos

que aúno no se consideran delitos pero que traen consigo diversos daños, los cuales se expondrán en el presente, analizándose también el concepto de "delito informático", "delincuente informático" manifestando la necesidad de reformar los artículos 211 bis del 1 al 7 del Código Penal Federal vigente, que sí bien es cierto prevén tales delitos, lo cierto lo es también que muchas de las conductas que cometen los delincuentes informáticos aún no se encuentran debidamente establecidas en tales numerales, existiendo así la imposibilidad de que se les castigue por tales actos, pues como se desprende del artículo 14 constitucional, "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 que se trata", no apreciándose así en el Código Penal Federal una actualización de todas éstas conductas.

Como sabemos, en la actualidad el Internet es el medio electrónico que más se utiliza para actividades económicas (compra venta de artículos, traspasos de cuentas, consultas de saldos de cuentas de débito, crédito, inversiones, etcétera), actividades culturales (consulta de la base de datos determinada para alguna investigación, ya sea de carácter docente o laboral), servicios (pagos, bolsa de trabajo, información en general, etcétera), diversión y un sin fin de actividades que se pueden realizar, mismas que a través del paso del tiempo ha crecido de manera considerable, pues si hace diez años que el internet se dio a conocer de manera comercial actualmente el número de usuarios de internet se ha elevado considerablemente, al día de hoy los medios de comunicación electrónica de éste tipo han sido cada vez más accesibles, incrementando por ello el número de

usuarios y de actividades electrónicas que se realizan cada día, más sin en cambio, debido al crecimiento de tales actividades de igual manera se han incrementado el número de posibilidades para que alguna de éstas personas se introduzca a los sistemas informáticos con fines no autorizados o con el fin de causar algún daño o sustraer algún tipo de información, que como ya se mencionó en líneas anteriores, lo puede hacer con fines de simple curiosidad o con la firme intención de realizar lo que quiere, ya sea para la obtención de un lucro o no, contemplando así en nuestro Código Penal Federal solo las conductas que se cometen contra equipos "protegidos por algún mecanismo de seguridad", quedando en una laguna cuando la intromisión se realiza en contra de equipos que no se encuentren protegidos por algún sistema de seguridad.

El "delito informático" implica actividades criminales que no encuadran en las figuras tradicionales del delincuente común, como el robo, el abuso de confianza, la alteración de documento, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho, incluso, en el ámbito 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 no existe una definición de carácter universal.

Por cuanto hace a nuestra legislación, el término de "delito informático" no existe, puesto que para que tal término exista se debe encontrar señalado en la

legislación vigente y en nuestro Código Penal Federal y Nuevo Código Penal vigente para el Distrito Federal, no se encuentra establecido, más sin en cambio a pesar de encontrarse señaladas algunas de las conductas que se encuadran dentro de tales "delitos informáticos", lo cierto es que tal delimitación de conductas, no son suficientes para encuadrar todas estas actividades realizadas por los sujetos activos, pretendiéndose en el presente trabajo de investigación proponer la tipificación de tales conductas a fin de que las mismas sean consideradas como delitos.

Desarrollándose así en el primer capítulo los conceptos de Derecho, Derecho Penal e Informática, a manera de entrar al estudio del tema del trabajo de investigación que se realiza. El segundo capítulo se desarrolla el tema de la informática jurídica, subdividiendo el tema de la informática jurídica documental, jurídica de control o de gestión y la meta documentaria o de decisión. En el capítulo tercero se desarrolla el tema de los conceptos generales de los delitos informáticos, desarrollándose el concepto del delito, la teoría heptatómica del mismo, los bienes jurídicos tutelados en los delitos informáticos y las formas de comisión actuales de los mismos. El capítulo cuarto señala a manera de introducción a los temas de los que se trata en la presente investigación, señalando los orígenes y antecedentes del internet, las conductas delictivas comunes y el uso del internet en el Derecho. El quinto capítulo señala la comparación del Delito informático en las diversas legislaciones que lo contemplan, tanto a nivel Nacional como extranjero.

CAPÍTULO I

EL DERECHO PENAL Y DERECHO INFORMÁTICO.

A) CONCEPTO DE DERECHO

Es de suma importancia en el presente trabajo de investigación, delimitar los términos y conceptos que se usan en éste, mismos términos generales que a continuación se señalan.

Como primer concepto es necesario señalar el concepto de DERECHO, mismo que se ha denominado por varios juristas de la siguiente manera:

Como término en general, la palabra DERECHO se define como "el conjunto de las leyes y disposiciones que determinan las relaciones sociales desde el punto de vista de las personas y de la propiedad. Facultad de hacer una cosa, de disponer de ella o de exigir algo de una persona: el padre tiene derecho de castigar a su hijo cuando éste lo merece. (...) . Derechos civiles, aquellos cuyo ejercicio garantiza el Código Civil a todos los ciudadanos: el derecho de testar es un Derecho Civil. El derecho natural: conjunto de reglas basados en la justicia natural. Derecho positivo, el establecido por las leyes: el derecho positivo está destinado a suplir las deficiencias del Derecho natural. Derecho de gentes o internacional.

Conjunto de leyes perteneciente a una materia determinada: Derecho canónico, administrativo, municipal, etcétera." ([1])

De igual manera se encuentra que la palabra Derecho tiene el significado siguiente:

La palabra DERECHO proviene del latín *directus*, directo; de *dirigere*, enderezar o alinear. La complejidad de esta palabra, aplicable en todas las esferas de la vida, y la singularidad de constituir la fundamental en esta obra y en todo el mundo jurídico (positivo, histórico y doctrinal), aconsejan, más que nunca, proceder con orden y detalle.

1ro Como adjetivo, tanto masculino como femenino . En lo material: recto, igual, seguido. Por la situación: lo que queda o se encuentra a la derecha o mano derecha del observador o de la referencia que se indique. En lo lógico: fundado, razonable. En lo moral: bien intencionado. En lo estrictamente jurídico: legal, legítimo o justo.

2do Como adverbio, y en consecuencia invariable, equivale a derechamente o en derechura; sin otra acepción jurídica que la figurada del camino derecho o recto, la vía legal , la buena fe. A ello equivale el empleo como sustantivo neutro: lo derecho.

([1]) GARCÍA PELAYO Y GROSS Ramón. Pequeño Larousse ilustrado, México, Distrito Federal 1995, ediciones Larousse, página 357.

El maestro Marco Antonio Díaz de León en su diccionario de Derecho Procesal Penal define el Derecho de la siguiente manera: "Conjunto de Normas jurídicas establecidas por el Estado, con la finalidad de regular y armonizar la conducta de los gobernantes, gobernados e individuos" ([2])

Marcel Plariol lo define de la siguiente manera: "La palabra derecho designa una facultad reconocida a una persona por la ley, y que le permite realizar determinados actos como son el de propiedad, de testar, potestad y político." ([3])

Cabanellas la define en su diccionario de Derecho como el "Conjunto de principios, preceptos y reglas a que están sometidas las relaciones humanas en toda sociedad civil, y a cuya observancia pueden ser compelidos los individuos por la fuerza" ([4])

Martha Morineau refiere el término "El Derecho es un conjunto de reglas que rigen las relaciones de los hombres dentro de la sociedad." ([5])

Rafael de Pina Vara define el Derecho como: "En general se entiende por Derecho todo conjunto de normas eficaz para regular la conducta de los hombres, siendo

---

([2]) DÍAZ DE LEÓN, Marco Antonio. Diccionario de Derecho Procesal Penal, tomo I, México, Distrito Federal 1993, editorial Porrúa, página 586.

([3]) MARCEL PLARIOL, Georges Ripert. Derecho Civil, Editorial Harla, México Distrito Federal 2001, Vol. 8 Pag: 1.

([4]) CABANELLAS, Guillermo. Introducción al estudio del Derecho Romano. Diccionario Enciclopédico de Derecho Usual Editorial Heliasta Tomo III 24 Edición, Buenos Aires Argentina, págs. 100 y 105.

([5]) MORINEAU IDUARTE, Marta y otro. Introducción al estudio del Derecho Romano. Derecho Romano. Tercera Edición Edit Harla, México 1993. Página: 30.

su clasificación más importante la de Derecho positivo y derecho natural. Estas normas se distinguen de la moral" ([6])

Marco Monroy refiere al respecto que "Derecho deriva de la voz latina *directum*, de dirigere, "dirigir", "encauzar" y que significa lo que está conforme a la regla, a la norma. Derecho se dice en italiano *diritto*; en portugués, *direito*; en rumano, *dreptu*; en francés, *droit*, en inglés *right*; en alemán, *recht*; en holandés *reght*." ([7])

Para efectos del presente trabajo de investigación, se entenderá por DERECHO como el conjunto de normas jurídicas establecidas por el Estado para regular la conducta de los hombres que viven en sociedad, dando con ello solo un concepto somero del término únicamente para efectos del presente trabajo, no entrando así en el estudio profundo que se requiere.

B) CONCEPTO DE DERECHO PENAL

Debido a que el presente trabajo se desarrolla en el ámbito de investigación del Derecho Penal es necesario de igual manera definir el concepto de Derecho Penal, mismo que se desarrolla de la siguiente manera.

Para el jurista Marco Antonio Díaz de León en su diccionario de derecho Procesal Penal el Derecho Penal significa: "Conjunto de Normas Jurídicas que fijan el poder

---

([6]) DE PINA VARA, Rafael. Diccionario de Derecho, vigésimo sexta edición, México, editorial Porrúa, 1998, página 228.

([7]) MONROY CABRA, Marco G., Introducción al Derecho, 12ª edición, editorial Temis, Bogotá Colombia 2001, Página 3.

sancionador y preventivo del Estado, en base a los conceptos de delito, responsabilidad del sujeto y pena" ([8])

Para el maestro Francisco Pavón Vasconcelos el término de Derecho Penal se define como: "Esta expresión se usa indistintamente para referirse al Derecho Penal, como conjunto de normas jurídicas que integran un ordenamiento punitvo determinado, o a la disciplina científica cuyo objeto lo constituye el Derecho Penal objetivo, vigente en cierto momento y lugar. A pesar de la costumbre del uso indiscriminado de la citada expresión, en las dos acepciones señaladas, debe tenerse el cuidado de darle un contenido preciso, según se la refiera al ordenamiento jurídico o a la ciencia o disciplina que hace de dichas normas su objeto de estudio. Nos permitimos advertir que empleamos la expresión aludida con referencia concreta al ordenamiento positivo penal, pues la disciplina que hace de ese conjunto de normas la materia de su examen metódico, se denomina ciencia del Derecho Penal o dogmática penal." ([9])

De igual manera en su libro de Manual de Derecho Penal Mexicano, aporta un concepto más claro de Derecho Penal refiriendo que es "... el conjunto de normas jurídicas, de Derecho Público interno, que definen los delitos y señalan las penas o medidas de seguridad aplicables para lograr la permanencia del orden social" ([10])

([8]) DÍAZ DE LEÓN, Marco Antonio, op cit. Página 586.
([9]) PAVÓN VASCONCELOS, Francisco. Diccionario de Derecho Penal, segunda edición. México, 1999, editorial Porrúa, página 354 y 355.
([10]) PAVÓN VASCONCELOS, Francisco. Manual de Derecho penal Mexicano, séptima edición, México 1985. Editorial Porrúa, página 17.

Para Rafael De Pina, el Derecho Penal es el: "Complejo de las normas del derecho positivo destinada a la definición de delitos y fijación de las sanciones. Denomínase por algunos autores derecho Criminal." ([11])

El Derecho Penal tiene como función el salvaguardar al hombre en su integridad y familia principalmente, así como en sus propiedades, posesiones y derechos, constituye la esencia del orden jurídico existente en la humanidad. Para lograrlo señala como punición a las acciones que son dañinas para la colectividad, imponiendo a los autores de los hechos delictivos las penas correspondientes, mismas que de acuerdo con el Nuevo Código Penal para el Distrito Federal en su artículo 30 son: "I. Prisión; II. Tratamiento en libertad de imputables; III. Semilibertad; IV. Trabajo en beneficio de la víctima del delito o en favor de la comunidad; V. Sanciones pecuniarias; VI. Decomiso de los instrumentos, objetos y productos del delito; VII. Suspensión o privación de derechos; y VIII. Destitución e inhabilitación de cargos, comisiones o empleos públicos", con el fin de resguardar los principios universales de bienestar, bondad, equidad y poder. Partiendo del orden de ideas anteriormente citados, podemos arribar a la siguiente noción:

El derecho Penal, es una rama del Derecho en general y encuentra su plena justificación en la finalidad del Estado, que tiende a preservar el orden social como una necesidad de salvaguardar bienes no sólo de interés social, sino también elevados intereses personales mediante la amenaza y aplicación efectiva de

([11]) DE PINA VARA, Rafael. Op Cit página 238.

penas que tutelan tales bienes, el Derecho Penal tiene dos acepciones, la del Derecho Penal sustantivo y la de Derecho Penal adjetivo.

DERECHO PENAL SUSTANTIVO.- Lo constituye el conjunto de normas jurídicas penales relativas al delito, penas y medidas de seguridad, lo cual es el objeto de estudio del Derecho Penal, por lo que al hacer referencia al Derecho Penal Sustantivo, específicamente nos referimos al Código Penal. (En Puebla denominado Código de Defensa Social).

DERECHO PENAL ADJETIVO.- Es el que pone en movimiento al Derecho Penal Sustantivo, mediante la observancia de formalidades que se encuentran dispuestas en un cuerpo legal. Por lo que al referirnos al Código Penal Adjetivo, estaremos hablando del Código de Procedimientos Penales.

Al Derecho Penal también se le conoce como Derecho Criminal.- En Italia se utilizó por primera vez el término de Derecho Criminal que eran los delitos de crimen (o sea donde había sangre); también por algunos tratadistas se le denomina Derecho de Defensa Social, mismo que a nuestra consideración es incorrecto el nombre de Derecho de Defensa Social, ya que todas las ramas del derecho son creadas para la defensa social, sin embargo el Estado de Puebla refiere a sus códigos penales y de Procedimientos Penales como de Defensa Social.

También se le ha denominado Derecho Transgresional.- diciéndose que es transgresional cuando se viola una norma pero se violan las normas no sólo del Derecho Penal, sino del Derecho Civil, Derecho Administrativo, etcétera. El Derecho Punitivo también se utiliza como sinónimo de Derecho Penal.

Es menester señalar brevemente el concepto de Derecho Procesal Penal, ya que lo hemos referido en líneas anteriores, a manera de diferenciarlo con el Derecho Penal, siendo definido el derecho procesal penal por el jurista marco Antonio Díaz De León como el "Conjunto de normas jurídicas que tienen por objeto la regulación del desarrollo y eficacia de ese conjunto de relaciones jurídicas, denominada proceso penal." ([12])

Carlos Fontan lo define como: "... la rama del ordenamiento jurídico que agrupa las normas que el Estado impone bajo amenaza de sanción, limitando y precisando con ellas su facultad punitiva" ([13])

El maestro Carrancá y Trujillo, refiere al respecto que: "En suma, el Derecho Penal objetivamente considerado ése conjunto de leyes mediante las cuales el Estado define los delitos, determina las penas imponibles a los delincuentes y regula la aplicación concreta de las mismas a los casos de incriminación. Es una disciplina jurídica y social, por mirar a las violaciones de la ley, a la defensa de la sociedad

([12]) DÍAZ DE LEÓN, Marco Antonio, op cit. Página 597.
([13]) FONTAN BALESTRA, Carlos, Derecho penal, introducción y parte general, editorial Albeledo Perrot, Argentina Buenos Aires 1991, página 20.

mediante la pena y las medidas de seguridad y a la significación y valoración social y jurídica de la conducta humana." ([14])

Para el maestro Jiménez de Asúa en su libro de lecciones de Derecho Penal refiere que "Por nuestra parte proponemos un concepto propio de la disciplina que cultivamos: Conjunto de normas y disposiciones jurídicas que regulan el ejercicio del poder sancionador y preventivo del Estado, estableciendo el concepto del delito como presupuesto de la acción estatal, así como la responsabilidad del sujeto activo, y asociado a la infracción de la norma, una pena finalista o una medida aseguradora" ([15])

Orellano Wiarco refiere al respecto que Derecho Penal "es el conjunto de normas de Derecho Público que estudia los delitos, las penas y medidas de seguridad aplicables a quienes realicen las conductas previstas como delitos, con el fin de proteger los bienes jurídicos fundamentales de la sociedad y de los individuos" ([16])

A fin de definir el concepto de Derecho Penal podemos señalar que: El derecho Penal, es una rama del Derecho público que encuentra su plena justificación en la finalidad del Estado, que tiende a preservar el orden social como una necesidad de salvaguardar bienes no sólo de interés social, sino también elevados intereses

---

([14]) CARRANCÁ Y TRUJILLO Raúl. Derecho Penal Mexicano. Parte General.. Editorial Porrúa, México, Distrito Federal 2001, página 37.
([15]) JIMÉNEZ DE ASÚA, Luis, Lecciones de Derecho Penal, tomo III, editorial Oxford, México 2001, página 2.
([16]) ORELLANO WIARCO, Octavio Alberto, Curso de Derecho Penal, parte general, segunda edición, editorial Porrúa, México 2001, página 5.

personales mediante la amenaza y aplicación efectiva de penas que tutelan tales bienes, delimitando en ello la aplicación de penas y medidas de seguridad.

C) CONCEPTO DE INFORMÁTICA.

El Diccionario de la Real Academia de la Lengua define la Informática como: "Conjunto de conocimientos Científicos y Técnicos que hacen posible el Tratamiento Automático de la Información por medio de Ordenadores"

El diccionario Gran Espasa ilustrado lo define como: "Conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automático de la información por medio de ordenadores electrónicos. Dentro de la informática se puede diferenciar varios campos: informática teórica (análisis numérico, lenguajes, teoria de la información); de los sistemas (arquitectura de los ordenadores, jerarquía de los recursos, comunicación entre procesadores, redes), tecnológica (hardware, componentes electrónicos, semi conductores, memorias, soportes, órganos periféricos); metodológica software y aplicativa (funciones de los ordenadores y tratamientos de la información).

Sin embargo esta definición es un tanto escueta y carente de fondo tecnológico, ya que las computadoras son sólo una herramienta para el tratamiento automático de la información.

La informática se puede definir de manera más amplia como el conjunto de conocimientos y herramientas científicas, técnicas y tecnológicas que se encarga del tratamiento racional y estructurado de la información por medios automáticos electrónicos digitales.

El término informática deriva de la palabra francesa *Informatique*, la que significa Información automática.

La primera contribución importante al nacimiento de la informática está dado por la teoría de la información.

La noción de la información fue definida por primera vez por Ralph Vinton Lyon Hartley en 1927 como la cantidad de elecciones o respuestas "Sí" o "No", que permiten reconocer unívocamente un elemento cualquiera en un conjunto de ellos, dividiendo el tiempo en elementos de tiempo en dos grupos iguales y excluyendo aquel en el cual el elemento no está presente. Esta definición asocia la noción de elemento e información que reduce el grado de incertidumbre de una opción, por consiguiente, el saber que el elemento buscado no se encuentra en uno de dos grupos, se puede excluir el grupo en el cual no existe el elemento y continuar con la búsqueda en el resto de los elementos, reduciendo la incertidumbre y el costo de las búsquedas siguientes.

Las computadoras son procesadores de datos, y su función es relativamente simple ya que los datos son procesados electrónicamente dentro del

microprocesador y en otros componentes; sin embargo bajo los conceptos informático y computacional, los datos pueden representar todo un reto, ya que la computadora únicamente puede procesar datos concisos y en formatos simples, esto es en forma digital en tanto "el mundo real" existe en datos analógicos.

Las señales que perciben habitualmente los sentidos humanos son datos que pueden estar representados en sonidos, imágenes, ideogramas, etc., cuya naturaleza es análoga, lo que significa que varía en su tipo y es continua en el tiempo, por lo cual es inutilizable en una computadora que está limitada por un reloj interno que "la prende y la apaga" un sinnúmero de veces por segundo.

La computadora es básicamente una máquina eléctrica, por lo cual, únicamente puede trabajar con datos que estén asociados con la electricidad. El procesamiento de datos se logra utilizando conmutadores que pueden estar encendidos o apagados. La computadora está fabricada enteramente con millones de conmutadores en forma de transistores que pueden procesar datos en forma de 0s y 1s.

Cada 0 y 1 es conocido como *bit*, que es abreviatura para *BInary digiT*, o dígito binario, que a su vez deriva del sistema de numeración binario:

0	1 bit
1	1 bit
0110	4 bit
01101011	8 bit

El sistema de numeración binario consiste de únicamente 2 dígitos: 0 y 1, a diferencia del decimal que utilizamos en la vida cotidiana compuesto por 10 numerales, del 0 al 9.

Números decimales	Números binarios
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000

Para que la computadora pueda trabajar con datos, es necesario convertir la información analógica a digital, esto es, convertirla en 0s y 1s.

La informática se puede definir de manera más amplia como: "Ciencia del tratamiento racional, particularmente por máquinas automáticas, de la información considerada como el soporte de conocimientos humanos y de comunicaciones en los aspectos técnico, económico y social. Conjunto de disciplinas científicas y de técnicas específicamente aplicables al tratamiento de datos efectuados por medios automáticos." ([17])

La informática es la rama de la cibernética entendiendo ésta como la ciencia de la comunicación y el control

([17]) TÉLLEZ VALDEZ, Julio. Derecho informático, segunda edición, México 2001. Editorial Mc Graw-Hill, página 282.

Suele confundirse la palabra cibernética con la informática, sin en cambio, la primera es la disciplina general en tanto que la segunda es una rama de la primera, la primera de los términos suele ser confundido con los medios electrónicos y su evolución, cabe señalar de igual manera los antecedentes de los primeros equipos de cómputo y de automatización.

Los primeros instrumentos diseñados para los cálculos o cómputos tiene sus orígenes desde épocas muy remotas, siendo el ábaco el primer dispositivo mecánico para realizar cálculos, del cual no se precisa su origen exacto, después tenemos la tabla de logaritmos de 1614, la regla de cálculo de 1630, la máquina de Pascal de 1642, la tarjeta perforada de 1804, la máquina de Babbage de 1834, el código de Hollerith de 1880; evolucionando con posterioridad a las máquinas que ya en realidad realizaban algún proceso automatizado, siendo ésta la MARK 1 en 1937 a 1944 la cual fue conocida también como ASCC por sus siglas en inglés (Automatic Séquense Controlled Calculator), posteriormente la ENAC en 1943 a 1945, la EDVAC en 1945-1952, la UNIVAC de 1951, la tercer generación de computadoras tiene su origen en el año de 1963 con la aparición de las primeras computadoras que cuentan con circuitos integrados monolíticos, la cuarta generación de computadoras tiene su origen a finales de los años setentas y es cuando las computadoras cuentan con los primeros circuitos integrados o chips, siendo éstos circuitos los que integran diversos componentes electrónicos en un solo chip de silicio, reduciendo con ello el tamaño de los aparatos y aumentando la velocidad de los mismos, apareciendo ya con ello la era comercial de las

computadoras, comenzando con la aparición de los llamados "PROCESADORES", un término que en la actualidad es común al momento de realizar la adquisición de un equipo de cómputo, pero que realmente se desconoce su origen, siendo el primer procesador el 4004 de la marca Intel, marca que es la pionera en la creación de los microprocesadores siendo el 4004 el primer microprocesador; sin embargo, como parte de la evolución de Intel y su mercado de consumo, en 1978 lanza al mercado la primera computadora personal de IBM, la cual contaba con un procesador 4004 de Integrated Electronics, que eventualmente cambiaría su nombre a Intel, 640KB de RAM, monitor Hércules ámbar y disco duro de 5 MB.

En 1974 Integrated Electronics Corporation, que posteriormente cambiara su nombre a Intel, presentó su Unidad Central de Procesamiento en un circuito integrado denominado 8080, el cual contenía 4,500 transistores y podía manejar 64k de RAM a través de un transporte de datos de 8 bits. El 8080 fue el cerebro de la primera computadora personal, la histórica MITS Altair 8800, la cual promovió un gran interés en hogares y pequeños negocios a partir de 1975, siendo aún éste tipo de computadoras limitada para cierto grupo de personas, no era muy común el tener una computadora de éstas.

Posteriormente El microprocesador Intel 8086, oficialmente conocido como iAPX 86 es un microprocesador de 16 bits diseñado por Intel en 1978 basándose en los del 8080 y 8085 siendo compatibles con el lenguaje ensamblador y tiene un conjunto similar de registros expandidos a 16 bits. Contaba con 4 registros generales de 16 bits que podían ser accesados como registros de 8 bits, y 4

registros de índice de 16 bits, incluyendo el apuntador de pila (stack pointer). Los registros de datos podían ser utilizados implícitamente por instrucciones, complicando el almacenamiento de valores temporales. Contaba con puertos de E/S de 64K a 8 bits o 32k a 16 bits e interrupciones vectorizadas fijas. La mayoría de las instrucciones únicamente podían acceder una ubicación de memoria, por lo cual un operando tenía que ser un registro y el resultado era almacenado en uno de los operandos. También tenía cuatro registros de segmentos que podían ser manipulados desde los registros de índice. Los registros de segmento permitían a la UCP accesar un megabyte de memoria en un modo inusual; en vez de proveer los bytes faltantes, como en la mayoría de los procesadores segmentados, el 8086 corría 4 bits hacía la izquierda el registro de segmento y lo agregaba a la dirección. Como resultado los segmentos se traslapaban, lo que la mayoría de las personas consideran ser un mal diseño.

Aún cuando esto fue ampliamente aceptado e inclusive útil para el lenguaje ensamblador, donde el control de segmentos es total, esto causaba confusión en lenguajes que tienen uso intensivo de apuntadores, tales como C. Esto hacía compleja la representación eficiente de apuntadores, e hizo posible tener dos apuntadores con diferente valor apuntando a la misma ubicación de memoria. Aún peor, este esquema hizo muy complejo expandir el espacio de direccionamiento a más de un megabyte, haciendo necesario cambiarlo, situación que llegó hasta el 80286. El microprocesador 8086 original tenía una velocidad de 4.77 MHz y eventualmente llegó a los 10 MHz. El microprocesador 8086 no tenía instrucciones de punto flotante, pero se podía agregar esta funcionalidad a través de un

coprocesador matemático externo, igualmente a manera de una pastilla de silicio. El Intel 8087 fue la versión estándar aunque fabricantes como Weitek ofrecieron alternativas de mayor desempeño. La primera computadora personal comercialmente exitosa fue creada por IBM en 1981. En su interior había un microprocesador Intel 8088. Las prestaciones de este circuito resultan avanzadas para el momento, con 8 bits trabajando a 4,77 MHz, aunque bastante razonables para una época en la que el microprocesador de moda era el Z80 de Zilog, el motor de aquellos entrañables Spectrum que hicieron furor en esos tiempos, gracias sobre todo a juegos increíbles, con más gracia y arte que muchos actuales. El 8088 era una versión de 8 bits y prestaciones reducidas del 8086.

En Febrero de 1982 Intel introduce al mercado los microprocesadores Intel 80186 y el 80188, que son una versión mejorada de los 8086 y 8088, incluyendo un transporte de datos externo a 16 y 8 bits respectivamente, y una velocidad que iniciaba en los 6MHz. Una de las principales características que incorporó Intel en su familia 8018x es la integración de la ALU, DMA, controladores de interrupción y temporizador en la misma pastilla ahorrando hasta 25 circuitos integrados en el diseño de la tarjeta madre, características que si bien le dieron supervivencia hasta nuestros días como microcontrolador, también marcaron su poca penetración en el mercado de las computadoras comerciales ya que no era del todo compatible con las tecnologías existentes. Una de las pocas computadoras que utilizaron este microprocesador fue la Siemens PC-D.

En Febrero de 1982, unos días después de la presentación del 80186, Intel presenta la siguiente generación de microprocesadores, el 80286 con velocidades iniciales de 6, 10, y 12 MHz, que con sus 134,000 transistores y 16 bits en la ruta de datos fue el microprocesador elegido para las primeras computadoras personales que llegaron al mercado en 1983. Este microprocesador fue fabricado con tecnología de 1.5 micrones, mejorando la anterior de 3. Los avances tecnológicos que permitieron integrar varias funciones y servicios en el 80186/80188, fueron utilizados en el 80286 para crear un microprocesador que soportara multitarea. El 80286 tiene dos modos de operación: modo real y modo protegido. En el modo real, se comporta igual que un 8086, mientras que en modo protegido incluye gestión de memoria con la extensión natural de las capacidades de direccionamiento del procesador. El 80286 tiene circuitería incorporada para la protección de datos. Otras características incluyen todas las características del juego de instrucciones del 80186, así como la extensión del espacio direccionable a 16 MB, utilizando 24 bits. El 80286 contiene 134,000 transistores dentro de la pastilla, un incremento del 360% con respecto al 8086. Externamente llegó al mercado en varios encapsulamientos como el PLCC, PGA y LLC. Este procesador se conoce comercialmente como el 286.

En 1985 llegan al mercado los llamados 80386 (llamados comercialmente los procesadores 386) trayendo consigo una nueva revolución tecnológica ya que se hablaba de una velocidad de proceso de 16-33 MHz, la velocidad del bus de datos era dada por el procesador, aparece la llamada Memoria caché la unidad FPU (o coprocesador matemático se incluye en el mismo circuito procesador). 386 SX

Estos chips ya son más modernos, aunque del Neolítico informático. Su ventaja es que son de 32 bits; o mejor dicho, el 386 es de 32 bits; el 386 SX es de 32 bits internamente, pero de 16 en el bus externo, lo que le hace hasta un 25% más lento que el original, conocido como DX. Lo curioso es que el original, el 386, sea el más potente. La versión SX fue sacada al mercado por Intel siguiendo una táctica comercial típica en esta empresa: dejar adelantos tecnológicos en reserva, manteniendo los precios altos, mientras se sacan versiones reducidas (las "SX") a precios más bajos. La cuestión es que ambos pueden usar software de 32 bits, incluso el conocido sistema operativo Windows 95, la desventaja de usar éste sistema operativo es su lentitud y los problemas que trae consigo en la realización de algún comando.

En el año de 1989 aparecen los primeros procesadores de la marca INTEL 40486 conocidos en el mercado como "486"; en el año de 1993 aparecen los procesadores PENTIUM; en el año de 1997 entra al mercado de consumo popular con una versión simplificada del Pentium II. El CELERON que carece de antememoria de nivel 2, soporte para doble procesador y la carcaza plástica que identificaba al Pentium II. Además de esto, el microprocesador únicamente funcionaba con un transporte frontal de datos a 66MHz. La combinación de velocidad de transporte frontal de datos a 66MHz y la falta de antememoria de nivel 2 redujo sensiblemente el desempeño del microprocesador, lo que dejaba una ventana de oportunidad a las empresas competidoras de Intel que ofrecían procesadores con mayor desempeño a la misma velocidad de reloj. En la siguiente edición del Celeron, el Celeron 300A Intel corrigió estos errores liberando la

velocidad de transporte frontal de datos e incorporando 128KB de antememoria de nivel 2 en la misma pieza del microprocesador, lo que significa que funciona a la misma velocidad de reloj que el procesador, lo que redundó en que un Celeron podía operar aún mejor que un Pentium II con 512KB de antememoria. Con estas características, el Celeron se hizo famoso en los círculos de entusiastas que alteraban el reloj para obtener un mayor rendimiento, también conocido como sobrerrelojeo u overclocking. Los Celeron originales utilizaban la ranura 1, pero eventualmente Intel comenzó a fabricarlos para formatos de Arreglos en Malla Plástica de Postes o formato PPGA por las siglas de su nombre en inglés Plastic Pin Grid Array, también conocido como zócalo 370.

Este tipo de procesadores aún el día de hoy se utilizan, pero con modificaciones, siendo éstas su velocidad, los hay comercialmente hablando desde 533 Mega hertz (Mhz) hasta 2.0 Giga Hertz (MHz). Los procesadores actuales para que se haga una comparación con los antecedentes que se refieren son el actual procesador PENTIUM IV y Centrino (o sus similares en las diferentes marcas), mismos que cuentan con una velocidad de hasta 3.0 Giga Hertz, comercialmente hablando, pues en proyectos de diversos equipos de cómputo, se manejan velocidades muy por superior a ésta. La capacidad desde los primeros equipos de cómputo ha cambiado radicalmente, puesto que las primeras computadoras comerciales contaban con un disco duro de almacenamiento de 100 MB, cuando actualmente es fácil encontrar una computadora (u ordenador) con un Disco Duro de 80 GB, es decir 8,000 veces más capacidad que las primeras computadoras.

Finalizando con los antecedentes de los equipos de automatización podemos decir que la informática es la rama de la cibernética que responde a la necesidad del hombre por eficientar los procesos de producción y en general todos aquellos procedimientos que le son, en alguna medida, útiles. El término "computadora" a pesar de ser de uso común, no es el adecuado, pues como se aprecia en los antecedentes de los equipos automatizados para realizar cálculos, éste es el término con el que se les denomina por la función que realizaban, sin en cambio los sistemas actuales no solo realiza cálculos, sino realiza diversas operaciones automatizadas, almacenamiento, desde luego cómputo y un sin fin de actividades, por ello suele ser denominada la "computadora" como ordenador o sistema informático, siendo éste concepto el más adecuado por algunos estudiosos de la materia, puesto que no solo se refiere a un equipo de cómputo, sino a éste y la interacción con otros componentes y otros ordenadores, ya sea a través de redes internas (Intranet o servidores) y redes externas (Internet).

D) CONCEPTO DE DERECHO INFORMÁTICO

Para Julio Téllez Valdez, jurista mexicano que ha desarrollado los más importantes estudios de Derecho informático nos indica al respecto que: "Aunque difícil de conceptualizar por el variado número de peculiaridades y muy a pesar de los opuestos puntos de vista que pudiera provocar, podemos decir que el Derecho Informático es una rama de las ciencias jurídicas que contempla a la informática

como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática)." ([18])

Desde luego, como parte en general el Derecho informático abarca distintos aspectos que en el presente trabajo de investigación no abordaremos, pues el estdio del Derecho informático no solo abarca las conductas delictivas a que se refiere el Derecho Penal informático como lo denominan algunos autores, sino que desde luego, abarca situaciones relativas al Derecho Civil, administrativo, laboral, etcétera, señalando así MEJAN lo siguiente: "...cuando el Derecho sirve a los propósitos de la informática. Esto es, cuando los procesos informáticos deben ser objeto de una protección jurídica por suponer un derecho de autor o información confidencial; cuando es menester celebrar contratos que tengan por objeto bienes informáticos; cuando se impone punir a quien roba esos bienes o a quien usa indebidamente la información sin derecho; cuando la información es dinero y es transmitida de un propietario a un destinatario y cuando debemos llegar a tribunales a probar la celebración de actos jurídicos que imputaron derechos y obligaciones a las partes a través de medios electrónicos." ([19])

Altmark refiere al respecto que: "Podemos sostener entonces que el Derecho Informático es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática." ([20])

([18]) TÉLLEZ VALDEZ, Julio. Op. Cit. Página 22.

([19]) MEJAN, Luis Manuel C.; "Transferencia Electrónica de Fondos. Aspectos jurídicos"; Fomento Cultural Banamex, México 1990, págs. 67-68.

([20]) ALTMARK, Daniel Ricardo; "La Etapa Precontractual en los Contratos Informáticos. Informática y Derecho. Aportes de Doctrina Internacional."; Ediciones Depalma, Buenos Aires, Vol. 1, Pág. 6.

Aún cuando no hay un sistema de normas dedicado a regular dichas situaciones, se ha dado en bautizar así al conjunto de normas, de distintas áreas del Derecho, entendiéndose así a manera de definición de Derecho Informático como el conjunto de normas jurídicas destinadas a regular, en diferentes ramos del quehacer humano, todas aquellas actividades, situaciones de hecho y relaciones surgidas de la interacción del hombre con los sistemas informáticos, computadoras u ordenadores; así, el término de Derecho Informático es un concepto que ha surgido de una nueva necesidad y del uso, como lo es el de los sistemas informáticos, pero que el mismo aún no se encuentra debidamente regulado ni definido.

No pretendiéndose dar en el presente trabajo un concepto generalizado de DERECHO INFORMÁTICO, pues no es la finalidad del presente, debido a que el concepto es demasiado amplio y su campo de aplicación no solo radica en los llamados "delitos informáticos", sino que abarca la relación con las diferentes ramas del Derecho.

E) EL DERECHO PENAL EN LA ACTUALIDAD

El Derecho es una ciencia que al igual que las demás ciencias debe de renovarse, pues los cambios que sufre la sociedad son demasiados y con gran rapidez, surgiendo ciencias nuevas como es la informática, la robótica, la cibernética, etcétera, pero las ciencias que se crearon desde hace varios años, de igual manera deben de evolucionar al grado de adaptarse a las necesidades actuales

que surgen, ya sea por el aumento de la población, por las nuevas condiciones o por los adelantos tecnológicos que el hombre crea, pues sería ilógico dejar al Derecho a un lado por ser ciencias aparentemente distintas.

El Derecho Penal al definirse en el inciso B del presente trabajo como la rama del Derecho Público encargada de preservar el orden social como una necesidad de salvaguardar bienes no sólo de interés social, sino también elevados intereses personales mediante la amenaza y aplicación efectiva de penas que tutelan tales bienes, delimitando en ello la aplicación de penas y medidas de seguridad, tiene la obligación de renovarse ante los diferentes cambios que surjan, adecuándose así a las necesidades que exige la sociedad a fin de no dejar impune un hecho que socialmente sea rechazado, pero por falta de tipificación, dicha conducta no pueda ser sancionada, generando con ello solo la impunidad.

F.- DERECHO PENAL INFORMÁTICO

Son pocos los autores que hacen referencia a éste concepto, pues el término de Derecho Penal informático al igual que el de Derecho informático aún no ha sido reconocido del todo, pues para que sea delimitado, es necesario inicialmente darle el término y reconocimiento al Derecho Informático, sin embargo, a manera de estudio podemos decir que el Derecho Penal Informático es el conjunto de normas jurídicas encargadas del estudio de las conductas antijurídicas, típicas, culpables y punibles que involucran para su comisión el uso de cualquier sistema informático o tecnológico.

El Derecho Penal y la informática tienen una estrecha relación, pues el Derecho Penal informático es el dedicado al estudio de todas aquellas conductas ilícitas que se derivan del uso de los nuevos sistemas informáticos y el uso de las tecnología actuales, no para la comisión de delitos comunes o ya conocidos apoyados del uso de las nuevas tecnologías, (verbigracia tenemos al delito común de amenazas que se hace a través del uso del teléfono celular), sino de aquellas conductas que no se habían conocido y que surgen derivadas del uso de esas nuevas tecnologías, por ejemplo la sustracción de archivos electrónicos, la intercepción de mensajes electrónicos, el robo de tiempo aire de telefonía celular, de televisión por cable, etcétera, un sin fin de actividades que hace treinta años no se pensaría que existieran simplemente por no existir tales adelantos tecnológicos.

A manera de resumen, podemos señalar respecto a éste capítulo en estudio que el Derecho se le considera como el conjunto de normas jurídicas establecidas por el Estado para regular la conducta de los hombres que viven en sociedad, siendo una de las ramas del Derecho Público el Derecho Penal, la cual tiene como objeto el estudio de las conductas típicas, antijurídicas, culpables, así como las penas y medidas de seguridad a fin evitar tales conductas.

Por ello podemos indicar que la sociedad se encuentra en constante movimiento, ante una serie de cambios que origina una gran novedad de circunstancias que hace unos años antes era una ficción imaginarlos, ante tales cambios y la creación de nuevos sistemas es necesario que de igual manera el Derecho se ajuste a tales cambios, teniendo como objetivo principal el que la normatividad jurídica y para el

caso del presente trabajo la normatividad penal, se ajuste a las circunstancias que han originado la creación de sistemas informáticos, por tanto en éste capítulo no solo se da los conceptos de Derecho, de Derecho Penal, sino también se habla de la imperiosa necesidad de ajustar ésta disciplina a los cambios modernos.

Se define el concepto de informática, mismo que para algunos aún en la actualidad es un término desconocido o mal entendido, mismo que se define a través de su raíz francesa de automatización de la información, un término que cuando se crea, no se pensó realmente el alcance que iba a tener en tiempos futuros, se habla de la interacción de disciplinas que para algunos, de igual manera se pensaba que no tendrían mucha relación como lo es el Derecho y el Derecho Penal con la informática, señalándose la necesidad de establecer esas normas jurídicas dedicadas a tipificar como delitos las conductas derivadas del uso de las nuevas tecnologías.

Así, podemos decir que es necesario estudiar el avance tecnológico que surge no solo a nivel nacional sino a nivel mundial, para así poder adecuar la normatividad jurídica nacional ante los cambios que surgen cada día con el uso de los avances tecnológicos, no solo para la aplicación de las normas en un caso específico, sino también para adecuar la norma jurídica de tal manera que se adecue a los posibles cambios que con el uso de los nuevos sistemas informáticos pudiera surgir, pero no solo de los delitos llamados "informáticos", sino también la aplicación de la normatividad ante los delitos ya comunes que se cometen con apoyo en el uso de las nuevas tecnologías, debiendo adecuar la normatividad

procesal penal a fin de que los nuevos medios electrónicos sirvan de prueba en un proceso, sin lugar a dejar lagunas en la ley que solo provoquen la impunidad de los delitos.

Apreciándose así la imperiosa necesidad de establecer un orden jurídico penal adecuado que vaya a la mano del rápido avance tecnológico que en los países desarrollados es más rápido que en el nuestro, pero no por ello dicho cambio ha de llegar.

CAPITULO II

LA INFORMÁTICA JURÍDICA

A) Informática jurídica documental

Antes de entrar al estudio de la informática jurídica documental, es necesario señalar qué se entiende por informática jurídica, refiriendo el maestro Julio Téllez al respecto que la informática jurídica es: "la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación" ([21])

Desprendiéndose del anterior concepto y de acuerdo con lo señalado por varios estudiosos del Derecho informático, la informática jurídica se divide en tres ramas importantes, las cuales son: A) La informática jurídica documentaria, B) Informática jurídica de control y gestión y C) Informática jurídica metadocumentaria, procediéndose a analizar los mismos de la siguiente manera.

Ríos Estavillo señala que la informática jurídica documental "es la aplicación de técnicas informáticas a la documentación jurídica en los aspectos sobre el análisis,

([21]) TÉLLEZ VALDÉS, Op cit. página 25.

archivo y recuperación de información contenida en la legislación, jurisprudencia, doctrina, o cualquier otro documento con contenido jurídico relevante" ([22])

La informática jurídica documental se refiere (Cfr.) a lo manifestado por el maestro Téllez Valdés como el área más antigua de la informática; sus orígenes suelen asociarse a los trabajos de John Horty, en la Universidad de Pittsburg. En los sistemas de informática jurídica documentaria se trata de crear un banco de datos jurídicos (o hábeas jurídico documentario) relativa a cualquiera de las fuentes del Derecho (menos la costumbre) a efecto de interrogarlo con base en criterios propios acordes a esa información y su relevancia jurídica.

La informática jurídica documental o documentaría se refiere en términos generales a la creación de las bases de datos que se requieren para la búsqueda de información jurídica en general, siendo éstas aplicables a la búsqueda a través de filtros en los diferentes medios de cómputo y dispositivos de lectura, ya sean programas pre cargados en el disco duro o a través de los comunes discos compactos. La utilidad práctica en la actualidad radica en los motores de búsqueda avanzados en los discos compactos que compilan leyes, contratos, jurisprudencia, etcétera.

La búsqueda en las bases de datos y aplicaciones de filtros para las búsquedas ha ido avanzado actualmente de una manera impresionante y se ha extendido el uso

([22]) RÍOS ESTAVILLO, Juan José. Derecho e informática en México. Informática jurídica y Derecho de la informática. Editorial UNAM, México, 1997, página 57.

a tantos usuarios que ya es familiar realizar éste tipo de búsquedas sin la necesidad incluso de conocimientos en la materia.

Uno de los más importantes archivos para la ejecución de los motores de búsqueda dentro de una base de datos es el *thesaurus*, el cual "se convierte en un léxico jerarquizado que comprende una red de interconexiones, exclusiones, discriminaciones y proximidades semánticas bajo la forma de listas de sustitutivos de contrarios, términos vecinos o genéricos, etcétera." A cada interrogación del *corpus*, el *thesaurus* orienta la explotación a fin de disminuir automáticamente en la conversación con el usuario los problemas de ruido y silencio.

Sus funciones principales son las siguientes:

a) Como diccionario analógico en su función de conexión permitiendo reconocer situaciones y expresiones jurídicas, tomando en cuenta la sintaxis gramatical, buscando antónimos y reagrupando sinónimos.
b) Como diccionario analítico en su función de discriminación excluyendo nociones afines no necesarias o incidentales, así como en las formas no deseadas, disminuyendo las figuras polisémicas y sinónimas.
c) Como índice en su función de adición de términos que conforman la base de datos o corpus.

Los thesaurus pueden ser abiertos o cerrados, dependiendo de qué se pueda o no agregar a ellos nuevos elementos. ([23])

En resumen, podemos señalar que cada día se han vuelto de mayor importancia las bases de datos sistematizadas. Recordemos que a lo largo de las diferentes fases de la historia de la humanidad, nos hemos visto siempre en necesidad de guardar, conservar, archivar cifras, nombres, mapas, planos, estadísticas y todo tipo de datos curiosos y siempre útiles para las ciencias y otras actividades del hombre. La historia misma requiere de auto-conservarse en algún tipo de registro, empero, la acumulación de tanto cúmulo de información requiere para su debida consulta en específico un orden para poder ser consultado, teniendo para ello la necesidad y ante los nuevos mecanismos informáticos de crear un sistema que permita la creación de diferentes filtros y eficacia para poder realizar la consulta deseada sin mayor margen de error y con la rapidez requerida.

B) Informática jurídica de control o gestión

Comenzamos diciendo que la informática jurídica no sólo tiene su aplicación para el almacenamiento de datos para después ser consultados, sino que una de las utilidades principales es la del control y gestión de cierto tipo de expedientes, teniendo una de sus primeras aplicaciones dentro del medio jurídico en los sistemas de control y gestión de expedientes en el Tribunal Superior de Justicia, conservando así un registro para el ingreso de expedientes que se presentan por

([23]) TÉLLEZ VALDÉS, Op. Cit. Página 37.

los litigantes ante la oficialía de partes, el número del expediente y el juzgado donde se radica, llevando con ello un mejor control de todos y cada uno de éstos, evitando con ello el mal manejo ya sea por negligencia o por algún tipo de interés.

Pero, la función de la informática jurídica de control y gestión no solo radica en servir en una base de control de registro, sino también para la tramitación de los expedientes que se llevan en las oficinas de Gobierno y a manera de ejemplo podemos decir que en la Procuraduría General de Justicia del Distrito Federal, en el año de 1995 se implementa como obligatorio el sistema denominado "APCOM" (Averiguaciones Previas computarizadas), que toma su base en un sistema operativo de MS-DOS, sirviendo éste para la tramitación de averiguaciones previas, contando el mismo con los diversos formatos para la elaboración de razones, fe, inspecciones ministeriales, declaraciones de denunciantes, testigos, probables responsables, conductores, etcétera, la cantidad necesaria de actuaciones que realiza el Ministerio Público para la integración de una averiguación previa, contando éste sistema con un control interno de registro de la base de datos de la averiguación previa, guardando en un servidor central el número de averiguación previa, fecha y hora de inicio y las personas que en ella intervienen. En el año 2000 se implementa el sistema operativo SCAMPA (Sistema de Control de las Actuaciones del Ministerio Público), siendo la finalidad de éste el registro de las actuaciones del Registro de las actuaciones que se llevaban a cabo por parte del personal del Ministerio Público, es decir, se debía de ingresar en el referido sistema la fecha de inicio, la fecha y hora de los hechos, las personas que intervienen (probables responsables, denunciantes, agraviados,

testigos, peritos, Agentes del Ministerio Público, Oficiales Secretarios), las determinaciones de la misma, fecha de consignación, fecha de propuesta del No ejercicio de la acción penal, etcétera, siendo éste un sistema aparentemente creado para el control y gestión de expedientes, más sin en cambio su poco utilidad solo dio origen a que fuera complicado y en poco tiempo ya no fuera obligatorio el registro de muchos de los datos de una averiguación previa.

En el año de 2002 se implementa como obligatorio el SSAP, Sistema Simplificado de Averiguaciones Previas, el cual desplaza al sistema APCOM, teniendo el nuevo sistema una plataforma en el sistema operativo de Windows, contando éste sistema con las diversas actuaciones, mejor presentación y control de las actuaciones del personal ministerial, evolucionando a través del tiempo, pero siendo desplazado por un sistema similar denominado SAP Sistema de Averiguaciones Previas, mismo que entró como obligatorio para personal de la Procuraduría General de Justicia a finales de marzo del año 2005, contando inicialmente éste nuevo sistema con un mayor registro de la base de datos de las averiguaciones que se inician en el Distrito Federal, incorporando la base de datos de vehículos robados que hasta entonces se realizaba en un sistema denominado CONAURO (Control de Autos Robados), teniendo características muy similares a las del sistema antecesor denominado SSAP.

Siendo de suma importancia la facilidad que ofrece el uso de los sistemas informáticos para la tramitación de una averiguación previa o de un expediente, pues los "formatos" se encuentran bajo éste sistema disponibles para que el

usuario únicamente "llene" los espacios que el sistema le va marcando , sin embargo no es la única finalidad de éstos, sino también lo es el del registro y control de todas éstas actividades que se realicen por parte de los usuarios.

Refiere el maestro Téllez Valdés que: "Desde hace tiempo se vienen desarrollando otros sectores en procesos de continua evolución. Uno de ellos es la llamada informática jurídica de control y gestión, que abarca los ámbitos jurídico – administrativo, judicial, registral y despachos de abogados, principalmente.

Dicha área tiene como antecedentes el tratamiento de textos jurídicos mediante el uso de procesadores de la palabra y, por otra parte, las experiencias obtenidas, en materia de automatización de registros públicos (en particular de bienes inmuebles)." ([24])

Pero no solo la informática de control y gestión ha tenido aplicaciones en el área del control y gestión gubernamental, pues su desarrollo en los últimos años ha crecido de una manera tan importante que es fácil encontrar diferentes despachos en los que su sistema de control y gestión de los expedientes tramitados es, incluso superior a los de Gobierno.

C) Informática jurídica meta documentaria o de decisión.

La informática jurídica además de servir, como ya lo hemos visto para el almacenamiento de información y su rápida recuperación y consulta, tiene una

([24]) Ibidem, pág. 41

aplicación que hasta el momento no se le ha dado el uso definitivo en todas las actividades que se encuentran reservadas para el hombre, ésta división de la jurídica informática se llama jurídica informática metadocumentaria o por algunos autores llamada de decisión, refiriendo Ríos Estavillo que se le puede denominar meta decisional, o metadocumental o de ayuda a la decisión, señalando que: "A diferencia de la informática jurídica documental, ésta rama se caracteriza por conformarse por bases de conocimiento jurídico.

Abarca una gran variedad de esfuerzos y proyectos que intentan obtener de las aplicaciones de la informática al Derecho resultados que vayan más allá de la recuperación y reproducción de información (documental o no), con la pretensión de que la máquina resuelva por sí misma problemas jurídicos, o al menos auxilie a hacerlo y contribuya al avance de la teoría jurídica, se subdivide en:

a) Sistemas expertos legales
b) Sistemas de enseñanza del derecho asistidos por computadora

Los sistemas expertos son la estructuración de conocimientos especializados que, acoplados a un mecanismo de diferencia, saca conclusiones a partir de la información que se le suministra en forma de preguntas y respuestas" [25]

Refiere el maestro Téllez Valdés, al respecto que "Un tipo de aplicación muy especial lo constituye la informática jurídica metadocumentaria, llamada así porque trasciende más allá de la esencia de los fines documentarios propiamente

---

([25]) RÍOS ESTAVILLO, Op. Cit., Pág. 62

dichos (sin duda alguna constituye el acercamiento más interesante con respecto a la muy difícil de comprender iuscibernética). Sus ámbitos principales de injerencia los podemos establecer en cinco vertientes bien determinadas; ayuda en la decisión, ayuda en la educación, ayuda en la investigación, ayuda en la previsión y ayuda en la redacción" (26)

La Informática Jurídica Metadocumental o metadocumentaria constituye aquella rama de la Informática Jurídica que tiene un mayor significado de complejidad, por cuanto no se agota en la recopilación de textos documentarios, en la realización de documentos jurídicos, o control de asuntos, sino que es aún más profunda en su aplicación de la Informática, extendiéndose por ejemplo: al campo decisional, educativo e investigativo.

Existe un factor determinante para la realización o puesta en marcha de la Informática Jurídica Metadocumental. Ese factor está constituido por el extraordinario invento de lo que se conoce como la inteligencia artificial, dando la oportunidad de crear sistemas de expertos artificiales, que al entrar en el ámbito jurídico se constituyen en sistemas de expertos legales artificiales.

La inteligencia artificial es una disciplina que estudia y desarrolla la capacidad de los autómatas y robots, con el fin de resolver problemas por medio de procesos afines a los del pensamiento humano. En otras palabras, la Inteligencia Artificial

(26) TÉLLEZ VALDÉS, Op. Cit. Pág. 45

constituye una disciplina que estudia y desarrolla mecanismos de dotación a las computadoras de facultades propias de la inteligencia humana.

Consiste entonces, en la incorporación de mecanismos manipulables en la computadora, que comprenden el conocimiento sobre algún tema, y los procedimientos necesarios para dar solución o respuesta a los problemas planteados acerca del tema en discusión.

En este orden de ideas, como parte de la inteligencia artificial, aparecen los sistemas de expertos artificiales, que consisten en la incorporación de conocimientos de expertos humanos sobre una determinada problemática o materia, para la solución de cualquier tipo de problema, sobre todo aquellos no solucionables por los métodos tradicionales de la Informática.

Es relevante explicar que la influencia de la Inteligencia Artificial en el campo decisional radica en sistemas de búsqueda basadas en la relación de caracteres por la propia computadora, dando respuesta a la pregunta realizada por el usuario, pero de manera pragmática y no filosófica, por cuanto la computadora u ordenador por constituirse en simplemente una máquina, carece de la capacidad de razonar.

De esta forma, cuando se hace referencia al campo decisional, es necesario tomar en cuenta la ayuda que estos sistemas pueden prestar no solamente al juez en su función pública jurisdiccional, sino también al propio abogado, quien podrá tener una mejor recopilación y actualización de la información jurídica a través de la

respuesta proporcionada por el computador u ordenador, obteniendo algo así como una posible predicción de la decisión judicial.

La Informática jurídica metadocumental educativa.

En este punto de vista, debe enfocarse la ayuda que el material informático presta al campo educativo, en el sentido de que en estos tiempos de alta informatización de la sociedad, se puede sacar provecho a la utilización de computadoras u ordenadores, como por ejemplo, lograr la enseñanza asistida por éstas.

Influencia de la informática jurídica metadocumentaria o metadocumental en el campo de investigación. Informática jurídica metadocumental investigativa.

□

En este sector la Informática Jurídica Metadocumental tiene su importancia en el hecho de que a través de sistemas de inteligencia artificial, se puede mediante las computadoras u ordenadores, establecer ciertas teorías, acerca de alguna hipótesis proporcionadas por el usuario.

La computadora u ordenador, utilizando el sistema de inteligencia artificial y mediante la información que se le haya preconstruido en la memoria, podrá dar ciertas teorías que pueden ayudar a obtener mejores y más variados puntos de vistas acerca de una determinada hipótesis, haciendo que la investigación sea más completa.

Influencia de la informática jurídica metadocumental en la redacción de documentos o demandas.- En este caso hay que aclarar que no se trata de la redacción automática de actos repetitivos, debido a que ese punto pertenecería a la Informática Jurídica de Gestión y Control.

De manera que, la Informática Jurídica Metadocumentaria va más al fondo, porque resulta que trata acerca de las posibles correcciones en la redacción del documento, referidas a redundancias, vacíos o errores legales, mal redacción, errores ortográficos y/o gramaticales, entre otras cosas, con la finalidad de conseguir como fin último la realización de un documento que llene todos los requisitos formales y materiales.

De lo anterior y a fin de dar un mejor conocimiento de lo que se está hablando es necesario establecer los términos de Inteligencia artificial, sin embargo, para poder definir la inteligencia artificial, es necesario definir primero qué es la inteligencia; la cual constituye la capacidad de razonar, adquirir conocimientos, utilizarlos, dando la posibilidad de manipular las cosas que se encuentren en nuestro mundo y fuera de él si fuese posible.

Según el Diccionario de Inteligencia Artificial, ésta constituye una multi-disciplina que abarca a la Informática, ciencia neurótica, filosofía, psicología, robótica y lingüística; y es devota a la reproducción de métodos o resultados del razonamiento humano y actividad cerebral.

En este sentido, se puede entender a la inteligencia artificial como una disciplina que estudia y desarrolla la capacidad de los autómatas y robots, con el fin de resolver problemas por medio de procesos afines a los del pensamiento humano. En otras palabras, la inteligencia artificial constituye una disciplina que estudia y desarrolla mecanismos de dotación de facultades propias de la inteligencia humana a los computadores u ordenadores.

Consiste entonces, en la incorporación de mecanismos manipulables en la computadora, que comprenden el conocimiento sobre algún tema y los procedimientos necesarios para dar solución o respuesta a los problemas planteados acerca del tema en discusión.

De esta manera, a través de la inteligencia artificial, se proyecta mediante técnicas, la introducción en la computadora del conocimiento y los procedimientos que son necesarios para que al surgir un problema, de la forma más sencilla y natural, se ofrezca una o varias soluciones al respecto.

En resumen podemos decir que el sueño del hombre, desde que se dio inicio a la revolución industrial ha sido el tener cada vez más máquinas automatizadas, a tal grado de que las exigencias son cada vez mayores, teniendo como objetivo en que algún día las máquinas lo hagan todo por el hombre, incluso y a manera muy futurista, sería el hecho de dejar a las máquinas tomar decisiones, principal objetivo de la inteligencia artificial, una posibilidad que a pesar de los adelantos, aún suena bastante remoto, pues una de las características del ser humano es la

de raciocinio, la de decisión, la inteligencia misma, que por ahora no puede ser igualada por ninguna creación del hombre mismo.

Desde luego, que la decisión en materia jurídica deberá depender siempre del hombre, pues no podemos dejar en manos de un sistema informático por muy avanzado que parezca las decisiones en las que se encuentre de por medio la vida, la libertad, las posesiones, propiedades o derechos; además de que resulta lógico, para el caso de que tal decisión violente los derechos y sea necesaria la exigibilidad de una sanción para quien la aplicó es necesario que la responsabilidad, desde luego, deba recaer en una persona y no en una máquina.

CAPITULO III
CONCEPTOS GENERALES DE LOS DELITOS INFORMÁTICOS.

A) Concepto de Delito.

El artículo séptimo del Código Penal Federal aún vigente y el ya derogado Código Penal para el Distrito Federal en materia de fuero común y para toda la República en materia de Fuero Federal definía como delito: "Delito es el acto u omisión que sancionan las leyes penales", un término que ha quedado obsoleto, no solo por no haberse incluido en el Nuevo Código Penal vigente párale Distrito Federal, sino por el concepto tan simple que se da del mismo.

En términos más detallados y de acuerdo con lo manifestado por el maestro DÍAZ DE LEÓN, el mismo define el término DELITO en los siguientes términos: "Acto u omisión que sancionan las leyes penales. Acción punible entendida como el conjunto de los presupuestos de la pena. Infracción culpable de la norma penal. Su concepto ha variado en el tiempo, según la doctrina y las legislaciones. Sin embargo, en términos generales, se le reconocen las siguientes características partiendo de su definición más común: Delito es la acción típica, antijurídica, culpable y punible; de esto se deduce: es una acción penal humana; lo que no es acción no interesa al Derecho Penal. Típica, porque la acción tiene que concordar con lo descrito en la norma peal. Antijurídica, porque la acción penal debe oponerse al orden jurídico penal vigente y no estar justificada por una causa de exclusión del injusto. Culpable, porque puede imputarse al autor, intencionado o

negligente, del delito cometido, dada la relación de causalidad existentes entre el agente y su acción. Punible porque está sancionado expresamente con una pena señalada en la norma penal. No obstante la multiplicidad de clasificaciones del delito, normalmente se reconocen los siguientes: dolosos, que son cometidos con conocimiento e intención de ejecutar la acción delictiva y de causar el daño efectuado; culposos, que se cometen al ejecutar un hecho negligentemente o sin prudencia; de lesión, que causan un daño directa y efectivamente (robo, homicidio, etcétera); de peligro, que no causan daño en el bien u objeto jurídicamente protegido, pero lo ponen en peligro inminente (abandono de persona y etcétera); instantáneos, la violación de la ley se extingue después de consumado el delito; permanentes, la violación perdura aún después de consumada la acción (rapto); formales, se consuman aunque no se haya producido el resultado dañosos (injurias, cheque); materiales, precisan que se realice el propósito del delito para su consumación (la muerte en el homicidio). ..." ([27]).

Para PAVÓN VASCONCELOS, en su diccionario de Derecho Penal refiere al término DELITO como: "Ordinariamente los códigos penales, al definir el delito, acuden a un concepto meramente formal del mismo. El artículo séptimo del Código Penal del Distrito Federal declara: "Delito es el acto u omisión que sancionan las leyes penales", definición que aceptan la gran parte de los códigos penales de los estados de la República. Igual fenómeno se opera en Códigos extranjeros y de manera ejemplificativa diremos que el artículo 1 del Código Penal Chileno lo define como: "Toda acción u omisión voluntaria penada por la ley", el

([27]) DÍAZ DE LEÓN, Op cit. páginas 582 y 583.

artículo 1 párrafo uno del Código Español precisa: "Son delitos o faltas las acciones u omisiones voluntarias penadas por la ley", noción que Rodríguez Devesa califica de "rancio abolengo", citando los conceptos de Aristóteles, San Agustín y santo Tomás, en los cuales se destaca la naturaleza voluntaria del delito (Derecho Penal Español, 1, página 326, séptima edición, Madrid, 1979). Tal concepto formal y genérico del delito, que vincula el hecho con la amenaza de pena, es también adoptada por muchos autores de la materia. Manzini lo estima el hecho para el cual es conminada una pena (Tratado de derecho Penal, 1. página 153, Ediar, Buenos Aires, 1948, trad. S. Sentis Melendo); Cuello Calón lo define formalmente como la acción prohibida por la ley bajo la amenaza de una pena, al considerar una noción verdadera del delito la suministra la ley al destacar la amenaza penal, sin la cual no hay delito, por inmoral y socialmente dañosa que sea una acción si su ejecución no ha sido prohibida por la ley bajo la amenaza de una pena (Derecho Penal, 1, página 281, décima cuarta edición, Bosch, Barcelona, 1964); G. Maggiore, lo estima toda acción legalmente punible (Derecho Penal, 1, página 251 editorial Temis, Bogotá, 1954), otros autores siguen el mismo camino y, en la doctrina alemana, antes de expresarse un concepto jurídico, material o dogmático del delito, se hace referencia a éste como al hecho punible (V. R. Maurach, Tratado de Derecho Penal, 1, p.p. 149-150, ediciones Ariel, Barcelona, 1962, trad. Juan Córdoba Roda; H. H. Jescheck, Tratado de Derecho Penal 1, p.p. 262 y ss. Bosch, Barcelona, 1981, trad. Mir Puig y F. Muñoz Conde).

La principal crítica a la definición formal del delito se apoya en la consideración, por una parte, de que al destacar en ella la amenaza de pena implícitamente se

otorga a ésta el carácter de elemento, cuando en realidad es una mera consecuencia del mismo y, por otra parte, su evidente tautología. Se acusa a éstas definiciones de tautológicas, dice Cousiño Mac Iver, "pues constituyen un verdadero círculo vicioso, ya que afirman –por una parte- que son delitos las acciones castigadas por la ley, y –por la otra parte- si se pregunta cuáles son las acciones castigadas por la ley, ellas responden que son delitos; o sea, repiten dos veces el mismo pensamiento sin aclarar nada en definitiva. Maggiore, observa que: "decir que el delito es un hecho castigado equivale a decir: el delito es el delito, sin avanzar un paso" y , agrega, que: "es la rueda de Ixión, que empujaba hacia delante, retrocede rondando por un plano inclinado". En la misma forma Beling, que se esforzó en reemplazar la alusión tautológica a la pena con la introducción, como elemento del delito, de la tipicidad, dice que definirlo como lo penado por la ley equivale a definir una vivienda como "una casa con comedor y dormitorio destinada a la habitación". Este reproche de tautología aparece con frecuencia en el pensamiento de los distintos autores, aún de los alemanes, como Mezger, fue formulado primeramente por Adolphe Franck provocando una airada y tardía réplica de Manzini, que lo llamó "profano de las ciencias jurídicas". Debe advertirse no obstante, que son también los numerosos los ius penalista que resisten las anteriores críticas, con valiosos argumentos como es el caso de Jiménez de Asúa y Blasco y Fernández de Moreda" (Derecho Penal Chileno, 1, p.p. 240-241 editorial jurídica de Chile, 1975). La inclusión en los Códigos de definiciones sobre el delito han sido cuestionadas. Los mismos autores del Código Penal de 1931 llegaron a admitir lo innecesario de la inclusión del artículo 7 definitorio de la infracción penal, por no reportar en su opinión utilidad alguna, y

por considerar además que, como toda definición resulta ser una síntesis incompleta (Ceniceros y Garrido, la ley penal Mexicana, p. 39, México, 1934). Abunda en tal punto de vista Luis Jiménez de Asúa, quien primeramente invoca la opinión de Rodolfo Rivarolo, para desatacar las dificultades que hay que vencer para definir el delito en cualquier plano, sea éste filosófico o "natural", e inclusive recuerda que "la cosa debe de preexistir a la definición y no ser creada por la definición misma". A opinión de Jiménez de Asúa, la innecesariedad de una definición en los Códigos radica en tales definiciones "nada enseñan a los doctos y nadan aclaran a los profanos" como ya lo había señalado Pedro Dorado Montero. A su entender, ésta afirmación se concreta a las definiciones que se hacen constar en los códigos, con relación al delito en general, pues la noción del delito puede ser construida científicamente con base en las disposiciones del propio ordenamiento jurídico. "Frente a la afirmación de que los legisladores deben de abstenerse de dar un concepto general del delito, faena propia del tratadista, pero infructuosa en los Códigos, se han esgrimido otros argumentos. La precisión de las leyes y la fijeza de su interpretación exigen –a juicio de los partidarios de definir el crimen en general- que sepamos a que atenernos a los términos posiblemente engendradores de equívocos. Son varios los códigos que incluso dedican un capítulo o un determinado número de artículos, al definir los términos que se usan en el texto legal (el vigente Código suizo llega a definir qué se entiende por mujer para los efectos penales, Art. 110 número 1). No falta quienes añadan, apoyándose en una tesis que estuvo muy de moda en otros años, que las leyes son en los países de régimen constitucional especies de documentos contractuales en donde se determinan los derechos de cada parte, y deducen de

que la necesidad de que las facultades del poder y de los individuos queden bien delimitadas, separándose claramente lo lícito de lo ilícito..." ([28])

La teoría heptatómica del delito refiere siete elementos integrantes del mismo, siendo ésta la teoría aceptada por varios tratadistas del Derecho Penal, elementos que son:

a) Conducta
b) Tipicidad
c) Antijuridicidad
d) Imputabilidad
e) Culpabilidad
f) Condiciones objetivas de punibilidad
g) Punibilidad

Procediendo a dar un breve concepto de éstos elementos:

LA CONDUCTA, como lo refiere el maestro López Betancourt, "es el primer elemento básico del delito, y se define como el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito. Lo que significa que solo los seres humanos pueden cometer conductas positivas o negativas, ya sea una actividad o inactividad respectivamente. Es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito, porque tiene una finalidad al realizarse la acción u omisión." ([29])

La conducta puede ser de acción o de omisión y esta última se subdivide en omisión simple y comisión por omisión.

([28]) PAVÓN VASCONCELOS, páginas 295 y 296.
([29]) LÓPEZ BETANCOURT, Eduardo. Teoría del delito. 12ª edición. Editorial Porrúa, México 2004, página 83.

La conducta tiene tres elementos:

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

2) un resultado.

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

El acto, es el comportamiento humano positivo o negativo que produce un resultado. Positivo será una acción, que consiste en una actividad, en un hacer; mientras la omisión es una inactividad, es cuando la ley espera una conducta de un individuo y éste deja de hacerla.

Delito de Acción: La acción se define como aquella actividad que realiza el sujeto, produciendo consecuencias en el mundo jurídico, en dicha acción debe de darse un movimiento por parte del sujeto, de esta manera, la conducta de acción tiene tres elementos:

a) movimiento;

b) resultado;

c) relación de causalidad.

La acción en sentido estricto, es la actividad voluntaria realizada por el sujeto, consta de un elemento físico y de un elemento psíquico, el primero es el movimiento y el segundo la voluntad del sujeto, esta actividad voluntaria produce un resultado y existe un nexo causal entre la conducta y el resultado. Dicho resultado de la acción debe ser sancionado por la ley penal, es decir, deberá configurar un delito descrito y penado en la ley, será intrascendente que lesione

intereses jurídicos protegidos por la ley o sólo los ponga en peligro según el tipo penal.

LA TIPICIDAD.

Como lo refiere el maestro López Betancourt, "La tipicidad es la adecuación de la conducta al tipo penal" ([30])

LA ANTIJURIDICIDAD.

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

La antijuridicidad es lo contrario a Derecho, por lo tanto, no basta que la conducta encuadre en el tipo penal, se necesita que esta conducta sea antijurídica, considerando como tal, a toda aquella definida por la ley, no protegida por causas de justificación, establecidas de manera expresa en la misma.

LA CULPABILIDAD.

Refiere el maestro Sergio garcía Ramírez que "la culpabilidad constituye uno de los más complejos temas del Derecho Penal. Las caracterizaciones son diversas y afectan la estructura del delito y la ubicación, en ésta, el dolo y la culpa. La

([30]) Ibidem, página 117

concepción psicológica entiende que la culpabilidad estriba en el nexo psíquico entre el sujeto y el hecho delictuoso. La concepción normativa destaca la contradicción entre la voluntad del agente y la norma jurídica, contrariedad que genera un juicio de reproche. La teoría de la acción finalista retira el dolo y la culpa de la culpabilidad, los ubica en la acción y entiende que aquélla es un mal uso de las facultades del agente.

Aquí rige el principio *nullum crime sine* culpa. A nadie puede serle atribuido un delito, con las consecuencias respectivas, si no hay culpabilidad de su parte. Se quiere evitar las consecuencias autoritarias que derivarían de una opinión contraria: delito sin culpabilidad" ([31])

LA PUNIBILIDAD.

La punibilidad es un elemento secundario del delito, que consiste en el merecimiento de una pena, en función o por razón de la comisión de un delito; dichas penas se encuentran señaladas en nuestro Código Penal. Cuello Calón, considera que la punibilidad no es más que un elemento de la tipicidad, pues el hecho de estar la acción conminada con una pena, constituye un elemento del tipo delictivo.

LA IMPUTABILIDAD.

La imputabilidad es la capacidad de querer y entender, en el campo del Derecho Penal. Querer es estar en condiciones de aceptar o realizar algo voluntariamente y

([31]) GARCÍA RAMÍREZ, Sergio. Panorama del Derecho Penal Mexicano. Editorial Mc Graw Hill, México, 1998, página 67.

entender es tener la capacidad mental y la edad biológica para desplegar esa decisión.

CONDICIONES OBJETIVAS DE PUNIBILIDAD.- López Betancourt refiere al respecto que "... Jescheck considera a las condiciones objetivas de punibilidad, como circunstancias que se hallan fuera del tipo injusto y del de culpabilidad, pero de cuya presencia dependen la punibilidad del hecho y la posibilidad de la participación." ([32])

B) Características.

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.

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.

([32]) López Betancourt, Op. Cit. página 247

Carlos Sarzana, en su obra Criminalista y tecnología, indica que 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, como mero símbolo" ([33])

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas" ([34])

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" ([35])

María de la Luz Lima dice que el "delito Electrónico" "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las

([33]) SARZANA, Carlo. "Criminalità e tecnologia" en "Computers Crime, Rassagna Penitenziaria e Criminología". Números 1-2 Año 1. Roma, Italia. Página 53.

([34]) CALLEGARI, Lidia. "Delitos informáticos y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985. página 115.

([35]) FERNÁNDEZ CALVO, Rafael. "El tratamiento de llamado "delito informático" en el proyecto de ley Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática" en Informática y Derecho. Página 1020

computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin" ([36])

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 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, a través de las cuales se hace uso indebido de cualquier medio informático para la intromisión a éstos sistemas de cómputo protegidos o no, con independencia si se obtiene o no un lucro.

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.

---

(36) LIMA DE LA LUZ, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio 1984 página 85.

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 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".

Según Téllez Valdés, este tipo de acciones presentan las siguientes características principales (Cfr.):

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.

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.

Carlos Correa refiere al respecto en relación a los delitos informáticos que: "Conforme a una definición abarcante de la Organización para la cooperación económica y el Desarrollo, delito informático ("computer crimini") es "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático" ([37])

([37]) CORREA M. Carlos, Derecho informático, Ediciones De palma, Buenos Aires Argentina 1987, página 295.

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 policiales encargadas de las investigaciones y los funcionarios judiciales.

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.

C) Delito con medios informáticos y

contra medios informáticos.

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

Dentro de este tipo de delitos o infracciones podríamos destacar:

1.- Acceso no autorizado
2.- Destrucción de datos
3.- Infracción de los derechos de autor
4.- Infracción del copyright de bases de datos
5.- Interceptación de e-mail
6.- Fraudes electrónicas
7.- Transferencias indebidas de fondos
8.- La alteración y modificación de datos

Los delitos contra medios informáticos se refieren en síntesis a todas aquellas conductas que tienen como objetivo la inestabilidad o tomar el control de algún medio electrónico, ya sea con la finalidad de obtener un beneficio o no.

Las conductas que se mencionan como contra medios informáticos podemos resumirlas como aquellas que se realizan en contra de los computadores o sistemas de informática a fin de obtener información o bien sabotear la misma, ello a fin de obtener u lucro o no, la obtención de información sin consentimiento del

que legalmente la pueda dar; en tanto que los delitos cometidos con medios informáticos se les llama a aquellos que se cometen con el uso de las nuevas tecnologías, siendo éstos incluso delitos de los llamados comunes o clásicos, pero con el apoyo de las nuevas tecnologías para la comisión de los mismos, tales como el delito de amenazas o de hostigamiento sexual que se puede realizar a través del correo electrónico, por el teléfono celular a través del uso de mensajes escritos (SMS).

D) Elementos del delito Informático a la luz de la Teoría heptatómica del delito.

Es necesario, antes de todo, el definir éstas conductas, desde luego como un delito, pues aunque varias de éstas conductas se encuentran señaladas en el Código Penal Federal, existen otras conductas comunes que aún no son consideradas como delitos, por lo que acreditamos así la existencia de una conducta, sin embargo, no es una conducta que se considere un delito.

Las conductas diversas donde se refiere a los sistemas informáticos son muchas y de las cuales tenemos principalmente:

CyberGrafitti - Defacements - Web Hacks
CyberStalking (CiberAcoso)
CyberTerrorism (CiberTerrorismo)
CiberTerrorismo * Hacktivismo Zapatista
Domain Name Service Hacks (Hacking de un servicio de Nombres de Dominio)
Electronic Fraud (Fraudes Electrónicos)
Hacktivismo (Hacking + Activismo)
ID Theft (Robo de identidad)

Phreaking / Phreaks (Hacking o Cracking Telefónico)
Social Engineering (Ingeniería social)
Warez (Piratería)

Se ha hablado en el presente trabajo de la teoría heptatómica, es decir, de la existencia de siete elementos del delito los cuales son: 1.- la conducta, 2.- la tipicidad, 3.- la antijuridicidad, 4.- Imputabilidad, 5.- Culpabilidad, 6.- Condicionalidad objetiva y 7.- Punibilidad.

En el mayor de los casos de éste tipo de conductas es de acción, pues se requiere la intervención y el ánimo del activo para su realización, así, se habla de la voluntad del querer realizarlo en todas las conductas que se describen en líneas anteriores, solo en algunos casos, no se requiere la voluntad, hablemos del caso del borrado imprudencial de archivos o de algún código fuente de archivos, lo cual no permite la ejecución de algún programa o el funcionamiento correcto del mismo, o en su defecto en general de cualquier sistema informático.

No se puede hablar de tipicidad, pues si bien es cierto, se trata de conductas en su mayoría dolosas o intencionales, lo cierto lo es también que la mayoría de las mismas no se encuentran tipificadas por la norma penal, razón por la que al no encontrarse tipificadas por la norma penal y ante la ausencia de uno de los elementos del delito, tal conducta no se puede considerar un delito.

E) Formas de comisión del Delito.

Como se ha venido mencionando en los capítulos anteriores, el artículo 7° del Código Penal Federal, aduce: "Delito es el acto u omisión que sancionan las leyes penales". Los delitos pueden ser: I. Dolosos; II. Culposos. El delito es doloso cuando el agente quiere o acepta el resultado, o cuando éste es consecuencia necesaria de la conducta realizada. El delito es culposo cuando habiéndose previsto el resultado, se confió en que no se produciría; cuando se causó por impericia o ineptitud.

Para Marco Antonio Díaz de León "el dolo constituye una de las formas de culpabilidad, la más grave y tiene como fundamento la voluntad del agente; en relación con éste grado, sin dolo o intención, no hay culpabilidad y por tanto hecho punible." ([38])

Luis C. Pérez indica que "la culpa representa la otra forma de actividad psíquica en personas normales, en la cual, a diferencia del dolo, el agente ocasiona un resultado de daño o de peligro, no querido por él, que en efecto únicamente de su imprevisión, negligencia, impericia o de una simple violación de reglamentos; pero, en esencia, la culpa es imprevisión de las consecuencias posibles." ([39])

([38]) DÍAZ DE LEÓN, Marco Antonio. Op. Cit, página 634.
([39]) PÉREZ, Carlos Luis. Tratado de Derecho penal tomo I. Editorial Tamis, Bogotá Colombia 1967, página 558.

Por ello, podemos indicar que la forma de comisión de éstos, se puede realizar tanto dolosa como culposamente, pues como se señala, con el dolo se requiere la intención del sujeto activo, que es la mayor de las conductas que se señalan como posibles "delitos informáticos" o actividades ilícitas relacionadas con los sistemas informáticos, pues en el mayor de los casos tales conductas se realizan con el afán de causar el daño, de realizar la intromisión o simplemente para experimentar algo nuevo, empero, la comisión de algunas de éstas conductas, por la simple negligencia o impericia, se pueden generar.

G) Bien Jurídico Tutelado.

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

Referente a la penalidad que pretendo se imponga por este tipo de conductas, creo que es la adecuada, ya que como mencioné en líneas precedentes, es importante que se proteja la base de datos que pudiera tener una persona, ya que

ésta es confidencial, lo cual atacaría el bien jurídico tutelado de la *privacidad*, y por las características de dicha conducta, además pueden provocar pérdidas económicas, con o sin un beneficio para los que la cometen; pudiendo ser cometidos imprudencialmente, pero en la mayoría de los casos, es una conducta que se realiza con la intención de transformar o difundir una información contenida en una base de datos; siendo importante señalar que son muchos los casos en que se produce este tipo de conductas, por lo cual consideramos adecuada se tipifiquen tales conductas. Al respecto, de no imponer una sanción menor es porque se ha visto en la práctica desafortunadamente que la imposición de sanciones menores no desalienta la comisión de estos delitos, es por ello que sancionar con una pena más elevada implica que el sujeto, en caso de que realice su conducta e intente hacerlo de nuevo es sabedor de que será una pena elevada que le causará más perjuicio, que el beneficio que haya obtenido de su conducta.

Ahora bien, como se desprende de lo anterior, el bien jurídico tutelado, en los llamados "delitos informáticos" lo es desde el patrimonio en los fraudes electrónicos, la sustracción de tiempo aire de servicios celulares o de uso de internet, etcétera, la propiedad intelectual, el daño a la propiedad para el caso de que los documentos electrónicos puedan ser susceptibles de valorar, así como también y más importante lo es, el derecho de la intimidad.

Así, ya se señala en el artículo 16 constitucional párrafo noveno el cual señala: "Las comunicaciones privadas son inviolables. La Ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas.

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente, por escrito, deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.", así el párrafo duodécimo señala: "La correspondencia que bajo cubierta circule por las estafetas, estará libre de todo registro, y su violación será penada por la ley.", desprendiéndose de ello la imperiosa necesidad de que el derecho a la intimidad y la privacía sea tutelado por la ley penal.

Sin en cambio, el uso del correo electrónico ha desplazado notablemente el uso del correo ordinario para la comunicación personal, así como también que las comunicaciones de voz han aumentado su uso con la aparición de los teléfonos celulares, por lo que éste tipo de comunicaciones son aún más fácil de interceptar o desviar, que el correo ordinario, por ello la imperiosa necesidad de que se regulen tales comunicaciones, a fin de que no quede el derecha de la intimidad en peligro de cualquier persona.

La intercepción e intromisión en las comunicaciones privadas de teléfonos celulares no son la excepción, pues incluso existen diversas maneras de

interceptar tales comunicaciones y a manera de ejemplo tenemos en la página electrónica www.la_biblia_de_los_motorola.com.es una manera de realizar tal intromisión a una llamada privada, señalándose así que: "ESCUCHAR LLAMADAS EN MOTOROLA Y HABLAR CON ELLOS Sólo funciona en teléfonos Motorola y en algunos casos nada mas. Cuando la radio base o los celulares participantes no están muy distanciados entre si. Si tienes cualquier teléfono analógico, desde el tortuga (PT500) hasta el StarTAC. Presiona Fcn 0 0 * * 8 3 7 8 6 6 3 3 Sto, aparecerá una secuencia de números, ahora presiona # aparecerá u5', vuelve a presionar 1 1 3 0 0 # 0 8 #, Comenzarás a escuchar conversaciones, las instrucciones de arriba muestran como escuchar el canal 300, pero hay mas canales disponibles en equipos Motorola. Ejemplo: 1 1 x x x # 0 8 # Donde las x representan el canal que quieres escuchar Hay tres posibilidades para cada canal: Que sea un canal de voz: En este caso escucharás lluvia o una conversación en curso. Si es lluvia espera ú orienta la antena del equipo hacia otras direcciones. Que sea un canal de datos. En este caso no escucharás otra cosa que la señal de los modems, por lo que no hay (por ahora) nada interesante en esto. Que sea un canal muerto. En este caso no escucharas absolutamente nada. El parlante queda completamente mudo. Este canal no sirve en tu caso. Para salir de este modo basta con apagar el equipo (con la tecla PWR) o con marcar la secuencia 0 1 # lo que hará que el teléfono se re-inicie (es como apagarlo y prenderlo nuevamente). Cosas que debes saber: Estando el teléfono en este modo no pagas nada, es mas el teléfono (para el que te llame en ese momento) aparece como apagado. Dado que dejó de ser un teléfono las teclas Send y End ya no cumplen función alguna. Lo mismo sucede con la tapa. No

importa que esté abierta o cerrada. Si tienes un teléfono con salida de manos libres personal lo puedes conectar al equipo de audio y grabar conversaciones. Estando en escucha de conversaciones el equipo no controla el estado de carga de la batería. Si la tienes muy baja es posible que se dañe el equipo. Por ello es recomendable cargarla a full antes de escuchar o usarlo con el cargador conectado. Las escuchas telefónicas están penadas por la ley en varios países. Nosotros solo ponemos esto aquí para que te des cuenta como te están mintiendo las empresas de telefonía celular al prometerte privacidad. Estando en una escucha basta con marcar 0 5 # 1 0 # y hablar como todos los días. Los otros dos que suponían, de esta forma, para escuchar una determinada conversación hay que marcar: Fcn 0 0 * * 8 3 7 8 6 6 3 3 Sto # 1 1 7 9 9 # 0 2 # 0 8 y comenzaremos a escuchar algo. Para participar habrá que marcar luego: 0 5 # 1 0 # y lo que digamos los otros dos lo escucharán. Ahora, ¿sigues pensando que el celular es tan seguro como dijo quien te lo vendió?"

Obteniendo la anterior información de un portal de Internet que sin en cambio es de fácil acceso, no se requiere mayor capacitación para hacer lo que se indica en el mismo, señalándose incluso en páginas similares, la misma realización de conductas pero con el uso de diversos teléfonos celulares ellos de la marca Ericsson, que en su momento cuando salen al mercado y como se señala en éstas páginas se introduce un sistema para "modo de prueba", el cual al quedar abierto se podía escuchar las conversaciones de otros teléfonos celulares, mismo sistema que se introduce a fin de realizar pruebas para el caso de alguna reparación, actualmente, la mayoría de teléfonos, ya no cuentan con éste modo de prueba,

pues los fabricantes se dieron cuenta que con el mismo se podían escuchar las conversaciones.

H.- Delitos, comisión y técnicas nuevas.

Los adelantos tecnológicos y el conocimiento de nuevas técnicas ha originado que los delitos se cometan con nuevas técnicas, no debiendo confundir los delitos comunes que gracias a los adelantos tecnológicos se cometen de nuevas maneras con los llamados delitos informáticos, a manera de ejemplo podemos especificar los delitos comunes como el robo, que debido al uso de los teléfonos celulares tan común, los sujetos activos tenían mayores formas de comunicación, actualizándose así la Ley prohibiendo incluso posteriormente el uso de teléfonos celulares y aparatos de comunicación dentro de las instalaciones bancarias.

A manera de resumen podemos señalar respecto a éste capítulo que por cuanto hace al concepto de delito se entiende como la conducta típica, antijurídica y culpable sancionada por las leyes penales o los ordenamientos jurídicos aplicables, definiéndose así un concepto de delito únicamente para efectos del presente trabajo de investigación, señalándose de igual manera la comisión de ciertas conductas –la mayoría aún no tipificada por la ley-, las cuales se cometen en contra de los nuevos sistemas que se han creado, así como de las conductas y tipificadas por la ley pero que encuentran otro medio de comisión mediante el uso de nuevos sistemas electrónicos o informáticos, señalándose así la necesidad de adecuar tales conductas y no dejar lagunas en la ley que solo provoquen la

impunidad de éstos actos, pues no es posible aplicar la ley por simple analogía, tal y como se señala en el artículo 16 de nuestra carta magna.

De igual manera se establece el delito informático, precisamente como aquéllas conductas que se cometen mediante el uso de éstos sistemas informáticos, las cuales deben de quedar definidas y adecuadas a la norma penal vigente.

CAPITULO IV
ANTECEDENTES DEL INTERNET Y LAS PRINCIPALES CONDUCTAS DELICTIVAS.

A) Antecedentes del Internet.

Es preciso señalar la diferencia existente entre la Red y la Web. La primera, es una red de redes, básicamente hecho de PC´s y cables que envían paquetes de datos a cualquier parte del mundo. El WWW. (world wide web) cuya traducción literaria es "mundo ancho telaraña" es abstracto (imaginario) un espacio de información, en donde las conexiones son uniones entre hipertextos. En la Web se encuentran documentos, sonidos, videos, información. La Web no podría existir sin la red y hace la red útil, ambos conceptos web y red definen al Internet. Internet se inició en 1967 a raíz del diseño de la Red ARPANET -Agencia para el Desarrollo de Proyectos de Investigación Avanzada- del Departamento de Defensa de los EE.UU. Dicha red unía universidades y redes de ordenadores de titularidad militar, contratistas de defensa y laboratorios universitarios que realizaban investigaciones militares. Esta red permitió, posteriormente, a los investigadores de todo Estados Unidos acceder directamente a los ordenadores de gran potencia que se localizaban únicamente en algunas universidades y laboratorios.

Los orígenes de Internet se remontan a casi cuarenta años atrás, como un proyecto de investigación en redes de conmutación de paquetes, dentro de un

ámbito militar. A finales de los años sesenta (1969), en plena guerra fría, el Departamento de Defensa Americano (DoD) llegó a la conclusión de que su sistema de comunicaciones era demasiado vulnerable. Estaba basado en la comunicación telefónica (Red Telefónica Conmutada, RTC), y por tanto, en una tecnología denominada de conmutación de circuitos, (un circuito es una conexión entre llamante y llamado), que establece enlaces únicos y en número limitado entre importantes nodos o centrales, con el consiguiente riesgo de quedar aislado parte del país en caso de un ataque militar sobre esas arterias de comunicación.

Como alternativa, el citado Departamento de Defensa, a través de su Agencia de Proyectos de Investigación Avanzados (Advanced Research Projects Agency, ARPA) decidió estimular las redes de ordenadores mediante becas y ayudas a departamentos de informática de numerosas universidades y algunas empresas privadas. Esta investigación condujo a una red experimental de cuatro nodos, que arrancó en Diciembre de 1969, se denominó ARPAnet. La idea central de esta red era conseguir que la información llegara a su destino aunque parte de la red estuviera destruida. ARPA desarrolló una nueva tecnología denominada conmutación de paquetes, cuya principal característica reside en fragmentar la información, dividirla en porciones de una determinada longitud a las que se llama paquetes. Cada paquete lleva asociada una cabecera con datos referentes al destino, origen, códigos de comprobación, etc. Así, el paquete contiene información suficiente como para que se le vaya encaminando hacia su destino en los distintos nodos que atraviese. El camino a seguir, sin embargo, no está preestablecido, de forma que si una parte de la red cae o es destruida, el flujo de

paquetes será automáticamente encaminado por nodos alternativos. Los códigos de comprobación permiten conocer la pérdida o corrupción de paquetes, estableciéndose un mecanismo que permite la recuperación.

El Internet como un medio comercial y de fácil uso de comunicación tiene su auge a principios del año de 1995, cuando la transferencia de datos se puede realizar a través de protocolos TCP/IP comerciales, es decir, a través de la conexión de una línea telefónica, un fax módem y una suscripción de servicio de proveedor de TCP/IP, el proveedor de servicio de internet, el cual proporciona el número telefónico al cual ha de marcarse, un nombre de usuario y una contraseña.

A manera de definición, podemos señalar que el Internet es "un conjunto de servidores de archivos distribuidos en todo el mundo e interconectados mediante un sistema maestro de redes de cómputo. Cumple con dos funciones básicas: Medio de comunicación y medio de información. Realiza la primera mediante el correo electrónico, los foros de discusión y el servicio de llamadas telefónicas. Como medio de información, Internet sin duda es el centro de documentación más grande y completo del mundo, a tal grado que puede comparársele con una inmensa biblioteca a la que se tiene acceso prácticamente desde cualquier computadora del mundo conectada a ella. Sin embargo, en una biblioteca sólo las autoridades tienen la facultad de introducir nuevos libros o documentos; en

cambio, Internet permite que los usuarios introduzcan libremente información, lo que propicia un crecimiento enorme e ininterrumpido del acervo disponible" ([40])

B) Conductas delictivas comunes.

Las conductas delictivas comunes son las de la intromisión a los sistemas informáticos que comúnmente NO se encuentran protegidos por ningún medio de seguridad, lo que es el caso común de más de la mitad de usuarios de computadoras a nivel personal, incluso tales conductas no tienen el propósito de realizar inicialmente la conducta delictiva, sin embargo ante el creciente número de actividades relacionadas con las computadoras, es fácil encontrar portales creados o dedicados a los "hackers", encontrando en internet u portal destinado a poner de manifiesto la vulnerabilidad de los principales sistemas operativos que se usan actualmente, siendo el más gravemente señalado el Windows en sus versiones 98, 2000 y XP, siendo éste portal el: http://www.hardhack.f2s.com/shadycenter/index2.html, y el cual al ingresar al mismo señala lo siguiente:

ATENCION: Toda la información y el software que encontrarás aquí, únicamente está permitido utilizarlos con fines educativos, no haciéndonos responsables del mal uso, que por desconocimiento o malicia, se pudiera hacer. Tampoco nos responsabilizamos de los daños ocasionados por una utilización inapropiada o con

([40]) ROJAS AMANDI, Víctor Manuel, El uso de internet en el Derecho, segunda edición, editorial Oxford, México 2001, página 1.

fines delictivos. Con este site no se pretende fomentar, ni la violencia, ni una conducta ilegal, sino dar a conocer el fascinante mundo de la informática, la electrónica y las telecomunicaciones.

De igual manera, al ingresar a éste portal se hace la mención de "NOTA IMPORTANTE: Asegúrate de que la conducta que estás realizando no sea considerada un crimen en el país donde estás"

Sin embargo, es indispensable señalar que la realización de tales conductas en nuestro país en efecto no están completamente delimitadas como delito, lo que deja abierta la posibilidad a los llamados ciber delincuentes a realizar as mismas, sin la preocupación de ser detenidos por tales conductas.

A manera de resumen, podemos señalar que las conductas delictivas comunes consisten en:

1. El acceso no autorizado; es decir, el acceso sin derecho a un sistema o a una red informáticos violando medidas de seguridad ;
2. El daño a los datos o a los programas informáticos, como la descomposición, el deterioro, la supresión de datos o de programas informáticos sin derecho a ello ;
3. El sabotaje informático que consiste en introducir, alterar, suprimir datos o programas informáticos, con la intención de obstaculizar el funcionamiento de un sistema de computadoras o de telecomunicaciones;

4. La intercepción no autorizada, es decir, la interceptación realizada sin autorización y por medios técnicos, de comunicaciones destinadas a un sistema o a una red informáticos, provenientes de ese sistema o esa red o efectuados dentro de dichos sistemas o red;
5. El espionaje informático, es decir, la adquisición, la revelación, la transferencia o la utilización de un secreto comercial sin autorización o justificación legítima, con la intención de causar una pérdida económica a la persona que tiene derecho al secreto o de obtener un beneficio ilícito para sí mismo o para una tercera persona; y
6. El espionaje informático consistente en la intromisión a sistemas de cómputo violando la intimidad personal del usuario.
7. El robo de servicios, ya sea de tiempo de internet, de señales de cable, etcétera.

C) El derecho de la Privacidad.

El creciente número de funciones que desempeña una computadora entendiéndose por ésta última la máquina que se encarga de "computar", es decir, de realizar operaciones de cálculo, términos que desde luego ha quedado obsoleto, adoptando el término actualmente en algunos países como España con el de "procesador", lo cual ha sido más aceptado, pues el mismo no solo se usa para la realización de cálculos, sino para el almacenamiento y control no solo de información, sino también de documentos de diversos tipos, como lo son archivos

de audio, de video, imágenes, fotografías personales, de negocios, documentos de texto, de hojas de cálculo, etcétera, un sin fin de archivos y documentos que se pueden almacenar en el procesador que el dejarlo a la vista y dominio de alguien no autorizado podría ser perjudicial.

En el orden de ideas del párrafo anterior, la privacidad es uno de los valores del ser humano y como se señala en las líneas anteriores, el dejar expuesta la misma, debido a nuestros documentos o imágenes, desde luego deber de ser tutelado por la ley penal, establecido así en el artículo 16 constitucional en su párrafo noveno.

Podemos señalar de igual manera que la necesidad de intimidad es inherente a la persona humana ya que para que el hombre se desarrolle y geste su propia personalidad e identidad es menester que goce de un área que comprenda diversos aspectos de su vida individual y familiar que esté libre de la intromisión de extraños. Así pues, debemos entender que todos los seres humanos tenemos una vida "privada" conformada por aquella parte de nuestra vida que no está consagrada a una actividad pública y que por lo mismo no está destinada a trascender e impactar a la sociedad de manera directa y en donde en principio los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia, ni les afectan.

Ciertamente el concepto de vida privada es muy difícil de definir con precisión pues tiene connotaciones diversas dependiendo de la sociedad de que se trate, sus circunstancias particulares y la época o el periodo correspondiente.

Sin embargo, dentro de esta esfera de vida privada podemos considerar a las relaciones personales y familiares, afectivas y de filiación, las creencias y preferencias religiosas, convicciones personales, inclinaciones políticas, condiciones personales de salud, identidad y personalidad psicológica, inclinaciones sexuales, comunicaciones personales privadas por cualquier medio, incluso algunos llegan a incluir la situación financiera personal y familiar.

Que la información contenida en un computador, actualmente es tan amplia que no solo se almacenan documentos, hojas de cálculo y documentos electrónicos, sino también para la mayoría de usuarios, también se almacenan imágenes, documentos personales, privados, etcétera, documentos que al quedar expuestos, constituyen la violación a la intimidad de las personas.

D) El delincuente informático.

A continuación se señala una lista de las conductas comunes realizadas por los "delincuentes informáticos"

Cracking ó Cracker.

Derivado del hacking. Persona que sin derecho penetra un sistema informático con el fin de robar o destruir información valiosa, realizar transacciones ilícitas, o impedir el buen funcionamiento de redes informáticas o computadoras. Alguien que viola la seguridad en un sistema. Este término fue acuñado por los hackers

para defenderse del mal uso periodístico del término "Hacker". El término "cracker" refleja la gran revulsión a los actos de robo y vandalismo perpetrados por los círculos de criminales conocidos como crackers.

CyberGangs (CiberPandillas)

Grupos de hackers o extremistas se reúnen para cometer o planear delitos, o para expresar ideas racistas, discriminatorias o xenofóbicas.

CyberGrafitti - Defacements - Web Hacks

Tipo de hacking más común. Hackers que penetran sitios web sin derecho para modificar su contenido, desplegando imágenes obscenas, amenazas, mensajes ridiculizantes, burlas, etcétera. Esta práctica es el equivalente del grafitti callejero que todos conocemos pero llevada a cabo en línea, es por eso que algunos expertos en seguridad informática han bautizado a los individuos que realizan este ilícito como "ciber-cholos".

CyberStalking (CiberAcoso)

Acosar, hostigar, molestar, intimidar o amenazar personas o entidades usando medios informáticos. El CiberAcoso puede ser definido como la conducta amenazante o aproximaciones no deseadas dirigidas a otra persona usando el Internet y otras formas de comunicación "en línea".

CyberTerrorism (CiberTerrorismo)

Aprovechamiento de las redes informáticas (Internet) para obtener información, fomentar o cometer actos de terrorismo. Los grupos extremistas, milicias y guerrillas pueden intentar ciberasaltos masivos contra el gobierno e infraestructura crítica de un país, como el transporte, la energía y servicios de emergencia.

CiberTerrorismo * Hacktivismo Zapatista

En el verano de 1998, un grupo denominado "Electronic Disturbance Theater (EDT)" llevó el concepto de "desobediencia civil electrónica" un paso más adelante. EDT organizó una serie de "ataques electrónicos" en contra de sitios web del Presidente Ernesto Zedillo, y del Presidente Bill Clinton (Pentágono y Casa Blanca), la Embajada Mexicana en Rusia, entre otros. El propósito era demostrar solidaridad con los Zapatistas Mexicanos.

El 15 de junio de 1999, el EDT empezó a enviar anuncios a través de emails incitando a miles de personas a que se uniera en un acto de Desobediencia Civil Electrónica para detener la guerra en Chiapas, México. Brett Stalbaum, uno de los líderes de EDT creó un programa de software llamado "The Zapatista FloodNet" para facilitar los ataques.

El 18 de junio 18,615 personas en 46 distintos países, apoyaron desde sus computadoras el ataque masivo ("mítin virtual") contra estos sitios de gobierno de México y Estados Unidos principalmente.

Ricardo Domínguez, neoyorquino de padres mexicano, es uno de los principales protagonistas del EDT. Domínguez, junto con miles de manifestantes y el EDT ha dirigido muchos ataques y mítines virtuales contra diferentes organismos y figuras de gobierno. Es uno de los primeros ciber-terroristas del planeta, según importantes fuentes de USA.

Domain Name Service Hacks (Hacking de un servicio de Nombres de Dominio)

Tipo de hacking. Además de la práctica conocida como defacement o web hacking, otra manera de alterar lo que los usuarios ven cuando entran a un sitio web es interfiriendo con el servicio de Nombres de Dominio (DNS) para que el Nombre de Dominio del sitio resuelva a la dirección IP de algún otro sitio, el cual podría ser pornográfico por poner un ejemplo. Si los usuarios teclean el nombre de dominio, los llevará a otro nombre de dominio, salvo que tecleen la dirección IP exacta, lo cual es muy poco probable.

Electronic Fraud (Fraudes Electrónicos)

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

- Subastas en línea
- Servicios de acceso a Internet
- Fraude con tarjeta de crédito
- Marcado internacional por módem
- Cargos "no autorizados" a tarjetas de crédito o recibos telefónicos (Web Cramming)
- Planes de mercadotecnia de multinivel (pirámides)
- Viajes y vacaciones
- Oportunidades de negocios
- Inversiones
- Productos y servicios relacionados con la salud

Hacking / Hacker

Individuo que sin derecho penetra un sistema informático sólo por gusto o para probar sus habilidades. Usualmente no tiene fines delictivos graves este tipo de intrusión.

Sin embargo, ellos mismos se definen como: 1. Una persona que disfruta el explorar detalles de sistemas programables y cómo maximizar sus capacidades; 2. Alguien que programa entusiastamente; 3. Una persona que es buena programando rápidamente; 4. Un experto en un programa particular, como un "hacker de Unix"; 5. De manera despectiva, un intruso malicioso que trata de

descubrir información sensible merodeando. Según ellos, el término correcto para esta definición despectiva es "cracker".

Hacktivismo (Hacking + Activismo)

Derivado del hacking. Uso de la red por grupos extremistas de cualquier tipo (políticos, religiosos, guerrillas, pro-derechos humanos, ambientalistas, etc.) para promover ciber-desobediencia civil o ataques en contra del gobierno. Algunos ejemplos de "ciber-guerra civil" son:

- 1995: Ciudadanos franceses e italianos protestaron contra las acciones y políticas de su gobierno sitiando la presencia de dichos gobiernos en internet.
- 1996: La Casa Blanca fue el blanco de una imensa tormenta de transmisión de correos electrónicos, cada uno conteniendo una copia del Bill of Rights. El objetivo era inhibir el sitio web de la presidencia.
- 1998: Una instalación nuclear de la India fue hackeada después de pruebas de armamento y bombas atómicas.
- Un grupo llamado "The Hong Kong Blondes" hackeo la red informática de la Policía China, como forma de protesta en contra de los arrestos políticos.
- 1999: El grupo "Electronic Disruption Theater", en apoyo a los Zapatistas Mexicanos, lanzó un ataque de "denegación de servicio" contra un sitio de información del Pentágono, usando la herramienta The Zapatista FloodNet.

La diferencia entre ciberterrorismo y hacktivismo es muy fina. En términos generales podemos decir que el fin último del ciberterrorismo es la destrucción física y/o electrónica de la infraestructura de un gobierno y su nación, y la motivación del hacktivismo es la protesta enérgica en contra del gobierno, la cual puede estar caracterizada por actos de "violencia electrónica".

ID Theft (Robo de identidad)

Aprovechamiento de datos personales obtenidos mediante engaños para hacerse pasar por otra persona, con el objeto de obtener beneficios económicos o cometer delitos.

Phreaking ó Phreaks (Hacking o Cracking Telefónico)

Penetrar ilícitamente sistemas telefónicos o de telecomunicaciones con el fin de obtener beneficios o causar perjuicios a terceros. Esta es una de las prácticas más antiguas en la historia del cibercrimen.

También se puede definir como el arte y ciencia de crackear una red telefónica (para, por ejemplo, hacer llamadas de larga distancia gratuitas). Por extensión, la violación de la seguridad en cualquier otro contexto, especialmente en redes de comunicaciones.

De los antecedentes no documentados y que han sido transmitidos a través de algunas páginas de internet que consultan los "phreaking ó phreaks", se cuenta la historia de los primeros sujetos que para obtener llamadas en los teléfonos públicos en Estados Unidos, imitaban ya sea por la voz o por algún otro medio

(aún no electrónico) el sonido de las monedas al entrar a la alcancía, para así poder hablar libremente, posteriormente se valían de pequeñas grabadoras o cables conectados a algún dispositivo de audio para así poder imitar éste sonido.

En la actualidad siguen predominando, aunque la técnica ya no se realiza con teléfonos públicos, sino con teléfonos celulares, consistiendo ésta conducta la de sustraer de la base de datos de las compañías de telefonía celular los códigos de acceso para la adquisición de tiempo aire (ello para los sistemas de pre pago), para así poder ingresar el llamado "saldo" al teléfono celular; éstas conductas, éste tipo de delincuente, ha quedado un poco atrás, pues esto lo realiza el "hacker", al acceder a las denominadas "páginas negras", las cuales son sitios que son conocidos por los expertos en materia de informática y que ninguna persona con conocimientos medios puede acceder, pues al tratar de ingresar a las mismas, existen sistemas de reconocimiento y protección de éstas páginas par evitar el acceso de personas extrañas, incluso con el riesgo de que al acceder, los datos de la computadora se vean dañados.

Desafortunadamente no existen muchos antecedentes de éste tipo de ataques, pues ello deja a la vista las fallas y deficiencias que pueden tener en algunas ocasiones los sistemas informáticos de las compañías telefónicas o de internet, pues es bien sabido de los "espacios" o "caídas del sistema" de las compañías celulares, teniendo como una de las compañías con más caídas en el sistema la compañía Telcel, sin embargo, no existe ninguna información documentada, de

igual manera se cuenta con los antecedentes de las llamadas cuentas piratas de internet, pero las mismas son compartidas en un espacio muy limitado, sin que de igual manera las compañías de servicio de internet lo den a conocer.

Social Engineering (Ingeniería social)

Muchos delincuentes, en lugar de aprovechar las debilidades de los sistemas informáticos, se aprovechan de las "debilidades mentales" de empleados de empresas o personas que puedan brindarles información que les ayude a penetrar sistemas informáticos. Estos criminales al usar esta técnica generalmente:

- Impersonan otros empleados de la misma empresa.
- Pretenden ser proveedores técnicos.
- Extorsionan o amenazan al personal.

Warez (Piratería)

Grupo de personas amantes de la piratería de software. Su meta es violar códigos de seguridad (cracking) o generar, obtener o compartir números de registro (regging) de programas de computo, para luego subirlos a Internet y compartirlos con el mundo.

Usualmente son delitos o ilícitos contra la Propiedad Intelectual o Derechos de Autor.

Es interesante además, la clasificación y características particulares de este tipo de conductas, y la relación de éstas con los tipos tradicionales, así como el perfil del delincuente informático (en especial el de los llamados *hackers*), los *virus* computacionales (un verdadero azote en la actualidad) y los mecanismos de prevención.

El perfil de los llamados delincuentes informáticos suele ser: jóvenes, con inquietud hacia los medios electrónicos y en el mayor de los casos con coeficientes intelectuales altos, con excepción de las conductas que se realizan por la imprudencia (por ejemplo el borrar el contenido de una computadora).

Señalando así y a manera de resumen que las conductas delictivas comunes por parte de los sujetos activos radican principalmente en el sujeto que:

1. Accese a información o a una computadora sin autorización o excediendo su acceso autorizado
2. Intercepte, modifique, altere, borre, destruya, provoque daño o pérdida de información contenida en computadoras o programas de cómputo.
3. Conozca, copie divulgue o distribuya a terceros información o comunicaciones no dirigidas a él, contenidas en computadoras.
4. Diseñe, introduzca programe, distribuya o provoque la transmisión o ejecución de programas de computación, datos, información, códigos, conjunto de instrucciones o comandos informáticos.

5. Diseñe, programe, comercialice, trafique, transmita, haga dispoinibles o distribuya programas de cómputo, números de serie o registro, palabras clave o códigos de acceso, o información de cualquier naturaleza que sirva para violar mecanismos de seguridad de computadoras o programas de cómputo;
6. Amenace, intimide, hostigue aceche o cause temor personas físicas o morales, mediante mensajes electrónicos, el uso de computadoras u otros mecanismos tecnológicos similares.
7. Obtenga sin consentimiento y/o mediante engaños datos o información personal de individuos para usarla con fines comerciales, obtenga un lucro directo o indirecto de dicha información, o la use o aproveche para cometer cualquier actividad ilícita.

Teniendo los sujetos que las realizan o en su caso por e modus operandi de los mismos, los nombres que se les han dado por costumbre dentro del ambiente informático, sin embargo, podemos señalar que el más usado es el concepto de Hacker o Cracker.

CAPÍTULO V
EL DELITO INFORMÁTICO EN EL DERECHO COMPARADO.

A) Antecedentes.

Refiere al respecto el maestro Téllez Valdés que: "Es indudable que así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un instrumento u objeto en la comisión de verdaderos actos ilícitos. Este tipo de actitudes concebidas por el hombre (y no por la máquina como algunos pudieran suponer) encuentran sus orígenes desde el mismo surgimiento de la tecnología informática, ya que es lógico pensar que de no existir las computadoras, estas acciones no existirían. Por otra parte, la misma facilitación de labores que traen consigo dichos aparatos propician que, en un momento dado, el usuario se encuentre ante una situación de ocio, la cual canaliza a través de las computadoras, cometiendo, sin darse cuenta, una serie de ilícitos. Por último, por el mismo egoísmo humano se establece una especie de "duelo" entre el hombre y la máquina, lo cual en última instancia provoca el surgimiento de ilícitos en su mayoría no intencionados, por ese "deseo" del hombre de demostrar su superioridad frente a las máquinas, y en éste caso específico las computadoras.

De esta forma podemos decir que éstas acciones, más que resultado de una situación socioeconómica se derivan de una actitud antropológica y psíquica,

aunque en el terreno de los hechos son una realidad sociológica bien determinada y que requiere, por ende, de un tratamiento jurídico específico." ([41])

B) Países Desarrollados.

Estados Unidos.

Este país adoptó en 1994 del **Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030)** que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa,. información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, 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. Definiendo dos niveles para el tratamiento de quienes crean virus:

a) Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.

([41]) Téllez Valdez, Op. Cit, página 103

b) Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

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.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

Alemania.

Este país sancionó en 1986 la **Ley contra la Criminalidad Económica**, que contempla los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

Austria.

La **Ley de reforma del Código Penal**, sancionada el 22DIC87, en el artículo 148, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

Gran Bretaña.

Debido a un caso de hacking en 1991, comenzó a regir en este país la **Computer Misuse Act** (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría.

El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

Holanda.

El 1° de Marzo de 1993 entró en vigencia la **Ley de Delitos Informáticos**, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

Francia.

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

Asimismo, esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte el artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros,

en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

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

Por último, esta ley en su artículo 462-2, sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

España.

En el Nuevo Código Penal de España, el art. 263 establece que el que causare daños en propiedad ajena. En tanto, el artículo 264-2) establece que se aplicará la pena de prisión de uno a tres años y multa... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión

y multa, agravándolas cuando existe una intensión dolosa y cuando el hecho es cometido por parte funcionarios públicos se penaliza con inhabilitación.

En materia de estafas electrónicas, el nuevo Código Penal de España, en su artículo 248, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

Internacionalmente, la Organización de las naciones Unidas reconoce las siguientes conductas como "DELITOS INFORMÁTICOS"

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.

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.

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.

Falsificaciones informáticas.

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

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.

Daños o modificaciones de programas o datos computarizados.

Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. las técnicas que permiten cometer sabotajes informáticos son:

Virus. 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.

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 tu

mor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

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

Acceso no autorizado a servicios y sistemas informáticos.

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

Piratas informáticos o hackers.

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

Reproducción no autorizada de programas informáticos de protección legal.

La reproducción no autorizada de programas informáticos puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna.

C) Países Subdesarrollados.

Los países sub desarrollados aún no cuentan con una legislación adecuada frente a los delitos informáticos, pues no se le ha dado el gran auge, algunos por lógica,

por tener una infraestructura escasa que no permite que el nivel adquisitivo de sus ciudadanos pueda adquirir algún tipo de sistema informático que permita a su vez que el usuario se familiarice con los ordenadores o computadoras.

Así tenemos a los siguientes países:

En la Argentina, aún no existe legislación especifica sobre los llamados ***delitos informáticos***. Sólo están protegidas las obras de bases de datos y de software, agregados a la lista de ítems contemplados por la Ley 11.723 de propiedad intelectual gracias al Decreto Nº 165/94 del 8 de febrero de 1994.

En dicho Decreto se definen:

Obras de software: Las producciones que se ajusten a las siguientes definiciones:

1. Los diseños, tanto generales como detallados, del flujo lógico de los datos en un sistema de computación.
2. Los programas de computadoras, tanto en versión "fuente", principalmente destinada al lector humano, como en su versión "objeto", principalmente destinada a ser ejecutada por la computadora.
3. La documentación técnica, con fines tales como explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento de software.

Obras de base de datos: Se las incluye en la categoría de "obras literarias", y el término define a las producciones "constituidas por un conjunto organizado de datos interrelacionados, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos".

De acuerdo con los códigos vigentes, para que exista robo o hurto debe afectarse una cosa, entendiendo como cosas aquellos objetos materiales susceptibles de tener algún valor, la energía y las fuerzas naturales susceptibles de apropiación. (Código Civil, Art. 2311).

Asimismo, la situación legal ante daños infligidos a la información es problemática:

- El artículo 1072 del Código Civil argentino declara *"el acto ilícito ejecutado a sabiendas y con intención de dañar la persona o los derechos del otro se llama, en este Código, delito"*, obligando a reparar los daños causados por tales delitos.

- En caso de probarse la existencia de delito de daño por destrucción de la cosa ajena, *"la indemnización consistirá en el pago de la cosa destruida; si la destrucción de la cosa fuera parcial, la indemnización consistirá en el pago de la diferencia de su valor y el valor primitivo"* (Art. 1094).

- Existe la posibilidad de reclamar indemnización cuando el hecho no pudiera ser considerado delictivo, en los casos en que *"alguien por su culpa o negligencia ocasiona un daño a otro"* (Art. 1109).

- Pero *"el hecho que no cause daño a la persona que lo sufre, sino por una falta imputable a ella, no impone responsabilidad alguna"* (Art. 1111).

- En todos los casos, el resarcimiento de daños consistirá en la reposición de las cosas a su estado anterior, excepto si fuera imposible, en cuyo caso la indemnización se fijará en dinero" (Art. 1083).

El mayor inconveniente es que no hay forma de determinar fehacientemente cuál era el estado anterior de los datos, puesto que la información en estado digital es fácilmente adulterable. Por otro lado, aunque fuera posible determinar el estado anterior, sería difícil determinar el valor que dicha información tenía, pues es sabido que el valor de la información es subjetivo, es decir, que depende de cada uno y del contexto.

Lo importante en este tema es determinar que por más que se aplique la sanción del artículo 72 de la ley 11723, la misma resulta insuficiente a efectos de proteger los programas de computación, los sistemas o la información en ellos contenidos de ciertas conductas delictivas tales como: el ingreso no autorizado, la violación de secretos, el espionaje, el uso indebido, el sabotaje, etc.

No obstante, existen en el Congreso Nacional diversos proyectos de ley que contemplan esta temática; aunque sólo dos de ellos cuentan actualmente con estado parlamentario. Los presentados por los Senadores nacionales Eduardo Bauza y Antonio Berhongaray, respectivamente.

Chile.

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

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

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

Venezuela

Venezuela es uno de las países más adelantados respecto a éste tema, con la creación de la ley federal contra los delitos informáticos, misma que señala la

clasificación de tales conductas, publicada en Caracas, Venezuela el 06 seis de septiembre del año 2001 constando de tres capítulos la cual podemos señalar lo siguiente: Ley Especial Contra los Delitos Informáticos

Título I. Disposiciones Generales

Artículo 1.- Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Artículo2.- Definiciones. A los efectos de la presente ley y cumpliendo con lo previsto en el art. 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por:

a. Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data.

b. Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c. Data: hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado.

d. Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e. Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

f. Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

g. Hardware: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus

componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

h. Firmware: programa o segmento de programa incorporado de manera permanente en algún componente de hardware.

i. Software: información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas.

j. Programa: plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.

k. Procesamiento de data o de información: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

l. Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.

m. Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

n. Tarjeta inteligente: rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

o. Contraseña (password): secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

p. Mensaje de datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

Artículo 3.- Extraterritorialidad. Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Artículo 4.- Sanciones. Las sanciones por los delitos previstos en esta ley serán principales y accesorias.

Las sanciones principales concurrirán con las accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley

Artículo 5.- Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.

La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

Título II. los delitos

Capítulo I

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información

Artículo 6.- Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Artículo 7.- Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

Artículo 8.- Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Artículo 9.- Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

Artículo 10.- Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Artículo 11.- Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12.- Falsificación de documentos. El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado

con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad.

El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Capítulo II De los Delitos Contra la Propiedad

Artículo 13.- Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 14.- Fraude. El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Artículo 15.- Obtención indebida de bienes o servicios. El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los

mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16.- Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. El que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penado con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Artículo 17.- Apropiación de tarjetas inteligentes o instrumentos análogos. El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario

autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Artículo 18- Provisión indebida de bienes o servicios. El que a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado, se haya indebidamente obtenido, retenido, falsificado, alterado, provea a quien los presente de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 19.- Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Capítulo III.- De los delitos contra la privacidad de las personas y de las comunicaciones

Artículo 20.- Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21.- Violación de la privacidad de las comunicaciones. El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22.- Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Capítulo IV De los delitos contra niños, niñas o adolescentes

Artículo 23.-Difusión o exhibición de material pornográfico. El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Artículo 24.- Exhibición pornográfica de niños o adolescentes. El que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Capítulo V.- De los delitos contra el orden económico

Artículo 25.- Apropiación de propiedad intelectual. El que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de

información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Artículo 26.- Oferta engañosa. El que ofrezca, comercialice o provea de bienes o servicios mediante el uso de tecnologías de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave. Título III

Otros países a pesar de encontrarse dentro del catálogo de los países sub desarrollados o en vía de desarrollo y contar con los medios necesarios a nivel mundial de tecnología personal y de sistemas, aún no lo contemplan con las consecuencias jurídicas que el uso de éstas tecnologías puede traer consigo, tal es el caso de nuestro país, pues aún no le ha dado la debida importancia a éste tema.

México

Solo el estado libre y soberano de Sinaloa contempla a los "delitos informáticos" estableciendo así en el artículo 217 del Código Penal de la entidad lo siguiente:

"Título Décimo.- Delitos contra el patrimonio .- Capítulo V, Delito Informático.
Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:

I. Use o entre a una base de datos, 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

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

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

El tipo penal que se define en el artículo anterior cumple con varios de los supuestos de los "delitos informáticos", sin embargo, a simple vista se puede apreciar que el mismo se encuentra dentro del catálogo de delitos patrimoniales, siendo esto incorrecto, pues con los delitos informáticos, no solo es el lucro el bien jurídico tutelado, sino son otros como ya se vio en el capítulo III del presente trabajo de investigación.

D) Código Penal Federal.

El Código Penal federal señala en su título noveno, capítulo II el "ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA" contiene los siguientes

numerales "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 equipo 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 copia información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de segurids del estudio de las conductas antijurídicas, típicas, culpables y punibles que involucran paas o equipos de informática del Estado, indebidamente modifique, as o 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 equipo de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

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

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

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

Al que estando autorizando para acceder a sistemas y equipo de informática de las instituciones que integran el sistema financiero, indebidamente copie

información que contenga, se le impondrá de seis meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en éste 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 éste Código.

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

"Artículo 400 bis.- ... Para los mismos efectos, el sistema financiero se encuentra integrado por las instituciones de crédito, de seguros y de fianzas, almacenes generales de depósito, arrendadoras financieras, sociedades de ahorro y préstamo, sociedades financieras de objeto limitado, uniones de crédito, empresas de factoraje financiero, casas de bolsa y otros intermediarios bursátiles, casas de cambio, administradores de fondos de retiro y cualquier otro intermediario financiero o cambiario."

Sin embargo, uno de los principales problemas que presentan los artículos referidos es que: para que se cometa el delito, los sistemas de cómputo deben de

encontrarse protegidos por algún sistema de seguridad y el usuario común, no cuenta con los medios de protección a sus sistemas de cómputo, además de que el mismo código no establece cuáles son ésos mecanismos de seguridad para proteger los sistemas informáticos.

E) Nuevo Código Penal para el Distrito Federal.

Por cuanto hace al nuevo Código Penal para el Distrito Federal publicado en la gaceta oficial del Distrito Federal en fecha 16 dieciséis de julio del año 2002 y el cual entró en vigor en fecha 12 doce de noviembre del año 2002, el cual abroga al anterior Código Penal para el Distrito Federal en materia de fuero común y para toda la República en materia de Fuero Federal del año de 1931 y el cual desde su publicación en el año de 2002 ha tenido 18 dieciocho reformas, siendo éstas de fechas 03 tres de octubre de 2002, 22 veintidós de abril de 2003, 15 quince de mayo de 2003, 13 trece de enero de 2004, 27veintisiete de enero de 2004, 29 veintinueve de enero de 2004, 04 cuatro de junio de 2004, 06 seis de septiembre de 2004, 13 trece de septiembre de 2004, 15 quince de septiembre de 2004, 15 quince de septiembre de 2004, 06 seis de octubre de 2004, 20 veinte de diciembre de 2004, 17 diecisiete de enero de 2005, 13 trece de mayo de 2005, y dos del 22 veintidós de julio de 2005.

Sin embargo, a pesar de tantas reformas en tan poco tiempo, no ha sido posible incluir un capítulo destinado para los "delitos informáticos", pues solo en el artículo 231 en su fracción XIV señala lo siguiente: Artículo 231.- ... XIV. Para obtener

algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución; o ..." no incluyendo ni siquiera los supuestos que señala el Código Penal Federal.

No adecuándose así, dentro del Código Penal Federal ni dentro del Nuevo Código Penal para el Distrito Federal toda la serie de conductas que se encuentran señaladas en otros códigos y que se encuentran delimitados como delitos informáticos.

CONCLUSIONES

PRIMERA.- Podemos concluir que ante los avances tecnológicos de nuestra era y ante el cambio constante y adelantos tecnológicos que con ello conlleva, pues el uso cada día más frecuente de sistemas de tecnología de la información, incluidos entre otros, los sistemas de telecomunicaciones e informáticos, permite procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza. Las más diversas áreas del conocimiento humano, están siendo incorporadas a sistemas informáticos, en lo científico, en lo técnico, en lo profesional y en lo personal, por lo que es necesario adecuar la normatividad jurídica acorde a tal rapidez de cambios.

SEGUNDA.- El desarrollo de las tecnologías de la información ha abierto las puertas a nuevas posibilidades de delincuencia. El acceso sin autorización (piratería informática), el sabotaje informático, la manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos, la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos, mediante los cuales es posible obtener grandes beneficios económicos.

TERCERA.- No existe un término aún exacto y mucho menos en la legislación mexicana que defina el concepto de "delitos informáticos" por lo que es necesario

que quede definido entendiendo para ello y para efectos de interpretación personal como: el conjunto de normas jurídicas encargadas del estudio de las conductas antijurídicas, típicas, culpables y punibles que involucran para su comisión el uso de cualquier sistema informático o tecnológico.

CUARTA.- la informática jurídica tiene tres divisiones, siendo éstas la informática jurídica documental, de control y gestión y la metadocumentaria o de control y decisión, siendo la primera de ellas la que se encarga de el almacenamiento y archivo de los documentos electrónicos, siendo éstos desde archivos de texto, ejecución, de imagen, video, audio, etcétera; la segunda de ellas se refiere a la ayuda que proporciona la informática al control de expedientes y escritos, en tanto que la tercera es la rama de la informática jurídica encargada del control de posibles decisiones tomados a través del ordenador, ingresando en éste previamente los datos para que ésta tome una solución que posiblemente se daría a un caso similar, aplicando para ello a lo que se denomina "inteligencia artificial", sin embargo, para efectos jurídicos no tiene aplicación, pues las determinaciones jurídicas que impliquen la vida, la libertad, los derechos, posesiones o derechos solo se deben tomar por parte del ser humano.

QUINTA.- Se señala como concepto de "delito informático" para efectos del presente trabajo como todas aquellas conductas ilícitas susceptibles de ser

sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático.

SEXTA.- Se señala como los principales conductas que pueden considerarse como "delitos informáticos" los siguientes: el acceso a información o a una computadora sin autorización o excediendo su acceso autorizado, la Intercepción, modificación, alteración, borrado, destrucción, provocación de daño o pérdida de información contenida en computadoras o programas de cómputo, conocimiento, copia, divulgación o distribución a terceros información o comunicaciones no dirigidas a él, contenidas en computadoras; Diseño, introducción programación, distribución o provocación de la transmisión o ejecución de programas de computación, datos, información, códigos, conjunto de instrucciones o comandos informáticos, Diseño, programa, comercialización, tráfico, transmisión, haga disponibles o distribuya programas de cómputo, números de serie o registro, palabras clave o códigos de acceso, o información de cualquier naturaleza que sirva para violar mecanismos de seguridad de computadoras o programas de cómputo; Amenazas, intimidación, hostigamiento acecho o causar temor personas físicas o morales, mediante mensajes electrónicos, el uso de computadoras u otros mecanismos tecnológicos similares, la Obtención sin consentimiento y/o mediante engaños datos o información personal de individuos para usarla con fines comerciales, obtención un lucro directo o indirecto de dicha información, o el uso o aprovechamiento para cometer cualquier actividad ilícita, mismos de los cuales no se encuentran regulados por las disposiciones legales mexicanas y las

que los señalan (Código Penal Federal) no abarca todas las posibles combinaciones de los mismos ni de las nuevas formas de comisión ni de resultado.

SÉPTIMA.- En la legislación actual mexicana, con excepción del Código Penal de Sinaloa, se señala la existencia de "delitos informáticos", sin embargo, el mismo se encuentra dentro del capítulo de delitos patrimoniales, siendo que en la comisión de éstas conductas no solo se afecta el patrimonio, sino en muchos de los casos la intimidad personal; por cuanto hace al Código Penal Federal a pesar de señalar varias de las conductas que pueden realizarse y considerarse como delitos informáticos, queda la principal laguna que deben de cometerse en contra de sistemas informáticos protegidos por algún mecanismo de seguridad, sin especificar el mismo.

OCTAVA.- Se propone usar el término de "sistemas informáticos" o el de ordenadores para señalar a cualquier equipo de cómputo o de tecnología que tenga las funciones de grabación, transporte, almacenamiento o reproducción de datos electrónicos, ello debido a que el primero de los términos abarca todos los sistemas relacionados con la computación y que pueden intercomunicarse entre sí, con la intención de que no existan lagunas en la legislación mexicana, abarcando así tanto los sistemas actuales como los que en el futuro puedan crearse.

NOVENA.- Se Propone una reforma estructural a la legislación mexicana, comenzando con ello con el Código Penal Federal, a fin de que éstas conductas que se señalan en la conclusión sexta se adecuen a la normatividad penal mexicana.

DÉCIMA.- La inclusión de éstos delitos en el Código Penal Federal en un apartado diseñado específicamente para ello como de "delitos informáticos" o bien, a través de la creación de una ley de carácter federal en razón de que la comisión de éstos delitos en muchas de las ocasiones de de carácter extra territorial.

DÉCIMA PRIMERA.- La difusión a las empresas, organismos, dependencias, particulares y a la sociedad en general, contribuirá notoriamente al nivel de concientización sobre el problema que nos ocupa. El siguiente paso será dar a conocer las medidas preventivas que se deben adoptar para evitar estas conductas ilícitas.

DÉCIMA SEGUNDA.- Qué con objeto de que se evite un conflicto de competencia entre los congresos locales y el de la Unión, éste, con base en las facultades que la Constitución Federal le confiere, establezca los criterios necesarios para delimitar, dada la naturaleza de los delitos informáticos, que pueden emplear para

su ejecución las vías generales de comunicación entre otros elementos, la jurisdicción federal y local de estos ilícitos.

DÉCIMA TERCERA.- Es necesaria la reforma al Código Penal Federal en el sentido de que contemplen las conductas que se señalan en las legislaciones internacionales como DELITOS INFORMÁTICOS, tales como Acceso indebido, Sabotaje o daño a sistemas, Sabotaje o daño culposos., Acceso indebido o sabotaje a sistemas protegidos, Posesión de equipos o prestación de servicios de sabotaje, Espionaje informático, Falsificación de documentos, Obtención indebida de bienes o servicios, Manejo fraudulento de tarjetas inteligentes o instrumentos análogos, Apropiación de tarjetas inteligentes o instrumentos análogos, Provisión indebida de bienes o servicios, Posesión de equipo para falsificaciones, entre otras.

BIBLIOGRAFÍA.

1.- ALTMARK, Daniel Ricardo; "La Etapa Precontractual en los Contratos nformáticos. Informática y Derecho, Aportes de Doctrina Internacional."; Ediciones Depalma, Buenos Aires, Vol. 1, 120 páginas.

2.- CABANELLAS, Guillermo. Introducción al estudio del Derecho Romano. Diccionario Enciclopédico de Derecho Usual Editorial Heliasta Tomo III 24 Edición, Buenos Aires Argentina. 402 páginas.

3.- CARRANCÁ Y TRUJILLO Raúl. Derecho Penal Mexicano. Parte general.. Editorial Porrúa, México, Distrito Federal 2001. 982 páginas

4.- CALLEGARI, Lidia. "Delitos informáticos y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985. 119 páginas.

5.- CORREA M. Carlos, Derecho informático, Ediciones De palma, Buenos Aires Argentina 1987, 341 páginas.

6.- DE PINA VARA, Rafael. Diccionario de Derecho, vigésimo sexta edición, México, editorial Porrúa, 1998. 525 páginas.

7.- DÍAZ DE LEÓN, Marco Antonio. Diccionario de Derecho Procesal Penal, tomo I, México, Distrito Federal 1993, editorial Porrúa. 1099 páginas.

8.- FERNÁNDEZ CALVO, Rafael. "El tratamiento de llamado "delito informático" en el proyecto de ley Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática" en Informática y Derecho. 1150 páginas.

9.- FONTAN BALESTRA, Carlos, Derecho penal, introducción y parte general, editorial Albeledo Perrot, Argentina Buenos Aires 1991. 750 páginas.

10.- GARCÍA PELAYO Y GROSS Ramón. Pequeño Larousse ilustrado, México, Distrito Federal 1995, ediciones Larousse. 1863 páginas.

11.- GARCÍA RAMÍREZ, Sergio. Panorama del Derecho Penal Mexicano. Editorial Mc Graw Hill, México, 1998. 191 páginas

12.- JIMÉNEZ DE ASÚA, Luis, Lecciones de Derecho penal, tomo III, editorial Oxford, México 2001. 367 páginas.

13.- LIMA DE LA LUZ, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. No. 1-6. Año L. Enero-Junio 1984. 100 páginas.

14.- LÓPEZ BETANCOURT, Eduardo. Teoría del delito. 12ª edición. Editorial Porrúa, México 2004. 313 páginas.

15.- MARCEL PLARIOL, Georges Ripert. Derecho Civil, Editorial Harla, México Distrito Federal 2001, Vol. 8 Pag: 1. 350 páginas.

16.- MEJAN, Luis Manuel C.; "Transferencia Electrónica de Fondos. Aspectos jurídicos"; Fomento Cultural Banamex, México 1990. 120 páginas.

17.- MONROY CABRERA, Marco G., Introducción al Derecho, 12ª edición, editorial Temis, Bogotá Colombia 2001. 554 páginas.

18.- MORINEAU IDUARTE, Marta y otro. Introducción al estudio del Derecho Romano. Derecho Romano. Tercera Edición Edit Harla, México 1993. 105 páginas.

19.- ORELLANO WIARCO, Octavio Alberto, Curso de Derecho Penal, parte general, segunda edición, editorial Porrúa, México 2001. 472 páginas.

20.- PAVÓN VASCONCELOS, Francisco. Diccionario de Derecho Penal, segunda edición. México, 1999, editorial Porrúa. 1127 páginas.

21.- PAVÓN VASCONCELOS, Francisco. Manual de Derecho penal Mexicano, séptima edición, México 1985. Editorial Porrúa. 558 páginas.

22.- PÉREZ, Carlos Luis. Tratado de Derecho penal tomo I. Editorial Tamis, Bogotá Colombia 1967, 650 páginas

23.- RÍOS ESTAVILLO, Juan José. Derecho e informática en México. Informática jurídica y Derecho de la informática. Editorial UNAM, México, 1997, 136 páginas.

24.- ROJAS AMANDI, Víctor Manuel, El uso de internet en el Derecho, segunda edición, editorial Oxford, México 2001, 248 páginas.

25.- SARZANA, Carlo. "Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Números 1-2 Año 1. Roma, Italia. 150 páginas.

26.- TÉLLEZ VALDEZ, Julio. Derecho informático, segunda edición, México 2001. Editorial Mc Graw-Hill. 283 páginas.

LEGISLACIONES CONSULTADAS

Constitución politica de los Estados Unidos Mexicanos.

Código Penal Federal.

Nuevo código penal para el Distrito Federal.

Código Penal para el Estado libre y soberano de Sinaloa.

Medios electrónicos:

http ://209.61.1 5 8.1 2 5/ecomder/confer/trabajos/ponen70.htm

http://publicaciones.derecho.org/redi/No._09_-_Abril_de_1999/viega

http://www.latinlex.com/cl/contenido/leg4.asp.

http://publicaciones.derecho.org/redi/No.05_Diciembre_de_1998/herrera.

http://www.ordenjuridico.com.mx