UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN

PROPUESTA JURÍDICA PARA ACLARAR EL CONTENIDO DEL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

P R E S E N T A:

IVONNE CABRERA HERRERÍAS

ASESOR: LIC. JUAN JESÚS JUÁREZ ROJAS

MÉXICO 2005

NUNCA CONSIDERES EL ESTUDIO COMO UN DEBER, SINO COMO UNA OPORTUNIDAD DE PENETRAR EN EL BELLO MUNDO DEL SABER.

Dedicatoria:

Con un pensamiento que dice: "LA ESENCIA DE LA GRANDEZA RADICA EN LA CAPACIDAD DE OPTAR POR LA PROPIA REALIZACIÓN PERSONAL Y SEGUIR SIEMPRE ADELANTE", dedico esta tesis a las personas más importantes de mi vida....

A DIOS

Por todo el amor y todas las bendiciones recibidas, por darme la oportunidad de existir y permitirme vivir la vida, por estar siempre conmigo y llenarme de fortaleza para seguir adelante ante las adversidades que se presenten. A ti dedico mi primer agradecimiento por concederme la dicha de haber conocido y estar hasta el último momento, con uno de mis dos grandes regalos, mi Padre, quien ahora ya no se encuentra físicamente pero cuyo recuerdo guardo en mi memoria con amor y respeto. Gracias por permitirme estar a lado de mi Madre, Hermanos, Sobrinos y toda mi Familia junto con mi amigos quiénes forman parte importante de mi vida.

A mis Padres

Un agradecimiento eterno por su amor, confianza y apoyo que siempre me han brindado.

A mi Padre Arturo Cabrera Díaz ✝; un claro ejemplo de fortaleza, humildad y lucha constante, quien dio siempre todo sin recibir nada a cambio, a ti dedico en especial este logro quien a pesar de no haber visto culminado tu anhelo, éste es en honor a ti. Hicimos realidad este momento y si estuvieras aquí se que compartirías esta felicidad como en esos grandes momentos en que estabas con nosotros. Gracias Papi por estar siempre a mi lado y por infundir en mi el fijarme metas y luchar por alcanzarlas, simplemente por enseñarme a ser feliz. Siempre te llevaré en mi mente y en mi corazón Te extraño y te Recuerdo con Amor.

A mi Madre Marina Herrerías Vázquez; quien me enseñó que ser mujer es mas que eso, es una esencia y una responsabilidad. A ti te dedico este logro por tu eterno amor, por las bellas cosas que me has obsequiado, por brindarme la libertad de elegir el rumbo de mi destino. Gracias por haberme dado el regalo mas preciado: la vida.

A mis Hermanos

Adrián, Verónica, Marina, Arturo y Leticia; quiero agradecerles por tenerlos a ustedes como hermanos, por brindarme todo su apoyo, por alentarme para alcanzar mis metas, por confiar en mi y por el sólo hecho de tenerlos a mi lado. Les dedico este logro esperando que este sea una motivación para fijarse metas en la vida sin importar cuantas veces lo tengan que intentar, desando que este triunfo profesional lo sientan como suyo también. Con amor, admiración y respeto gracias a todos ustedes.

A mis Sobrinos

Gracias por hacerme muy feliz desde el primer momento en que llegaron a mi vida:

Diego (hermanito), sencillez, ternura, y capacidad para hacer las cosas, elementos necesarios para luchar y seguir adelante.

Emmanuel, comparto tu dedicación y tu buen corazón.

Ilse, niña con gran ternura y anhelo, sigue adelante.

Leticia, lucha por tus sueños mi Vivi.

Lupita, esperando que tu carácter te lleve muy lejos.

Jessica, actitud, inteligencia y amor grandes cualidades....

Abimelec y Axel los mas pequeños pero grandes tesoros.

A todos y cada uno de ustedes gracias por ser como son e inspirarme a seguir adelante. Con todo amor y cariño les dedico este logro esperando que sirva de ejemplo para su superación personal, guiándolos al estudio constante durante toda su vida.

A mi Novio

Ing. Xavier Rosas; mi gran amor, mi mejor amigo: Un gran ser.

Agradezco a Dios por haberte conocido y formar parte importante de mi vida desde hace diez años; te doy gracias por tu presencia incondicional, por tu amor, por tus enseñanzas, por tu motivación para seguir adelante, por que en los momentos en que sentí caer me brindaste tu mano y las palabras precisas. Gracias por enseñarme que la vida no es tan trágica y que cada día vale la pena vivirlo, por compartir conmigo un logro mas en la vida y por haber creído en mi. Con respeto y gratitud te lo dedico fruto de tu esfuerzo y dedicación.

Juntos en la trayectoria, TE AMO.

A mi Familia

A mi Bisabuela Delfina†; ser excepcional con corazón enorme y una sencillez inigualable, mujer que dejó huella y que le estoy muy agradecida por esos años felices que vivimos con ella.

A mi Abuelita Graciela por su apoyo y cariño que me brinda.

A mis Tios y Primos como un testimonio de mi infinito aprecio y agradecimiento.

A todos mis Cuñados; gracias por su apoyo tan valioso en momentos circunstanciales, por su muestra de cariño al estar a mi lado formando parte de esta familia y seguir en la lucha constante de superarse, a ustedes les dedico con infinito cariño este logro.

A la Familia Rosas Velázquez

Este logro se lo dedico con mucho cariño, respeto y admiración a una gran familia muestra de amor, respeto y unión. Gracias por permitirme compartir con ustedes la grandeza de la vida. Gracias Profesora Rosa María, por ser como es, por su humildad, y sencillez que la caracteriza, por creer en mi, y por todo su apoyo y cariño que me brinda día con día. Gracias Ing. Agustín por sus palabras, por estar a mi lado aún en los momentos más difíciles y por alentarme en la lucha constante del aprendizaje.

A mis Compañeros y Amigos

Por que a través de mi época escolar desde la prepa cada uno de ustedes me brindan su amistad sincera que hasta hoy seguimos conservando. Por su apoyo y motivación se los dedico con mucho amor a Ricardo Mejía, Mónica Gómez, Miguel Angel Hernández, Benjamín Olvera y Cuauhteemoc.

A mis grandes amigas de la Universidad

Nohemí, mujer sencilla con simpatía y nobleza enorme, te agradezco el haber compartido un salón de clases, tus ocurrencias, tu apoyo, y simplemente por ser Mimi.

Fani, como no dedicar este logro a la mujer con agallas para salir adelante, a la que siempre se adelanta y con la que compartí mas que un café.

Paola, personalidad y fuerza pero con una dulzura increíble con quien compartí mas que un juego.

A ustedes les dedico y les doy las gracias por compartir muchos de mis logros, muchos momentos felices y cinco de los mejores años de mi vida, gracias por ser mis amigas y hacerme creer que existe la verdadera amistad.

A mis Profesores

Quienes depositaron en mi su tiempo, esfuerzo y dedicación plena en esta loable labor que es la enseñanza. Gracias por mostrarme el camino.

Y a todos aquellos que me ayudaron en algún momento de mi vida y que han estado a mi lado.

AGRADECIMIENTOS

Por ser parte importante e indispensable para la elaboración de este trabajo:

A la Magna Casa de Estudios la Universidad Nacional Autónoma de México, que me acogió en su seno de conocimiento y libertad.

Por Mi Raza Hablara el Espíritu.

A la Escuela Nacional de Estudios Profesionales Aragón, por haberme cobijado durante mi desarrollo académico, permitirme consumar mis estudios y formarme como profesionista.

Al Instituto de Investigaciones Jurídicas, que me dio la oportunidad de colaborar en sus proyectos de investigación y en especial al Dr. Enrique Cáceres y el Lic. Edgar quiénes con su apoyo y cooperación fue posible la realización de este trabajo.

A mi Asesor Lic. Juan Jesús Juárez Rojas un agradecimiento especial, quien gracias a su esfuerzo y ética profesional me brindó su ayuda para la realización del presente trabajo de investigacion. Gracias por su paciencia y orientación.

Al Honorable Jurado el cual es integrado por el Maestro Bernabé Luna Ramos, Lic. Juan Jesús Juárez Rojas, Lic. Marisela Villegas Pacheco, Lic. Regina Rojas García y el Lic. Rubén Martin Cortés Sánchez; por haber dado su visto bueno en esta tesis y darme la oportunidad de contar con su experiencia en este mundo del saber.

PROPUESTA JURÍDICA PARA ACLARAR EL CONTENIDO DEL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL

CONTENIDO

INTRODUCCIÓN..... I

CAPÍTULO I DERECHO INFORMÁTICO

1.1 DERECHO 1

1.1.1 CONCEPTO DE DERECHO..... 2
1.1.2 ELEMENTOS Y CARACTERÍSTICAS DEL DERECHO..... 3
1.1.3 LA NORMA JURÍDICA 6
1.1.4 DERECHO PENAL..... 7
1.1.5 OBJETO Y FIN DEL DERECHO..... 8

1.2 ASPECTOS FUNDAMENTALES DEL DERECHO INFORMÁTICO..... 9

1.2.1 LA INFORMACIÓN COMO UN BIEN JURÍDICO..... 9
1.2.2 DIFERENCIA ENTRE CIBERNÉTICA E INFORMÁTICA..... 11
1.2.3 CONCEPTO DE DERECHO INFORMÁTICO..... 13

1.3 INTERNET..... 15

1.3.1 HISTORIA.....15
1.3.2 CONCEPTO..... 18
1.3.3 EL IMPACTO SOCIAL DE INTERNET..... 19

CAPÍTULO II DELITO

2.1 EVOLUCIÓN HISTÓRICA DEL CONCEPTO DEL DELITO..... 23

2.2 CONCEPTO DE DELITO..... 25

2.3 ELEMENTOS CONSTITUTIVOS DEL DELITO..... 27

2.3.1 PRESUPUESTOS DEL DELITO..... 27
2.3.2 ELEMENTOS DEL DELITO..... 28
2.3.3 ELEMENTOS SEGÚN FERNANDO CASTELLANOS..... 28
2.3.4 ELEMENTOS SEGÚN FRANCISCO PAVÓN..... 30
2.3.5 ANÁLISIS DE LOS ELEMENTOS DEL DELITO..... 31

2.4 CLASIFICACIÓN DOCTRINAL DEL DELITO..... 36

2.4.1 EN FUNCIÓN DE SU GRAVEDAD..... 36
2.4.2 SEGÚN LA FORMA DE LA CONDUCTA DEL AGENTE..... 36
2.4.3 POR EL RESULTADO..... 37
2.4.4 POR LA LESIÓN QUE CAUSAN..... 37
2.4.5 POR SU DURACIÓN..... 37
2.4.6 POR EL ELEMENTO INTERNO O CULPABILIDAD..... 38
2.4.7 DELITOS SIMPLES Y COMPLEJOS..... 38
2.4.8 DELITOS UNISUBSISTENTES Y PLURISUBSISTENTES..... 38
2.4.9 DELITOS UNISUBJETIVOS Y PLURISUBJETIVOS..... 39
2.4.10 POR LA FORMA DE PERSECUCIÓN..... 39
2.4.11 DELITOS COMUNES, FEDERALES, OFICIALES, MILITARES Y POLÍTICOS.. 39

2.5 CLASIFICACIÓN LEGAL DEL DELITO..... 41

2.5.1 INTRODUCCION AL *ITER CRIMINIS*..... 41
2.5.2 LA ACCIÓN U OMISIÓN..... 42
2.5.3 INSTANTÁNEO..... 44
2.5.4 PERMANENTE O CONTINUO..... 44
2.5.5 CONTINUADO..... 45
2.5.6 DOLO..... 46
2.5.7 CULPA..... 48
2.5.8 TENTATIVA..... 49
2.5.9 SUJETOS..... 51

CAPÍTULO III DELITOS INFORMÁTICOS

3.1 INTRODUCCIÓN A LOS DELITOS INFORMÁTICOS..... 56

3.2 TERMINOLOGÍA DE LOS DELITOS INFORMÁTICOS..... 56

3.2.1 DELINCUENCIA INFORMÁTICA..... 56
3.2.2 CRIMINALIDAD INFORMÁTICA..... 57
3.2.3 COMPUTER CRIMEN..... 57
3.2.4 DELINCUENCIA DE CUELLO BLANCO..... 57
3.2.5 ABUSO INFORMÁTICO..... 57
3.2.6 DELITO ELECTRÓNICO..... 58
3.2.7 DELITOS INFORMÁTICOS..... 59

3.3 CONCEPTO DE DELITO INFORMÁTICO..... 60

3.4 ELEMENTOS QUE INTERVIENEN EN LOS DELITOS INFORMÁTICOS.....61

3.4.1 SUJETO ACTIVO..... 61
3.4.2 SUJETO PASIVO..... 63

3.5 CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS..... 64

3.6 CLASIFICACIÓN DE DELITOS INFORMÁTICOS.....67

3.6.1 CLASIFICACIÓN SEGÚN ACTIVIDADES DELICTIVAS GRAVES..... 67
3.6.2 CLASIFICACIÓN SEGÚN LA ACTIVIDAD INFORMÁTICA..... 68
3.6.3 CLASIFICACIÓN SEGÚN EL INSTRUMENTO, MEDIO O FIN U OBJETIVO... 71

3.7 SITUACIÓN INTERNACIONAL Y ORGANIZACIONES..... 74

3.7.1 LEGISLACIÓN EN OTROS PAÍSES..... 74
3.7.2 ORGANIZACIONES EN MATERIA DE PREVENCIÓN DE DELITOS INFORMÁTICOS..... 84

CAPÍTULO IV PROPUESTA JURÍDICA PARA ACLARAR EL CONTENIDO DEL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL

4.1 CÓDIGOS PENALES DE LAS ENTIDADES FEDERATIVAS QUE SANCIONAN DICHAS CONDUCTAS ILÍCITAS..... 92

4.1.1 CÓDIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA..... 92
4.1.2 ESTADO DE MORELOS..... 94
4.1.3 ESTADO DE TABASCO..... 95
4.1.4 ESTADO DE NUEVO LEÓN..... 95

4.2 DELITOS QUE ESTABLECE EL CÓDIGO PENAL FEDERAL EN MATERIA DE DELITOS INFORMÁTICOS..... 97

4.2.1 ATAQUES A LAS VÍAS DE COMUNICACIÓN..... 97
4.2.2 VIOLACIÓN DE CORRESPONDENCIA..... 100
4.2.3 PORNOGRAFÍA INFANTIL..... 101
4.2.4 DELITOS EN MATERIA DE DERECHOS DE AUTOR..... 106
4.2.5 REVELACIÓN DE SECRETOS..... 110
4.2.6 ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA..... 111

4.3 ANÁLISIS EN MATERIA DE DELITOS INFORMÁTICOS DEL TÍTULO NOVENO CAPÍTULO II DEL CÓDIGO PENAL FEDERAL..... 114

4.3.1 LA REFORMA DEL 17 DE MAYO DE 1999 DEL CÓDIGO PENAL FEDERAL..... 114
4.3.2 ANÁLISIS JURÍDICO SOBRE EL ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA..... 115

4.4 PROPUESTA DE REFORMA AL CAPÍTULO II DEL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL SOBRE DELITOS INFORMÁTICOS.....122

4.4.1 PROPUESTA PARA MODIFICAR EL TEXTO DEL CAPÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL SOBRE DELITOS INFORMÁTICOS..... 124

CONCLUSIONES.....127

GLOSARIO DE TÉRMINOS..... 130

BIBLIOGRAFÍA 141

INTRODUCCIÓN

En la actualidad el uso de la tecnología es cada vez más frecuente, y se ha visto ampliada de manera vertiginosa a la par de los avances científicos, dando apertura a la llamada era de la información. La aparición de una nueva era informática a traído consigo el surgimiento paralelo de conductas ilícitas con la creación de los sistemas informáticos.

Uno de los problemas evidentes de nuestro país, es el hecho de que tanto estas conductas como las tecnologías en materia de informática y comunicación, rebasan en su avance a la regulación jurídica; el atraso legislativo y lento enfoque resolutivo a esta problemática se convierten en actividades potentes de la delincuencia informática.

Con el derecho de libre circulación, se encuentra la dificultad de decidir cuando se debe proteger penalmente ciertas conductas. La delincuencia informática en México es una realidad palpable, el aumento del nivel de los delitos representa una amenaza para la economía de un país y también para la sociedad en su conjunto; desde ésta perspectiva se considera que dicha delincuencia se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora.

El presente trabajo pretende hacer un análisis de la situación que guarda el Derecho Penal Mexicano frente a estas nuevas conductas (Delitos Informáticos), para ello resultó necesario, recurrir al método deductivo el cual va de lo general a lo particular; es por eso que comenzaremos nuestro trabajo dando una definición sobre lo que es el Derecho en una perspectiva general, que sirva como punto de partida para el estudio de los aspectos fundamentales del Derecho Informático, así como definir Internet, conocer su historia y su impacto social.

Seguidamente en el capítulo II, realizaremos un estudio de lo que es el delito, para esto es necesario hacer referencia tanto a su concepto, como a los elementos que lo integran y a su clasificación tanto doctrinal, como la que establece el Código Penal Federal. Lo anterior en razón de una mejor comprensión y que nos sirva como antecedente para el desarrollo del presente trabajo para llegar a establecer las características que revisten los llamados Delitos Informáticos.

Posteriormente, en el capítulo III referente a los Delitos Informáticos, tendremos a la vista un análisis de estos delitos comenzando con su terminología atendiendo a realidades concretas en virtud de la problemática para poder definirlos, establecer su concepto, sus elementos, características y clasificación, así como las diversas posturas que se han adoptado a nivel internacional en cuanto a su naturaleza jurídica y las diversas organizaciones internacionales que trabajan en su problemática, a fin de entender plenamente a la figura jurídica de estos delitos.

Para finalizar el presente trabajo, en el último capítulo, hacemos una propuesta que nos lleva al análisis de las legislaciones tanto local como federal en donde ésta última tiene un estudio que trata de adecuar la realidad tecnológica a nuestro país lo que nos lleva de una manera específica al análisis del capítulo II en su artículo 211 bis y sus numerales respectivos los cuáles son idóneos, o bien dan pauta a la propuesta jurídica de adicionar un numeral más al artículo 211 con los términos a los que hace referencia el mismo.

Hay que destacar que, para el desarrollo de la presente investigación se hizo un planteamiento del problema, el cual se formula de la siguiente manera: ¿Cuál sería la propuesta jurídica que permita como alternativa disminuir la vaguedad que el Titulo Noveno del Código Penal Federal contempla en su normatividad?. La hipótesis a este planteamiento se contempla a que si se incluye un numeral mas al artículo 211 bis con definiciones y términos, esto ayudaría en lo posible evitar que con el avance tecnológico queden obsoletos en un corto tiempo. Por lo tanto, si quedara establecida la propuesta sería mas óptimo para impartir la justicia pues con esto se lograría brindar una mejor protección a los bienes jurídicos y una adecuada interpretación de la Ley.

CAPÍTULO I

DERECHO INFORMÁTICO

1.1 DERECHO

Es indudable que antes de hablar de una rama jurídica tan reciente como lo es la del Derecho Informático, se tenga que enunciar su concepto y sus elementos primordiales respecto al derecho en general, y al derecho penal. La idea de derecho es la unidad de todos los valores jurídicos y tiene una finalidad personalista en cuanto busca la dignidad de la persona y el respeto a sus derechos.

El Derecho regula la vida del hombre desde su nacimiento o aun antes de este y se extiende hasta después de su muerte. La actuación de la norma se hace de manera espontánea cuando las personas la cumplen, y en forma forzosa cuando la violan, en cuyo caso se ha ideado el proceso como instrumento por el cual el Estado a través del órgano jurisdiccional, resuelve los conflictos de intereses entre los individuos.

En relación a lo anterior es menester mencionar a Jacinto Pallares, quien afirmaba que "el derecho es la fuerza que coordina todas las actividades sociales del hombre; y que el derecho es la síntesis de todas las incontables energías de la sociedad, porque todas ellas se destruirían mutuamente y matarían el organismo social si el derecho, como fuerza soberana, no interviniera armonizando y conciliando, en una suprema síntesis de equilibrio, todas esas corrientes impetuosas de la vida humana, material, económica, intelectual, artística, moral y religiosa; es por eso, que si el derecho desapareciera, la humanidad solo duraría el tiempo necesario para su propia destrucción".[1]

Con este pensamiento pone de relieve la enorme importancia del derecho como un sistema para evitar la anarquía, imponer el orden en la sociedad, solucionar los conflictos entre los sujetos, permitirles la convivencia y coexistencia pacíficas, el libre ejercicio de sus derechos y, en términos generales, armonizar todas las actividades de la colectividad. El derecho forma parte de la cultura, es un deber ser, implica valores como la justicia, la seguridad, la paz, el bien común, y en general, el orden de la vida humana. Ahora bien, para una ordenación adecuada de estos actos, es preciso que exista un sistema normativo que indique las obligaciones y los derechos de las personas, lo cual constituye en su forma más sencilla el derecho.

---

[1] PALLARES, Jacinto, citado por RAMÍREZ SÁNCHEZ, Jacobo, *Introducción al Estudio del Derecho Civil*, Ed. Textos Universitarios UNAM, segunda ed. México, 1997 p.19.

El sentido intencional del Derecho consiste en que objetivamente se produzca el comportamiento que establece como necesario para la vida social, como necesario para la estructura de la colectividad y para el funcionamiento de la misma, con independencia del modo de pensar y del sentir del sujeto obligado.

1.1.1 CONCEPTO DE DERECHO

Atendiendo a la etimología de la palabra, el vocablo "derecho" toma su origen de la voz latina *directus*, que significa recto, directo, participio del verbo *dirigiere*: dirigir.

La palabra "derecho" ha sido utilizada empleando para ella diversas acepciones, a saber:

Como conjunto de reglas o preceptos de conducta de observancia obligatoria que el Estado impone a sus súbditos.

Como la disciplina científica que tiene por objeto el conocimiento y la aplicación de esas reglas de conducta.

Como el conjunto de facultades que tiene un individuo y que le permiten hacer algo frente a los demás y frente al Estado mismo.

Con base a estos elementos, son muchos los conceptos que se han vertido sobre el Derecho. De ellos ha parecido pertinente resaltar el formulado por el maestro Villoro Torazo, por considerar que este engloba en forma general los rasgos más importantes de dicha disciplina. En este sentido, tenemos que el Derecho es el "Sistema racional de normas sociales de conducta, declaradas obligatorias por la autoridad, por considerarlas soluciones justas a los problemas surgidos de la realidad histórica".[2]

Una vez que se ha señalado lo anterior, pasaremos a estudiar a los elementos del derecho y sus características, lo cual nos va a permitir a lo largo de este trabajo un análisis con fundamento a los conceptos básicos que permita darle un mejor entendimiento y de esta forma poder comprender el objetivo del presente trabajo.

---

[2] VILLORO TORAZO, Miguel, *Introducción al Estudio del Derecho*, Ed. Porrúa, México, 1975 p.127.

1.1.2 ELEMENTOS Y CARACTERÍSTICAS DEL DERECHO

La mayor parte de los elementos esenciales del Derecho son reconocidos por la casi totalidad de las nociones del Derecho, motivo por el cual es importante resaltarlos.

1) El Derecho. Un fenómeno exclusivamente humano

Todos los autores están de acuerdo. Aristóteles, Cicerón, los juristas romanos, y la mayor parte de los tratadistas modernos que explícitamente relacionan el Derecho con la libertad y la razón del hombre. El Marxismo también reconoce esta nota esencial del Derecho cuando hace del Derecho una *ideología*, ya que las ideologías sólo se pueden dar entre los hombres. Recaséns Siches, para quien el Derecho es "Vida humana objetivada", pone el acento en el carácter humano del Derecho.

2) El Derecho. Un ordenamiento de la razón

Kant lo hace del punto de partida de su noción, puesto que estudia el Derecho en cuanto el *Pensar Jurídico*, diferente de otros modos de pensar. Kelsen lo exagera hasta hacer del orden normativo percibido por la razón el único objeto de la ciencia jurídica.

3) El Derecho. Presupone la libertad humana

El Marxismo-Leninismo es el que más limita esta afirmación sin llegar a desconocerla. Para él, la verdadera libertad sólo será posible en la sociedad comunista y la grandeza de las grandes personalidades reside "En la capacidad del individuo para salirse con la suya y realizar su voluntad superando toda clase de obstáculos". Vyshinsky, Golunskii y Strogovich defienden abiertamente que el Derecho es un sistema de normas y un orden coactivo, lo cual no puede darse sin la presuposición de la libertad humana.

4) El Derecho. Una forma de vida social

Sería inútil insistir sobre esta nota ya que es evidente y admitida por todo, y especialmente puesta en evidencia por la Escuela Histórica del Derecho.

5) El Derecho. Tiene como fin la Justicia

Este es un elemento esencial del Derecho y es el mas discutido de todos.

6) El Derecho. Es diferente de la moral

Primero, la Escuela Racionalista del Derecho Natural, luego, Kant y Kelsen se esforzaron en descartar las diferencias, hasta el punto que el último hace al Derecho irreducible a la Moral.

El que sean diferentes no implica que se deban excluir o que no puedan darse relaciones entre uno y otra, sino sencillamente significa que el sentido de la palabra "derecho" no es el mismo de la palabra moral, y esto por que cada palabra tiene un contenido de la otra palabra.

7) El Derecho. Debe ser promulgado por un legislador

El Positivismo insistió sobre este carácter del Derecho. Santo Tomás defendió que la promulgación es de la esencia de la ley.

8) El Derecho. Esta condicionado por la realidad

Las diversas escuelas del Empirismo Jurídico han destacado el papel de la realidad en la formación del Derecho: la Escuela Histórica, el de la realidad histórica en general; el Sociologismo Jurídico, el de la realidad de los vínculos colectivos de una sociedad; el Marxismo, el de los factores económicos, y el Positivismo, el de las decisiones políticas.

9) El Derecho. Debe realizarse en la historia

El Derecho no debe quedar como una especulación teórica, utópica, sino que debe realizarse en la realidad histórica. Hay que dar a cada uno lo suyo dentro de sus límites espaciales y temporales.[3]

Ahora bien para dar inicio a las características, sería prolijo enunciar autores y conceptos específicos que encierran o mencionan las tres características comunes y principales del derecho, sin embargo nos apoyaremos en Recaséns Siches en cuanto concibe al derecho como valor, norma y hecho; eso que se llama derecho, es un objeto que esencialmente tiene tres dimensiones recíprocamente unidas, de un modo íntimo e inseparable y estas son:

1. Dimensión de Hecho. Comprende conductas humanas reales, hechos humanos y sociales, en los que el derecho vive, se gesta y se produce.

[3] Cfr. VILLORO TORAZO, Miguel, *Introducción al Estudio del Derecho*, Ed. Porrúa, México, 1975 pp.112-116.

2. Dimensión de Norma. Es un juicio lógico, en ocasiones breve, conciso, referido a una conducta, a un deber o a una facultad, que trae consigo consecuencias derivadas de su cumplimiento.

El derecho no se presenta en normas aisladas, a veces se inicia configurando una norma o aplicando una norma en particular, pero esa norma no esta aislada, pertenece a un orden, a un sistema que ha sido creado intencionalmente y que es por lo general eficaz. Norma, orden y sistema basan su existencia en el ánimo del ciudadano, en su eficacia, no en la pulcritud de un juicio o en la perfección de sus contenidos lógicos.

3. Dimensión de Valor. Consistente en que sus normas, mediante las cuales se trata de satisfacer una serie de necesidades humanas, esto intenta hacerlo de acuerdo con las exigencias de unos valores, de la justicia y de lo demás valores que ésta implica, entre los que figuran la autonomía de la persona, la seguridad, el bien común y otros.[4]

En base a estas tres características el Derecho puede y debe ser estudiado desde tres puntos de vista:

-Como un conjunto de hechos sociales generadores de las normas y de otros hechos sociales en los que las normas son realizadas, lo cual suscita una consideración sociológica.

-En su dimensión de una normatividad específica. en cuanto a los caracteres especiales de ésta.

-Como valor, es decir, desde el punto de vista de la estimativa.[5]

Como conclusión se puede decir que toda definición del Derecho debe ser tal que: 1) incluya todas las notas esenciales de lo jurídico, sin que el afirmar una implique la exclusión de otra; 2) ofrezca a todos los sentidos de la palabra "derecho" unas notas comunes, aplicables a todos los sentidos aunque no en la misma forma; y 3) distinga la importancia de cada una de las notas esenciales, de tal suerte que las más importantes deben encontrarse en todos los sentidos de la palabra "derecho" y las menos importantes sean las que soporten todo el peso de las diferencias entre estos sentidos.[6]

---

[4] Cfr. RECASÉNS SICHES, Luis, citado por CISNEROS FARÍAS, German. *Teoría del Derecho*, Ed. Trillas, segunda ed. México, 2000 pp. 14-15.

[5] Cfr. RECASÉNS SICHES, Luis. *Introducción al Estudio del Derecho*. Ed. Porrúa, tercera ed. México, 1968 pp. 45- 46.

[6] Cfr. Ob. Cit., VILLORO TORAZO, Miguel, p.111.

1.1.3 LA NORMA JURÍDICA

En el orden social hay tres clases de normas que tienen semejante envoltura en cuanto al juicio lógico que las protege, y semejante contenido en cuanto al valor protegido: las normas jurídicas, las normas morales y las reglas del trato social. A continuación haremos una valoración de las primeras por ser materia de nuestro estudio.

Consecuentemente el valor o la finalidad de cada grupo social será protegido mediante normas. Estos se van transmitiendo de generación en generación hasta formar patrones culturales que se encuentran inscritos en valores o finalidades que requieren a su vez de normas mejor confeccionadas, es decir lo que es nuestro Derecho Consuetudinario; así tendremos que los artículos de una ley, instituciones jurídicas, definiciones, conceptos jurídicos, decretos, y códigos, se presentan mediante signos gramaticales, formando un juicio lógico llamado norma jurídica.

De lo anterior se desprende que la norma jurídica tiene ciertas características particulares:

La norma jurídica es bilateral. Impone obligaciones a alguien, concede facultades a alguien.

La norma jurídica es coactiva. Las obligaciones impuestas por la norma pueden ser cumplidas de manera espontánea, en su defecto, se cumplen aún en contra de la voluntad del obligado.

La norma jurídica es heterónoma formal. Las obligaciones y facultades provienen de una voluntad ajena al individuo. Las crea el poder público siguiendo ciertas formalidades exigibles por una ley específica por la creación de normas jurídicas.

La norma jurídica es de concordancia externa. El cumplimiento de una obligación o la exigencia de una facultad se circunscribe a la conducta, hechos, omisiones establecidas, sin tomar en cuenta los motivos interiores de su cumplimiento. El obligado o facultado puede hacerlo de buena o mala gana, lo que importa es la concordancia entre lo que la norma prescribe y la conducta exige.

La norma jurídica tiene sanción, *strictu sens.* En caso de incumplimiento se da una consecuencia jurídica que puede ser la declaración de inexistencia, la nulidad, el castigo, la indemnización u otras sanciones.

La norma jurídica es correlativa. En las normas jurídicas se da una curiosa relación de juicios conexos, que van desde la exigencia por el facultado del cumplimiento de un deber y cumplido éste, ahora el facultado se convierte en obligado frente quien ahora está facultado para exigirle una contraprestación.

La norma jurídica es codificable. El derecho, como ley o norma jurídica, requiere para su validez de una formalidad externa, expresa, pública y de iniciación determinada en cuanto al tiempo, para considerarse obligatoria frente a los ciudadanos u obligados en general.[7]

Por tanto, la existencia de una norma es lo que da soporte jurídico a todos aquellos hechos que nos ponen en contacto con el Derecho. Las normas jurídicas son tales no porque gocen de ninguna cualidad intrínseca y especial que les dé ese carácter, sino simplemente porque son respaldadas en su cumplimiento por el poder coercitivo del Estado. Una parte importante de las normas jurídicas son en sustancia, órdenes o prohibiciones de hacer algo respaldadas por la amenaza de una sanción al que las infrinja.[8]

La diferencia esencial de la norma jurídica es sin lugar a dudas el poder coactivo ya que esta característica la hace diferente de cualquier norma del orden social, pues es la única que cuenta con la fuerza del Estado para asegurar el cumplimiento del deber o de la obligación impuesta por una norma.

1.1.4 DERECHO PENAL

Todos los intereses que el Derecho intenta proteger son de importancia incalculable; sin embargo, de entre ellos hay algunos cuya tutela debe ser asegurada a toda costa, originándose así la necesidad y justificación del Derecho Penal, que por su naturaleza esencialmente punitiva, es capaz de crear y conservar el orden social; por otro lado el Estado puede aplicar a los actos ilícitos dos clases de sanciones: civiles y penales. Las primeras, las aplica en el caso de que el acto ilícito lesione de una manera indirecta a la sociedad y directamente a un particular, estudiaremos las segundas por ser aquellas que lesionan en forma mediata a un particular e indirectamente a la sociedad; motivo por el cual es imprescindible definir al Derecho Penal como *un conjunto de leyes que determinan los delitos y las penas que el poder impone al delincuente.*

---

[7] Cfr. CISNEROS FARÍAS, German. *Teoría del derecho*, Ed. Trillas, segunda ed. México, 2000 pp. 20-33.

[8] Cfr. LA TORRE, Ángel, *Introducción al Derecho*, Ed. Ariel, Barcelona, 1999 PP. 13-16.

Por último hay que resaltar de una manera muy breve a los elementos del Derecho Penal citados por Efraín Moto Salazar y estos son:

Delito.-Se produce dentro de la sociedad y se presenta como un hecho dañoso, puesto que destruye la convivencia pacífica de los individuos.

Delincuente.-Lo consideran como un hombre peligroso para el vivir social; que sea peligroso por el ejercicio de su libre albedrío, o de su locura o su incapacidad para vivir, etc.

Pena.-Es un mal necesario, se justifica por distintos conceptos parciales. Por la intimidación, la ejemplaridad, la expiación en aras del bien colectivo, la necesidad de conservación del orden social.[9]

1.1.5 OBJETO Y FIN DEL DERECHO

El objeto del derecho es regular la conducta de los asociados por medio de normas jurídicas. Pero hay que tener en cuenta que el derecho no es solo el positivo vigente, sino que también está constituido por los principios que integran los derechos civiles, políticos, económicos, sociales y culturales de la persona, así como también por su contenido valorativo y por su ideal de justicia. Es decir, importa tanto el estudio del concepto del derecho como el de sus aplicaciones en la realidad social.

Al término *derecho* han ido unidas algunas connotaciones respecto a sus fines y al hablar de estos se citan la seguridad y la justicia como los fines primordiales del Derecho; en este sentido diremos que los valores de dignidad, honor, libertad, seguridad, orden social, bien común, paz, justicia, ocupan rangos de confección lógica y jurídica de mayor fuerza. Estos valores se encuentran encerrados en el concepto de justicia y forman parte de las grandes finalidades del derecho.

[9] Cfr. MOTO SALAZAR, Efrain, *Elementos de Derecho*, Ed. Porrúa, México, 2002 pp. 307-308.

1.2 ASPECTOS FUNDAMENTALES DEL DERECHO INFORMÁTICO

Una vez revisados los elementos básicos del Derecho de una forma general, ahora se presentaran los rasgos más significativos del llamado Derecho Informático. Es importante mencionar que en la reiterada interrelación Derecho-Informática, en lo términos de un Derecho Informático se contemplan una serie de implicaciones tanto de orden social, técnico, práctico y evidentemente jurídico suscitadas por el uso de la Informática.

1.2.1 LA INFORMACIÓN COMO UN BIEN JURÍDICO

Como lo expresa el artículo 19 de la Declaración Universal de los Derechos del Hombre de 1948; la palabra información (del latín in-formare, poner en forma) es una noción abstracta, no obstante que posee una connotación vinculada a una de nuestras mas grandes libertades, la de opinión y expresión de informaciones e ideas por cualquier medio que sea.

La palabra información, por su misma generalidad, se ha visto asociada fundamentalmente al fenómeno de la comunicación y que dentro de ésta se considera a la información como cierto número de mensajes, afirmaciones verdaderas o falsas, dirigidas a un individuo, quien las recibe, modifica, acepta o rechaza.

Ahora bien, además de la información general que responda a las necesidades de un amplio público, también tenemos aquélla mucho más especializada y sectorizada que satisface necesidades documentarias, y cuyo manejo es objeto de incursión ya no tanto de los medios de comunicación sino de los medios informáticos.[10]

Por tal, la Información Jurídica es aquella que emana de uno o varios órganos del Estado bajo un procedimiento determinado también en la ley, que dará contenido a las relaciones sociales bajo los principios y valores del derecho como son el bien común, la seguridad jurídica, principios generales del derecho, entre otros. La determinación de la información jurídica esta basada en diversos aspectos:

La información jurídica está determinada con base en un nivel protector, restrictivo y coactivo del individuo en la sociedad, ésta, al igual que las otras informaciones de diversas materias, conforman un conjunto de medios para ejercer el poder.

---

[10] Cfr. TÉLLEZ VALDEZ, Julio, *Derecho Informático*, Ed. Mc Graw Hill, segunda ed. México, 1996 p. 63.

El valor de la información jurídica se basa no solamente en un conjunto de disposiciones que norman la vida del hombre en sociedad como poder político, sino que también involucran aspectos individuales.

Por lo tanto la información jurídica es, por su propia naturaleza, necesaria para gobernantes y gobernados; lo cual implica la necesidad de una adecuada estructuración, organización y sistematización para su conocimiento.[11]

Al respecto se puede afirmar que la información jurídica es un bien jurídico de carácter patrimonial en razón de que pueda ser utilizada por el titular de la misma en su divulgación o explotación, e incluso sin necesidad de que exista tal autorización la información puede ser utilizada, divulgada o explotada por él mismo, el titular, ya sea con un carácter eminentemente económico o moral, cuestión que se adecua al concepto de patrimonio que entendemos como "...el conjunto de bienes, derechos y obligaciones de una persona, pecuniarios o morales, que forman una universidad de derecho...".[12]

Cabe anotar que la información contenida y transmitida a través del ciberespacio no es susceptible de ser únicamente un derecho protegido por La Ley Federal del Derecho de Autor, toda vez que puede tratarse de información que no sea una creación original tutelada por el artículo 13 del cuerpo de leyes ya mencionado, pudiendo ser una información o contenido de carácter privado, económico o social, que atañe de manera particular al individuo que la posé o a varios individuos a los que aprovecha, llámese persona física o moral, características que en un concepto colectivo poseen en su conjunto de manera individual los integrantes en la sociedad, por lo tanto, es ésta quien tiene interés preponderante de que la información como bien jurídico sea tutelada por el Derecho Penal; nada mas acorde con el siguiente criterio:

"La tutela del Derecho Penal está creada por una exigencia del Estado, para mantener el orden jurídico y las funciones inherentes a sus órganos, cualquiera que sea su jerarquía de quiénes lo ejercen, cuya autoridad viene en mengua y desprestigio cuando otras personas, que carecen de facultad decisoria y poder coactivo, ejercen funciones de tal, entrañando ello lesión a la fe pública, que es un bien jurídico colectivo que debe ser protegido mediante la tutela penal contra aquellos hechos que lesionan la confianza individual y que son susceptibles de engañar aún a los órganos del Estado ".

---

[11] Cfr. FIX FIERRO, Héctor, *Informática y Documentación Jurídica* UNAM, Facultad de Derecho, México, 1990. pp. 26-27.

[12] GUTIERREZ Y GONZÁLEZ, Ernesto. *Derecho Sucesorio, Inter-vivos y mortis causa,* Ed. Porrúa, tercera ed. México, 1998 p. 55.

De esta forma la valoración del merecimiento de protección o importancia social del bien jurídico a tutelar debe tenerse en claro que se refiere a una afectación de la generalidad de los componentes del grupo social y no solo a la minoría de un sector social determinado, por lo que su valoración debe ser desde un punto de vista colectivo; así para determinar si la información tiene un inminente carácter colectivo, se debe de abordar el tema en función a su trascendencia para los individuos, es decir, no resulta suficiente para la comprobación del merecimiento de protección que el interés social, en la información o contenido, trascienda a la generalidad, es preciso que su lesión o puesta en peligro posean una importancia trascendental capaz de provocar un daño en los individuos integrantes del grupo social.

1.2.2 DIFERENCIA ENTRE CIBERNÉTICA E INFORMÁTICA

El concepto de cibernética ha sido utilizado en diversas disciplinas que parte desde un estudio de carácter propiamente derivado de la ciencia política, hasta estudios con enfoques matemáticos; y ante esta situación nos parece pertinente resaltar en forma breve los orígenes de cómo surgió el término Cibernética.

El término cibernética fue utilizado por primera vez en 1848 por el Francés Ampere en una clasificación de las ciencias políticas, ya que el había creado un sistema para coordinar todo el conocimiento humano y había introducido el término cibernética para indicar el arte del Gobierno entendido en sentido político.

En 1948, un notable personaje matemático originario de Estados Unidos Norbert Wiener, escribió un libro que intituló Cibernética, empleando este término para designar a la nueva ciencia de la comunicación y control entre el hombre y la máquina; es decir, los estudios de Wiener fueron dirigidos en forma matemática al estudio del comportamiento humano visto y representado en una máquina, esto es, por un lado, la identidad de los mecanismos de control y regulación tanto en los hombres como en las máquinas, y por el otro la conexión entre estos mecanismos y la transmisión de informaciones.[13]

Su aparición obedeció a tres factores, a saber:

Un factor social, por que eran tiempos que requerían un aumento de producción y, por consiguiente, en el capital.

[13] Cfr. LOSANO, Mario G, *Curso de Informática Jurídica*, México, 1965. pp. 14-21.

El factor Técnico-Científico, fue muy importante por que varias líneas de pensamiento, originadas en muy diversas esferas de actividad, como lo que fue la ciencia y la técnica, se empezaron a reunir, y lograron los avances tales que hicieron menester una ciencia que facilitara su interrelación y desenvolvimiento.

El factor Histórico, por que surge de la mencionada necesidad del nacimiento de una ciencia de unión que controlara y vinculara a todas las demás. Surge entonces la cibernética como una unidad multidisciplinaria. Para Wiener esto es lo que constituye el propósito de la cibernética: abarcar de manera total y multidisciplinaria a todas las ciencias.[14]

Si atendemos a la etimología de la palabra, el vocablo "cibernética" toma su origen de la voz griega *kybernes*, concepto referido al arte de gobernar. Esta palabra alude a la función del cerebro con respecto a las máquinas.[15]

Otros autores han redefinido la cibernética como es el caso de Jagjit A. Sing, quien señala que la cibernética es la inquisición interdisciplinaria hacia la naturaleza y base física de la inteligencia humana, con el propósito de reproducirla en forma sintética, mientras que para Neville Moray, la cibernética, es la ciencia que relaciona las entradas y las salidas de un sistema, sus inputs y outputs.[16]
De estas definiciones quedan implícitas dos conceptos fundamentales que es el de comunicación y sistema, por lo tanto se puede conceptuar a la cibernética como "La ciencia de comunicación y control".[17] Los aspectos aplicados de esta ciencia están relacionados con cualquier campo de estudio. Sus aspectos formales estudian una teoría general del control, extractada de los campos de aplicación y adecuada para todos ellos.

Después de hacer referencia a lo que es la cibernética, es necesario comprender el término Informática.

La palabra informática es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en el año de 1962. En sentido general, la Informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones.

---

[14] Cfr. BEER, Stafford. *Cibernética y Administración*, Ed. Nacional, México, 1965 p. 27.

[15] Cfr. COROMINAS, Joan. *Breve diccionario Etimológico de la lengua castellana*, Madrid, 1983.

[16] Cfr. LIVAS, Javier. *Cibernética, Estado y Derecho*, Ed. Gernika, México, 1988 pp 55-86.

[17] TÉLLEZ VALDEZ, Julio. Ob. Cit. p. 4.

Mora y Molino, la definen como el estudio que delimita las relaciones entre los medios, los datos y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado. [18]

Ahora bien, es indispensable destacar la diferencia entre la Cibernética e Informática; aunque ambas tratan la información en forma matemática, lógica y analítica, existen diversas diferencias que a continuación veremos en el siguiente cuadro:

CIBERNÉTICA	INFORMÁTICA
En sus aspectos más generales, trata del empleo de métodos científicos para explicar fenómenos en la naturaleza o en la sociedad y la forma de representación del comportamiento humano de forma matemática en una máquina.	Parte del estudio de las computadoras, de sus principios y de su utilización. Comprende materiales tales como programación; estructura de la información; ingeniería del software; lenguajes de programación; hardware; arquitectura de las computadoras, entre otras.
Entre otros aspectos, trata de la creación de instrumentos informáticos que simulen actividades del hombre; por ejemplo, robots; desarrollo de la inteligencia artificial; utilización de métodos neurísticos, entre otros.	Es un instrumento de apoyo para el desarrollo de la propia cibernética.
Implica en esencia un sistema en el cual puede o no existir entre las partes (isomorfismo).	Esta, por su parte, implica también un sistema en el que siempre habrá relación entre las partes que lo integran. [19]

1.2.3 CONCEPTO DE DERECHO INFORMÁTICO

El Derecho Informático, como una nueva rama del conocimiento jurídico, es una disciplina en continuo desarrollo, teniendo en su haber (al menos hasta esta fecha) incipientes antecedentes a nivel histórico; sin embargo, podemos decir que las alusiones más específicas sobre esta interrelación, (la cual fue mencionada en el punto anterior), la tenemos a partir del año de 1948 con la obra de Norbert Wiener; en donde nos expresa la influencia de la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico.

---

[18] Cfr. MORA, José Luis y MOLINO, Enzo. *Introducción a la Informática*, México, 1974, p.12.

[19] Cfr. RIOS ESTAVILLO, Juan José. *Derecho e Informática en México*. UNAM, México, 1984 pp. 38- 39.

Como ha señalado Vittorio Frosini, el binomio informática y derecho indica con claridad la interacción entre dos ciencias, de la cual surge un campo fecundo del saber; por una parte, la computadora se considera un instrumento utilizado por el jurista para crear bancos de datos jurídicos y para facilitar la administración de la justicia, y por otra, recurrir a la computadora plantea una serie de problemas que deben ser regulados por la ley. [20]

Lo primero que diremos al respecto es que, por la propia integración terminológica, estamos en presencia de información informatizada, por lo que, al conjugarla con el derecho, lo primero que tenemos que determinar es precisamente algo jurídico, normativo y regulador de los efectos en el uso (activo o pasivo), de una computadora.

Sin definir conceptos, otros han señalado que la informática como objeto de regulación jurídica ha dado origen al llamado Derecho de la Informática.

El Derecho Informático, ha sido considerado por Carracosa López como el "conjunto de normas que regulan las acciones procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones". [21]

Para Emilio Suñé "es el conjunto de normas reguladoras del objeto informática o de problemas directamente relacionados con la misma". [22]

Por otro lado Julio Téllez afirma que es "El conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática". [23]

Definiciones se pueden señalar muchas. Desde nuestra perspectiva podemos conceptualizar al Derecho Informático como el "conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática a los problemas que se deriven de la misma en las que exista algún bien que es o deba ser tutelado jurídicamente por las propias normas".

---

[20] Cfr. FROSINI, Vittorio, *Informática y Derecho*, Ed. Temis, Colombia, 1988 p135.

[21] CARRACOSA LÓPEZ, Valentín,, citado por FIX FIERRO, Héctor. *Informática y Documentación Jurídica*, UNAM, Facultad de Derecho, México. 1990 p. 53.

[22] SUÑÉ, Emilio, *Introducción a la Informática Jurídica y al Derecho Informático*, Ed. Monográfico, Madrid, 1986 p 77.

[23] TÉLLEZ VALDÉZ, Julio, Ob. Cit. p 58.

1.3 INTERNET

Para poder comprender el funcionamiento de Internet es necesario definirla, y para definirla tenemos que conocer su historia, su evolución y analizar su futuro a la luz de las distintas variables científicas, económicas y académicas relacionadas con la gran Red. El concepto Internet no es único, sino polifacético. Un gran fenómeno mundial con diversas aristas.

1.3.1 HISTORIA

Internet no nació como un proyecto, ni tampoco se concibió como red de un sistema de cómputo como se podría suponer. Internet nació como un sistema político-militar el cual debía satisfacer las necesidades del Ministerio de Defensa de Estados Unidos de Norte América. La gestación de la autopista de la información tuvo lugar hace casi treinta años

En 1957, en plena Guerra Fría la ex Unión Soviética puso en órbita el primer satélite artificial llamado *Sputnick*, lo cual causó alarma a militares y a civiles de los Estados Unidos y ante esta situación de desconfianza, la reacción del actual Presidente Dwight Eisenhower creó la ARPA siglas de la Agencia de Proyectos Avanzados de Investigación (Advance Research Projects Agency), con el objeto de promover la investigación y el desarrollo de nuevas tecnologías para la Defensa Nacional. La principal preocupación que tenían los Estados Unidos era que una guerra nuclear pudiera cortar las comunicaciones, así que las vías para conectar redes tenían que ser flexibles.

Los creadores de este sistema tuvieron el cuidado de desarrollar reglas voluntarias que cubrieran todos los aspectos de dicho sistema, por lo tanto se desarrolló una tecnología que permitiría segmentar la información en pequeños trozos, cada uno de ellos etiquetados con la dirección de un servidor de destino en la red, que a su vez, se conectaba con computadoras o nodos.

En 1962, J. C. R Licklider Doctor en Psicoacústica y profesor del Instituto Tecnológico de Massachussets, fue elegido para presidir uno de los departamentos de la ARPA, él tenía como misión tratar de utilizar todos los descubrimientos realizados en materia de tecnología aplicada a la computación militar para su uso por el sector privado.

Vislumbró como trasformar el uso gubernamental de las computadoras en algo más práctico e interactivo, y para expandir rápidamente la tecnología, intuyó la necesidad de movilizar los esfuerzos de ARPA hacia el sector privado, (en especial las universidades).

El Departamento a cargo de Licklider, fue nombrado *Técnicas de Procesamiento de Información IPT o IPTC*, estos conceptos son los que transformaron los proyectos iniciales en la actual *autopista informática* como es: gente interconectada, recursos interconectados, información interconectada, etc. Esto constituyó la piedra angular a lo que daría origen **Arpanet**.

En 1964, la Empresa Rand Corporation, integrante del grupo militar industrial, y bajo el secreto militar, estudió el problema sobre el ataque nuclear y llegando a una posible solución, la cual se hizo pública en ese año, se crea una red sin autoridad central que pueda operar en un entorno fragmentado. Una red de ordenadores interconectados capaz de trabajar incluso cuando uno o varios de ellos quedaran aislados. Todos los ordenadores tendrían el mismo status: autonomía para generar, enviar y recibir mensajes. Este concepto se le conoce como *packet witching networking*, es decir, se dividen los mensajes en diferentes paquetes.

En 1968, en Gran Bretaña, tanto la Empresa Rand Corporation, el Instituto Tecnológico de Massachussets, y la Universidad de California-Angeles, investigaron a partir de esta idea y realizaron el primer ensayo de *Red de Comunicaciones* el cual se produjo en el Laboratorio de Física de este país.

En 1969, dentro de ARPA nace **Arpanet** (Advance Research Projects Agency Network), la cual funcionó con un programa de computación especial denominado Network Control Protocol, que hizo posible el uso descentralizado de la red, esta era la forma de soiucionar las eventualidades de un ataque nuclear.

Todos los Organismos Gubernamentales y Militares quedaban conectados sin perjuicio de lo que ocurriera en la superficie, dado que las computadoras de la red eran independientes y no existía un centro que organizara el tráfico de información. Con el nacimiento de Arpanet como solución a un problema de Seguridad Militar se gesta lo que luego sería la International Networking (red internacional) Internet.

En 1970, Arpanet creció más allá de sus objetivos originales de sistema de información del Ministerio de Defensa, y es en los primeros años de la década de los setenta donde ARPA, transfiere el proyecto de la Red a la Empresa Bolt Beranek y Newmann.

A partir de este momento la Bolt Beranek y Newmann tendría a su cargo el desarrollo de los nodos y la conexión de Arpa con sus cinco centros de investigación.

En 1972, nace el correo electrónico (e- mail), lo cual hizo que el tráfico de información se incrementara en forma explosiva, dando lugar a la creación de numerosas redes y que cada uno fuera ingresando al nuevo sistema de interconexión.

En 1980, ya había mas de 200 nodos, la estructura descentralizada de la red hacía fácil su expansión, no importando que tipo de computadora, sólo bastaba que hablara el mismo lenguaje utilizado por Arpanet, y con la continuación de las investigaciones nace el protocolo TCP/IP, un sistema de comunicaciones sólido bajo el cual se integrarían todas las redes que actualmente componen Internet.

El desarrollo de este protocolo fue llevado a cabo por Vinton Cerf en la Universidad de Stanford. Son las primeras referencias a Internet como una serie de redes conectadas entre sí, específicamente aquellas que utilizan el protocolo Transfer Control Protocol, responsable de transformar los datos en paquetes, y el Internet Protocol, es el encargado de manejar el viaje de los paquetes a través de distintos nodos y redes dada la dirección de su destino.

En 1983, Arpanet separó su parte militar en lo que se conoce como *Milnet*, debido a su crecimiento, de modo que ya sin fines militares se puede considerar esta fecha como el nacimiento de Internet.

En 1985, Arpanet pasa de la Agencia ARPA a la National Science Fundation), financiada por el Gobierno de Estados Unidos de América y una de sus obras es mejorar los enlaces troncales de la red a fin de interconectar los cinco centros de supercomputadoras de los Estados Unidos naciendo así el primer Backbone, o Columna Vertebral, se denomina a las redes centrales de gran capacidad.

En 1986, a fines de este año, más de 5000 nodos se encontraban conectados.

En 1989, para ese momento más de 100.000 nodos estaban interconectados, y en marzo de ese mismo año da comienzo al proyecto World Wide Web (WWW), la cual marcaría los destinos de la Red.

En 1990, la National Science Fundation deja de subsistir el desarrollo de la Red.

En 1994, eliminaron las restricciones comerciales existentes hasta ese momento y a finales de este año ya había 3.8 millones de nodos registrados y más de treinta millones de usuarios.

En 1995, es el año del gran boom de Internet. Puede ser considerado como el nacimiento de la Internet comercial. Desde ese momento el crecimiento de la Red ha superado todas las expectativas y para lo cual es posible utilizar este sistema para objetivos de índole muy diversa, incluidos claro, los de carácter comercial.

A partir de este año empiezan a incrementarse de una manera casi exponencial el número de servicios que operan en la red. Gobiernos de todo el mundo se conectan a la red, y el registro de dominios deja de ser gratuito para pagarse una cuota. El web continúa creciendo y cambiando de manera a veces impredecible.[24]

1.3.2 CONCEPTO

A partir de su funcionamiento, servicio y tecnología empleada del desarrollo del Internet no se ha integrado de manera definitiva una definición general aceptada, sin embargo es necesario establecer algunos conceptos sobre este gran fenómeno mundial, para dar una idea de lo que es Internet:

"Internet es un sistema maestro de diversas redes de computación que cumple dos funciones básicas: como medio de comunicación, en donde Internet ofrece una amplia gama de canales de enlace, entre los que se hallan la comunicación escrita (por ejemplo el e-mail), la comunicación verbal (contacto por teléfono) e incluso comunicación verbal (tele conferencia en Internet), y como medio de información, Internet puede compararse con una gran biblioteca".[25]

"Internet es una federación de redes de computadoras que emplean los mismos protocolos para comunicarse".[26]

De los anteriores conceptos podemos deducir que el Internet es una red que conecta a su vez a otras redes de computadoras a nivel mundial, utilizando en México, como medio de conexión, las redes terrestres e inalámbricas de telefonía pública, y tiene como fin la transmisión y recepción de información que se encuentra en el espacio telemático, entre redes y usuarios.

---

[24] http://geocities.com

[25] BARRIOS, Gabriela, MUÑOZ DE ALBA, Marcia, y PÉREZ BUSTILLO, Camilo. *Internet y Derecho en México*, Ed. McGraw Hill, México, 1998 p. 75.

[26] CRÍCKET LIU, Jerry Peek, RUSS Jones; BRUS Bryan y NYE Adrián, *Administración de Servicios de Información*. Ed. Prentice Hall, segunda ed. México. 1998 p.1.

1.3.3 EL IMPACTO SOCIAL DE INTERNET

Una vez que ha quedado definido lo que se debe entender por Internet, y a fin de que podamos entender el por qué el Internet ha tenido un impacto de tan grandes magnitudes es necesario explicar su funcionamiento; no sin antes mencionar en forma breve aquellos conceptos que a manera de antecedente nos van a ayudar a comprender mejor este funcionamiento:

Red: Conexión de varias computadoras a través de un cableado especial, para compartir datos y en términos reales, las redes se pueden conectar mediante diferentes formas de construcción o arquitecturas que pueden utilizar diferentes tipos de cables como lo puede ser las líneas telefónicas, fibras ópticas, satélites etc.

Modem: Es un dispositivo electrónico que sirve para convertir señales digitales a análogas y viceversa, con el fin de transmitir a través de líneas telefónicas los datos que las computadoras manejan de manera digital o binaria.

Ciberespacio o Espacio Telemático: Es el territorio imaginario que hay al otro lado del monitor del ordenador y en el que se puede visualizar programas, datos y otros elementos.

En el argot del Internet se podría decir que es el área por la que viajan los usuarios de ordenadores y navegan a través de una red.

Por lo tanto, el Espacio Telemático es el espacio abstracto que contiene información, la cual es transmitida a través de las redes de telecomunicaciones informáticas, espacio material y más adecuado a través del Internet.

Telemática: Es un término que alude al conjunto de métodos, técnicas y servicios que resultan del uso conjunto de la informática y las telecomunicaciones.

Telecomunicaciones: Es toda emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonido o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos, u otros sistemas electromagnéticos.[27]

[27] http://www.servitel.es/atv/ayu/INTERNET/DICCIO/diccio.htm

Con respecto a su funcionamiento, el Internet trabaja con redes, las cuales se conectan con servidores y a su vez a las computadoras de los usuarios mediante protocolos denominados TCP/IP, así lo que mantiene funcionando al Internet son millones de servidores que ejecutan millones de programas, todos conectados entre sí mediante estos protocolos que permiten que el usuario se conecte con su computadora a dichos servidores y a otros usuarios.

El funcionamiento de Internet implica el envío de información de un equipo interconectado a otro hasta que dicha información alcanza su destino, esto se traduce en la conexión con un módem de una computadora a otra a través de una línea telefónica ya sea terrestre o inalámbrica, la información de esta manera entra al espacio telemático en donde se encuentran interconectadas otras computadoras a los servidores formando de esta manera un sistema global de transferencia de información denominado Web, el cual se usa para enviar una serie de datos y proveer el acceso a una variedad de servicios.

Estas páginas o sitios pueden ser accedidas mediante una dirección que incluye un comando de distribución denominado *http* por sus siglas en inglés *hiper text transfer protocol*, en español Protocolo de transferencia de hipertexto el área de la Web, que se señala con www (world wide wibe).

El Internet y el Ciberespacio, como ya se mencionó, pertenece al ámbito de las Telecomunicaciones, en razón de esto y su proliferación acelerada en los distinto sectores de la sociedad; se ha vinculado con diversos campos que atañen de manera directa aspectos importantes para la vida del país, ya que se encuentran ligados a las fuentes de información que generan y utilizan los gobiernos federales y estatales en sus tres poderes; así como cuestiones de política económica e inversión extranjera, distribución, operaciones bancarias, indicador del movimiento bursátil, generador de relaciones jurídicas contractuales, educación e investigación entre otros; a estos se suman los que realiza el público usuario que ha hecho del sistema una herramienta para sus actividades, formándose de esta manera un universo de contenidos e información en el ciberespacio.

Desafortunadamente no todos los usuarios los generan o utilizan de manera positiva, esto en razón de varias conductas, circunstancias y comportamientos lo cual explicaremos con mayor detenimiento en el capítulo III sobre los Delitos Informáticos del presente trabajo.

Los servicios que te ofrece Internet son:

Páginas web propias
Correo Electrónico
Transferencia de archivos
Investigaciones
Cursos
Servicio de Chat
Transmisión de Voz
Comunicación en tiempo real
Comercio Electrónico.
Medio masivo de publicidad

La trascendencia y el impacto social que el Internet ha tenido en la última década, ha provocado necesariamente que tanto las autoridades, como la sociedad en si misma, tenga que considerar la influencia que este medio de comunicación tiene y tendrá en el futuro, ya que poco a poco nos percatamos de que cada vez la utilización de ésta red informática, ha desplazado y modificado diversas costumbres tanto individuales como sociales, así como en la forma de comunicación interpersonal.

Evidentemente el Internet se perfila como medio de comunicación que satisface los requerimientos actuales de los usuarios y de ahí el éxito de dicho esquema y la rápida multiplicación de los denominados cibernautas, por lo cual el Internet ha sido comparado con mucho a la invención de la radio, cuyo contexto en su época, revolucionó la forma de relacionarse de los habitantes de una comunidad social determinada.

Es claro el pronóstico de Internet, como influencia en el ámbito social de una comunidad que se encuentra ligada irremediablemente a esta doble posibilidad, ya que por un lado se ubica la de crear comunidades virtuales en que cada persona adopte el rol o papel que más le satisfaga, sin que sea necesario circunscribirse a una realidad social, mientras que por el otro lado se haya la posibilidad virtual de que técnicamente desaparecer la distancia geográfica habida entre dos usuarios, lo que permite conocer y participar de una sociedad y cultura que se podría encontrar a muchos kilómetros de distancia.

La era de la informática se ha consolidado de forma tal que sus implicaciones han modificado substancialmente la forma de pensar y diversas conductas de la comunidad social, esto se ha generado inevitablemente que existan diversas influencias en el entorno social en que nos desenvolvemos.

Es claro que esta utilización de la informática se ha revestido de diversas ventajas y desventajas que necesariamente influyen en el grupo social en que se desenvuelven; en términos generales consideramos que las principales ventajas y desventajas en el uso de la informática y la cibernética pueden ser catalogadas en los siguientes rubros:

Ventajas del uso de Internet.

-Estimula el uso de nuevas formas de aprender y consultar información.
-Cuenta con buenas herramientas de apoyo al trabajo colaborativo como diseño , desarrollo y evaluación de proyectos, investigación, experimentación y trabajo interdisciplinario.
-Ayuda a aprender de otros y con otros
-Estimula el trabajo global y la interdisciplinariedad
-Sistematización de la Información
-Educación a distancia

Desventajas al usar Internet.

-La cantidad y calidad de la información circulante
-El tiempo que el usuario requiere para navegar
-Estabilidad de las conexiones (lentitud)
-Metodologías de trabajo poco eficaz
-La carencia de mapas de navegación
-Demasiada información poco confiable
-Problemas Jurídicos
-Medio masivo de propagación de virus informáticos

Para concluir diremos que el entender el derecho como tecnología supone un cambio de perspectiva, que hará posible que el Derecho, desde su propia esencia, pueda aprovechar convenientemente las ventajas de las nuevas tecnologías, y ponerse a la altura de los tiempos garantizando y haciendo posible las imprescindibles condiciones de orden, control, seguridad, eficiencia y justicia que la sociedad requiere para una adecuada estructuración de las interacciones económicas, sociales y políticas.

CAPÍTULO II

DELITO

2.1 EVOLUCIÓN HISTÓRICA DEL CONCEPTO DEL DELITO

El delito fue siempre una valoración de la conducta humana condicionada por el criterio ético de la clase que dominaba la sociedad. Los conceptos se desarrollan en los siglos XVIII, XIX y XX, que se describen a continuación.

El concepto jurídico encabezado por: Romagnosi, Carmignanni, y Carrara, establecen que el delito es la infracción de la ley del Estado promulgada para proteger la seguridad ciudadana, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso. Para Carrara el delito es un ente jurídico (creación de la ley) y no un fenómeno social (ente de hecho). Es un ente jurídico porque es una contradicción entre el hecho del hombre y la ley. Por eso no se define como acción sino como infracción, lo que supone la antijuridicidad la esencia del delito y no solo su elemento.

Al decir acto externo, se refiere a que no son sancionables los actos internos o pensamientos, sólo los actos exteriorizados del hombre. El pensar en matar no es delito, mientras no lo exteriorice. Con acto positivo se refiere a las acciones voluntarias humanas. Con acto negativo, se refiere, a un "no hacer" lo que la ley manda a hacer, o sea a la omisión.

Moralmente imputable, significa a que el hombre comete el delito en base a su libre albedrío, el hombre puede escoger entre la comisión de un delito o no. Con políticamente dañoso se refiere a que el delito al violar los derechos de otra persona, también está perjudicando a la sociedad.

Este concepto jurídico no es aceptado, porque el delito no es algo creado por la ley, la ley solo la define, es mas, sólo la describe en el tipo, el delito es un hecho humano, aparece con el hombre, y desaparecerá con él. El delito es al hombre como la enfermedad a él.

En ese mismo orden, el concepto filosófico de Pellegrino Rossi, Franck, Pessina, de la Escuela Clásica; establece que el delito es una violación de un derecho fundado sobre la ley moral. Para esta concepción, el delito consiste en la violación de un deber. La pretensión de validez es socavada porque lo que lo que ayer fue delito deja de serlo con el paso del tiempo y con la abrogación de la ley que lo concibió como delito.

Por otro lado, el concepto sociológico establecido por Rafael Garófalo, Enrico Ferri, Tarde, Colanjanni, Durkheim de la Escuela Positivista; consideran al delito como la lesión de los sentimientos altruistas fundamentales de piedad y probidad, en la medida en que son poseídos por la comunidad y en la medida en que son indispensables para la adaptación del individuo a la sociedad. Aunque esos sentimientos son inherentes al ser humano, no son los únicos. Este concepto rechaza lo que la ley considera como delito.

El concepto dogmático, del que parten Binding, Beling, Mayer, Mezger, establece que el delito es la acción u omisión voluntaria típicamente antijurídica y culpable, y enumera los elementos constitutivos del delito.

El delito es un acto u omisión voluntaria, quedan descartadas las conductas que no son conducidas por la voluntad, como las conductas por fuerza irresistible, acto reflejo o situaciones ajenas a lo patológico (sueño, sonambulismo, hipnotismo), supuestos en los que no existe conducta, por tanto no hay delito.

El delito es un acto típico, todo acto humano para considerarse como delito debe adecuarse al tipo penal. Es decir debe haber tipicidad. Si no hay adecuación no hay delito, o peor aun, si no hay tipo, la conducta no es delito.[28]

[28] Cfr. JIMÉNEZ DE ASÚA, Luis, Lecciones de Derecho Penal, Ed Harla, México Vol. 7 1998 pp.128-173.

2.2 CONCEPTO DE DELITO

El profesor Guillermo Cabanellas en su Diccionario Enciclopédico de Derecho Usual nos enseña acerca del delito lo siguiente. Etimológicamente la palabra delito proviene de la similar latina *delitum*, aún cuando en la técnica romana poseyera significados genuinos, dentro de una coincidente expresión calificadora de un hecho antijurídico y doloso sancionado con una pena. En general, delito es culpa, crimen, quebrantamiento de una ley imperativa, entre otros.

El delito siempre ha sido considerado como un fenómeno natural o social, así como un fenómeno jurídico.

Como fenómeno social varios son los autores que han querido dar una definición del delito.

Garófalo, considera al delito ya sea social o natural como una lesión de aquella parte del sentido moral que consiste en los sentimientos altruistas fundamentales (Piedad y Probidad), según la medida en que se encuentran las razas humanas superiores, la cual es necesaria para la adaptación del individuo a la sociedad.

Sin embargo, varios son los autores que han pretendido ofrecernos una definición o un concepto de lo que se entiende por delito o su equivalente infracción.

Un concepto moderno del delito según el profesor español Luis Jiménez de Asúa, fue formulado por Romagnosi y Feuerbach; luego mejorado por Carming; y finalmente, perfeccionado por Carrara, quien lo expuso de la siguiente manera: Delito es "infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo, positivo o negativo moralmente imputable o políticamente dañoso".[29]
Sin embargo, ampliando el concepto anterior el profesor Jiménez de Asúa define el delito como un acto típicamente antijurídico, culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción

La palabra Delito deriva del verbo latino *delenquere*, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley.[30]

---

[29] Ibidem., p. 137.

[30] Diccionario Jurídico Mexicano Ed. Porrúa, UNAM, México 1994.

De acuerdo a su etimología y, estableciendo desde luego que, *Concepto* es la idea, forma y modo de ver el delito que se expresa en una fórmula llamada definición, la cual debe indicar lo que es el delito y debe sintetizar los criterios, tenemos lo siguiente:

El delito siempre ha sido considerado como un fenómeno natural o social, así como un fenómeno jurídico como se vio anteriormente, sin embargo, el delito así definido, tiene un carácter predominantemente objetivo, puesto que contiene una relación delito-pena, la cual la hace carecer de todo nexo moral del acto con el agente; y en ese mismo orden el concepto del delito pueden ser agrupado de dos formas: formal o nominal, y substancial o material.

El concepto nominal o formal define al delito como una conducta humana que se opone a lo que la ley manda o prohíbe bajo la amenaza de una pena. Es la ley la que establece que hechos son delitos, fija caracteres delictuales a un hecho.

El concepto substancial o material del delito establece elementos del delito como presupuestos para que un hecho humano sea considerado como delito.[31]

El delito es un acto humano típicamente antijurídico culpable y sancionado con una pena. De este método analítico, se obtienen los elementos constitutivos del delito que se expresarán posteriormente, por lo tanto concluimos que en nuestro Régimen de Derecho, *Delito* es la conducta que la ley le brinda esa categoría como lo establece el Código Penal Federal vigente en su artículo 7° que a la letra dice: "Delito es el acto u omisión que sancionan las Leyes Penales", y cuya excepción se encuentra en las Leyes Inconstitucionales por adolecer de validez Constitucional, es decir, las que son contrarias al Principio de Igualdad Jurídica o establecen penas de las proscritas en nuestro régimen de derecho.

31 http://www.geocities.com/teoriadeldelito/ y http://www.lexisnexis.cl/

2.3 ELEMENTOS CONSTITUTIVOS DEL DELITO

Ahora bien, antes de iniciar el estudio de los elementos del delito y de sus aspectos negativos, consideramos necesario precisar ciertos conceptos, como son los presupuestos, elementos y circunstancias del delito en general, para posteriormente analizar su validez la cual es reconocida por los estudiosos del Derecho Penal al precisar cuáles son sus elementos constitutivos y cuáles sus elementos que son consecuencia; por lo que sólo mencionaremos a Fernando Castellanos Tena, y Francisco Pavón Vasconcelos, por ser el punto de partida a nuestro particular punto de vista.

2.3.1 PRESUPUESTOS DEL DELITO

Se puede definir a los presupuestos del delito como "las circunstancias jurídicas o de hecho, cuya existencia debe ser previa a la realización del delito".[32]

Manzini los define como "aquellos elementos jurídicos anteriores a la ejecución del hecho, positivos o negativos, a la existencia o inexistencia de los cuales está condicionada la existencia del título delictivo del que se trata".[33]

Ahora bien, dichos presupuestos se dividen en dos: Generales y Especiales.

Los presupuestos generales son aquellos que necesariamente deben de ocurrir por la configuración de un delito, ya que su ausencia implicaría la imposibilidad de integrarlo, o bien, aquellos comunes al delito en general, tal es el caso de la norma penal, el sujeto activo, el sujeto pasivo y el bien jurídicamente tutelado. Y por otro lado tenemos a los especiales, que son aquellas condicionantes de la existencia de un delito concreto y cuya ausencia pede originar la no aparición del delito, o bien, aquellos propios de cada delito e particular.

Una vez analizados los presupuestos del delito, se procederá a estudiar los elementos del mismo.

---

[32] CASTELLANOS TENA, Fernando Lineamientos elementales de Derecho Penal Ed. Porrúa decimooctava ed. México, 1986 p.134.

[33] Manzini *Tratado de Derecho Penal*, Torro II 20° ed. Ed. Abeledo Perrot Buenos Aires. 1954 p. 37.

2.3.2 ELEMENTOS DEL DELITO

Por elemento, en general, debemos entender "la parte integrante de algo, aquello que es indispensable o necesario para que ese algo tenga existencia".[34]

Los elementos del delito están divididos en dos: esenciales o constitutivos y accidentales.

Por elemento esencial, tenemos que, es aquel indispensable, necesario para constituir el delito en general o el delito en particular (tales como la conducta, la tipicidad o la antijuridicidad). Los elementos accidentales son aquellos que no son indispensables para que exista el delito, su función es la de agravar o atenuar la pena y de dichos elementos se desprenden las circunstancias del delito, mismas que dan lugar a la clasificación en orden al tipo.

En ese mismo orden de ideas y expuestos los puntos anteriores, hay que precisar que la validez de este método de estudio por esta teoría, parte de la definición que los doctrinarios hacen y que a continuación se mencionan.

2.3.3 ELEMENTOS SEGÚN FERNANDO CASTELLANOS

El maestro Castellanos Tena, considera elementos constitutivos del delito a la acción, la tipicidad, la antijuridicidad, y la culpabilidad. Excluye de los elementos del delito a la imputabilidad por considerarle un presupuesto de la culpabilidad, a la punibilidad y las condiciones objetivas de penalidad, por tenerles como consecuencia del delito.

Define a los elementos del delito de la siguiente manera:

Empezaremos por mencionar a la *conducta*, término que prefiere pues dentro de éste se puede incluir correctamente tanto el hacer positivo como el negativo, es decir, el comportamiento humano, voluntario, positivo o negativo, encaminado a un propósito.

Por lo tanto la *ausencia de conducta* produce la inexistencia del delito, uno de los aspectos negativos o impeditivos de la figura delictiva, es decir la base indispensable del delito como de todo problema jurídico.

---

[34] PORTE PETIT, Celestino. *Apuntamientos de la parte general de derecho penal* Ed. Porrúa16ª ed. México,1997 p. 200-201.

El segundo elemento que enumera es a la *tipicidad*, y que define como el encuadramiento de una conducta con la descripción en la ley.

Por consiguiente la atipicidad es la ausencia de adecuación de la conducta al tipo, y establece algunas causas de atipicidad como son; ausencia de calidad exigida por la ley en cuanto a los sujetos activo y pasivo, el faltar el objeto material o el objeto jurídico, cuando no se dan las referencias temporales o espaciales requeridos en el tipo, o al no realizarse el hecho por los medios comisivos específicamente señalados por la ley, o bien si faltan algunos de los elementos subjetivos del injusto legalmente exigidos.

El tercer elemento es la *antijuridicidad* que la define como la violación del valor o bien protegido a que se contrae el tipo penal respectivo, por lo tanto la ausencia de antijuridicidad ocurre ante la presencia de alguna causa de justificación.

Y el cuarto elemento es la *culpabilidad* por lo que establece que es el nexo intelectual y emocional que liga al sujeto con su acto, su ausencia da origen a la *inculpabilidad* la cual opera al hallarse ausentes los elementos esenciales de la culpabilidad; como son el conocimiento y la voluntad.

Por otro lado a la *punibilidad* no lo considera elemento del delito por ser una consecuencia de éste, como es: el merecimiento de penas, la amenaza estatal de imposición de sanciones si llena los presupuestos legales y la aplicación fáctica de las penas señaladas en la Ley. La ausencia de ésta son las causas que dejando subsistente el carácter delictivo de la conducta o hecho, impiden la aplicación de la pena.

Ahora bien, la *imputabilidad* tampoco la considera elemento del delito por ser un presupuesto de la culpabilidad, por eso lo ve como el soporte básico y esencialísimo de ésta; es decir es la capacidad de querer y entender en el campo del Derecho Penal, para lo cual establece que su ausencia o bien la inimputabilidad tiene causas, las cuales son capaces de anular o neutralizar, ya sea el desarrollo o la salud de la mente, en cuyo caso el sujeto carece de aptitud psicológica para la delictuosidad, y en este sentido enumera dichas causas como los estados de inconsciencia los cuáles son: el permanente, que son los trastornos mentales; los transitorios, que son producidos por ingerir sustancias tóxicas o estupefacientes, sin que se haya producido esa incapacidad en forma intencional ó imprudencial y los trastornos originados en las toxiinfecciones así como los trastornos patológicos; el miedo grave; la sordomudez y los menores de 18 años.[35]

[35] Cfr. CASTELLANOS TENA, Fernando. Ob. Cit. pp. 147-279.

2.3.4 ELEMENTOS SEGÚN FRANCISCO PAVÓN

En ese mismo sentido el doctrinario Francisco Pavón Vasconcelos también refiere a los mismos elementos del delito con algunas diferencias como lo es al nombrar a la conducta como *hecho* por su mayor contenido comprensivo de la conducta humana, de su resultado y del nexo causal entre una y otra, sin descartar que también establece dos formas de conducta que son la acción y la omisión; considerando la primera como una conducta positiva expresada mediante un hacer, una actividad, un movimiento corporal voluntario con violación de una norma prohibitiva, y la segunda como una conducta negativa, la cual es inactividad con violación de una norma preceptiva (omisión simple), o de ésta y una prohibitiva (omisión impropia o comisión por omisión).

Referente a la *antijuridicidad* el establece que es un juicio valorativo de naturaleza objetiva, que recae sobre la conducta o el hecho típico en contraste con el derecho, por cuanto se opone a las normas de cultura reconocidas por el Estado. Y en cuanto al cuarto elemento que es la *culpabilidad* lo significa en dos sentidos; en sentido estricto dice que es reprochabilidad y en sentido amplio se estima como el conjunto de presupuestos que fundamentan la reprochabilidad personal de la conducta antijurídica.

Al igual que el maestro Castellanos, la *imputabilidad* la establece como un presupuesto de la culpabilidad y no como un elemento del delito a la cual la define como la capacidad del sujeto para conocer el carácter del ilícito del hecho y determinarse espontáneamente conforme a esa comprensión; y en ese mismo sentido dice que la *punibilidad* es la amenaza de pena que el Estado asocia a la violación de los deberes consignados en las normas jurídicas, dictadas para garantizar la permanencia del orden social, es decir, su consecuencia.

También menciona sus aspectos negativos; a saber la *ausencia del hecho* y por ello del delito que surge al faltar cualquiera de sus elementos que lo componen como es la ausencia de conducta en la cual se encuentra la vis absoluta (fuerza irresistible que proviene necesariamente del hombre), y la fuerza mayor (la cual encuentra su origen en una energía distinta ya natural o subhumana), la inexistencia del resultado como es la ausencia de adecuación típica, en la cual concreta las mismas causas que Castellanos.

También hace referencia a que la agresión antijuridica no significa necesariamente lesión al derecho atacado de ello son las causas de justificación, y por lo que toca a la *culpabilidad* menciona dos causas genéricas de exclusión que son: el error y la no exigibilidad de otra conducta. En los primeros casos se encuentra comprendida la excluyente de incriminación de error invencible y, las eximentes putativas de legítima defensa, estado de necesidad, ejercicio de un derecho y cumplimiento de un deber. En el segundo de los supuestos están comprendidas las excluyentes de incriminación de estado de necesidad, de temor fundado e irresistible, el aborto entre otros.

Por último considera a las excusas absolutorias como el aspecto negativo de la punibilidad y los casos como los delitos cometidos por menores de edad, enfermos mentales, sordomudos como casos de inimputabilidad.[36]

Debido a que el objetivo de este trabajo no es hacer un análisis de cada doctrinario por mas interesante que éste sea lo cual implicaría otro tema de estudio. A continuación se establecen aquellos elementos constitutivos del delito así como sus aspectos negativos desde una perspectiva objetiva y personal.

Los Elementos Constitutivos del Delito como ya lo vimos son los supuestos previstos en la norma jurídica, satisfecha la hipótesis legal por actos materiales que la configuren, produciendo la obligación (delito) y la pena para sancionarle.

2.3.5. ANALISÍS DE LOS ELEMENTOS DEL DELITO

Por consiguiente los Elementos Específicos del Delito son, la acción, la tipicidad, antijuridicidad, y la culpabilidad ,los cuáles son propios de cada delito y eso permite diferenciarlos.

Acción.
Solo puede ser delito la conducta humana, revistiendo las características que la ley le establece pues quien va a determinar que actos de los seres humanos tienen la categoría de delito, contemplándolos como una acción u omisión tal como lo establece el Código Penal Federal en su artículo 7° y para el Distrito federal en su artículo 15. La acción es conducta omisiva o activa voluntaria, que consiste en un movimiento de su organismo destinado a producir cierto cambio.

[36] CFR. PAVÓN VASCONCELOS, Francisco. *Manual del Derecho Penal Mexicano*. Parte General. Ed. Porrúa, quinta ed, México 1974 pp.180-434.

Tipicidad.
Al respecto es importante mencionar que no debemos confundir al tipo penal con la tipicidad. El tipo es una creación legislativa de conductas que pueden acontecer en el mundo fáctico, descritas en preceptos penales de un hecho, es decir, es la descripción de la conducta que el legislador considerará como delito.

Sin embargo, la tipicidad es considerada como "la adaptación de la conducta al tipo previamente descrito, o la adecuación de un hecho cometido a la descripción que de ese hecho se hace en la Ley Penal",[37] es por eso que la tipicidad constituye uno de los elementos esenciales del delito, su ausencia impide su configuración, tan es así que en nuestra Constitución en su artículo 14 establece que "En los juicios del orden criminal queda prohibido imponer, por simple analogía y aún por mayoría de razón, pena alguna que esté decretada por una ley exactamente aplicable al delito de que se trata".

Lo anterior significa, que en caso de que una persona cometa alguna conducta, que a decir de la sociedad es considerada delictiva, pero la misma no está prevista en una ley penal, al sujeto que la cometa no se le podrá castigar, en virtud de que no puede haber delito sin tipicidad.

El tipo es el hecho descrito en el Código Penal o en leyes especiales, dotado de sanción (pena, medida de seguridad, o ambas), y a la vez protege bienes jurídicos. En tanto que la tipicidad es la correspondencia entre una conducta determinada y el esquema legal que plantea la figura de cierto delito.

Ahora bien, el tipo "es la descripción concreta hecha por la ley de una conducta a la que en ocasiones se suma su resultado, reputada como delictuosa al conectarse a ella una sanción penal".[38]

Concluimos entonces que la tipicidad es la adecuación, es el encaje del acto humano voluntario, ejecutado por el sujeto a la figura descrita por la ley como delito. Si la adecuación no es completa no hay delito. Es decir, es el contenido de la norma jurídica o bien la hipótesis legislativa.

---

[37] ZAMORA JIMÉNEZ, Arturo. *Cuerpo del Delito y tipo penal.* Ed. Angel México, 1999 p. 56.

[38] PAVÓN VASCONCELOS, Francisco., Ob. Cit p. 294.

Antijuridicidad.
La antijuridicidad es la oposición del acto voluntario típico al ordenamiento jurídico. La condición de la antijuridicidad es el tipo penal. Como ya vimos el tipo penal es el elemento descriptivo del delito, por lo tanto la antijuridicidad es el elemento valorativo.

Toda conducta que se realice en la forma en que la Ley la cataloga la figura delictiva, es antijurídica por contravenir una norma de derecho. El delito existe cuando se consagra en la norma jurídica con validez constitucional. Los hechos materiales actualizan la obligación (delito) prevista en la Ley y producen la coercitividad que contempla la norma para sancionar la conducta.

Culpabilidad.
La culpabilidad como se expresó anteriormente, no podría considerarse el nexo intelectual y emocional ya que la responsabilidad penal se determina por resultados materiales criminosos y no en elementos subjetivos, como ideas y emociones, tampoco se puede considerar una reprochabilidad ya que ésta es la facultad del Estado para sancionar a los ciudadanos que han cometido delitos y en ese caso se estaría hablando de responsabilidad penal; así como tampoco se podría definir como la reprobación jurisdiccional pues ésta, en dado caso sería la consecuencia. Y ante ésta perspectiva se deduce que la culpabilidad para nosotros es la que permite determinar la responsabilidad penal que puede corresponder al autor del delito, según el tipo de conducta que realizó. Consecuentemente se dice que es el instrumento que precisa el grado de responsabilidad penal que corresponde al delincuente, cuando se determina la existencia del delito.

Coincidimos con los doctrinarios que se consultaron para el estudio del delito, en que la imputabilidad no es elemento constitutivo del delito al igual que la punibilidad, lo cual se explica de la siguiente manera:

Imputabilidad.
La imputabilidad no es elemento del delito en el entendido de que el delito existe cuando se consagra la conducta con esa categoría en la ley, tampoco es un presupuesto de la culpabilidad ya que el autor de la conducta es delincuente o infractor según la Ley Penal que rija sus actos, mas bien nos permite conocer qué ley le resulta aplicable al autor de la conducta cuando estos actos materiales constituyen delitos por así ordenarlo las normas de derecho.

Esta figura jurídica sólo describe quiénes son los sujetos de la Ley Penal. La imputabilidad no es la capacidad de querer y entender en el campo del Derecho, por que la Ley es obligatoria y rige los actos de los gobernados, se entienda su contenido o no.

Punibilidad.
Al igual que la imputabilidad no lo consideraremos como un elemento del delito por ser este ya existente en la Ley pero, con independencia de que se señale o no responsabilidad penal, pues sería totalmente absurdo establecer un delito en la Ley y no establecer su sanción.

La pena (del latín *poena*, sanción) es la privación o disminución de un bien jurídico a quien haya cometido, o intente cometer un delito. La causa de la pena es el delito cometido, la esencia es la privación de un bien jurídico y el fin es evitar el delito a través de la prevención general o especial.[39]

Continuando con el estudio, y de acuerdo con Alberto Mancilla Ovando mencionaré la inexistencia del delito ante la falta de sus elementos constitutivos los cuáles son los siguientes:

Ausencia de Conducta.
La ausencia de conducta significa que en el mundo exterior no se han materializado los actos que prevé la norma jurídica como constitutivos de delito, por lo tanto, existe ausencia cuando los sujetos de la ley penal no han realizado la acción u omisión que la ley penal establece como delito.

No se puede considerar ausencia de conducta, la excluyente de incriminación denominada *vis* absoluta o fuerza física exterior e irresistible que consagra el artículo 15 fracción I del Código Penal Vigente.

La excluyente de responsabilidad, establece un derecho del gobernado que realiza la conducta delictiva con ausencia total de su voluntad. En esos casos, la conducta material constituye delito y el resultado es criminoso, pero el autor de la conducta no es castigado, porque la eximente le excluye de la imposición de responsabilidad penal que corresponde al delito. Como derecho, la excluyente de incriminación integra la esfera jurídica de los gobernados y declarada su existencia, la conducta adquiere validez constitucional y licitud de sus defectos, produciendo la prerrogativa de no ser castigado por el delito que cometió.

[39] Cfr. MANCILLA OVANDO Jorge Alberto, Teoría Legalista del Delito, Ed. Porrúa, México 1999 pp. 18-38.

La Atipicidad.
La ausencia de tipicidad significa que la conducta no satisface la hipótesis legal que establece el delito. Los casos de atipicidad que describen los doctrinarios sólo enuncian cuándo la conducta no es delito en ley. Si los actos materiales no configuran delito, no puede hablarse de su existencia, menos aún de su inexistencia, porque no se satisfacen los supuestos de la norma jurídica.

Ausencia de Antijuridicidad.
La ausencia de antijuridicidad significa que la conducta no es contraria a los dictados de las normas del derecho penal. El acto u omisión, no configuran el delito que prevé la ley, en tales circunstancias, el hacer o el dejar de hacer de un gobernado es el ejercicio de su derecho de libertad, por tratarse de actividades propias de su esfera jurídica. Es erróneo determinar que las excluyentes de incriminación, nos quita a la conducta la categoría de delito tal cual se consagra en la ley. La conducta es delito y la eximente excluye la responsabilidad penal al delincuente. Por estas razones, la conducta que es delito, siempre es delictiva, lo que se suspende es la facultad de castigar del juez al no poder imponer responsabilidad penal. En conclusión se dice que toda excluyente de incriminación es un derecho, que integra la esfera jurídica de libertad de los gobernados. El ejercicio de ese derecho no exime de la responsabilidad penal e impide que se castigue al delincuente.

La Inculpabilidad.
Por último diremos que la no culpabilidad significa que el acusado no es el autor de la conducta que constituye delito en la ley y por consecuencia no habrá responsabilidad penal.

La Inimputabilidad.
Al hablar de ésta figura jurídica coincidimos con éste autor al establecer que no existe ésta en el Derecho Penal, pues para la ley penal todos somos sujetos, desde los menores hasta los que la codificación denomina inimputables. Los menores son sujetos que la ley crea (Consejo Titular de Menores), los adultos en ejercicio de sus facultades mentales y aquellos que no poseen estas aptitudes, son sujetos del Código Penal Federal. Por estas razones, la inimputabilidad jamás produce la inexistencia del delito.

La Ausencia de Punibilidad.
Por otro lado la no punibilidad significa la ausencia de responsabilidad penal en el delito, deja subsistente el carácter de delito de la conducta e impide la aplicación de la pena, por no existir sanción en ley.[40]

[40] Cfr. MANCILLA OVANDO Jorge Alberto., Ob. Cit. P. 34-38.

2.4 CLASIFICACIÓN DOCTRINAL DEL DELITO

2.4.1 EN FUNCIÓN DE SU GRAVEDAD

Tomando en cuenta la gravedad de las infracciones penales, se han hecho de diversas clasificaciones. Según una división bipartita se distinguen los delitos de las faltas; la clasificación tripartita habla de crímenes, delitos y faltas o contravenciones. En esta división se consideran crímenes a los atentados contra la vida y los derechos naturales del contrato social, como el derecho de propiedad; por faltas o contravenciones, las infracciones a los reglamentos de policía y de buen gobierno.

2.4.2 SEGÚN LA FORMA DE LA CONDUCTA DEL AGENTE

Estos pueden ser de acción y de omisión. Los de acción se cometen mediante un comportamiento positivo; en ellos se viola una ley prohibitiva. En los delitos de omisión el objeto prohibido es una abstención del agente, consisten en la no ejecución de algo ordenado por la Ley.

Por lo tanto, debe agregarse que los delitos de omisión violan una ley dispositiva, en tanto los de acción infringen una prohibitiva.

Los delitos de omisión suelen dividirse en delitos de simple omisión y de comisión por omisión, también llamados delitos de omisión impropia. Los delitos de omisión simple, consisten en la falta de una actividad jurídicamente ordenada, con independencia del resultado material que produzcan.

Los delitos de comisión por omisión, o impropios, son aquellos en los que el agente decide no actuar y por esa inacción se produce el resultado material.

En los delitos de omisión, hay una violación jurídica y un resultado puramente formal (se viola una ley dispositiva), mientras que en los de comisión por omisión, además de la violación jurídica se produce un resultado material (se infringe una ley dispositiva y una prohibitiva).

2.4.3 POR EL RESULTADO

Según el resultado que producen, los delitos se clasifican en formales (delitos de simple actividad o de acción) y materiales (delitos de resultado o de resultado material).

Los delitos formales. son aquellos en los que se agota el tipo penal en el movimiento corporal o en la omisión del agente, no siendo necesario para su integración que se produzca alguna alteración en la estructura o funcionamiento del objeto material. Son delitos de mera conducta, se sanciona la acción en sí misma.

Los delitos materiales son aquellos en los cuales para su integración se requiere la destrucción o alteración de la estructura o del funcionamiento del objeto material.

2.4.4 POR LA LESIÓN QUE CAUSAN

En razón del bien jurídico, los delitos se dividen en delitos de daño y de peligro. Los primeros, consumados causan un daño directo y efectivo en intereses jurídicamente protegidos por la norma penal violada, como el fraude etc. Los segundos no causan daño directo a tales intereses, pero los ponen en peligro, como el abandono de personas.

2.4.5 POR SU DURACIÓN

Se dividen en instantáneos, instantáneos con efectos permanentes, continuados y permanentes.

Instantáneo.- Este puede realizarse mediante una acción compuesta de varios actos o movimientos. Para la calificación se atiende a la unidad de la acción, si con ella se consuma el delito no importando que a su vez, esa acción se descomponga en actividades múltiples, el momento consumativo expresado en la ley da la nota al delito instantáneo. Existe una lesión y una acción jurídica. El evento consumativo típico se produce en un solo instante, como en el robo art. 367 del Código Penal Federal Vigente.

Instantáneo con Efectos Permanentes.- Es aquel cuya conducta destruye o disminuye el bien jurídico tutelado, en forma instantánea, en un solo momento, pero permanecen las consecuencias nocivas del mismo, como podría ser el caso del acceso ilícito a sistemas y equipos de informática.

Continuado.- En este delito se dan varias acciones y una sola lesión jurídica, es decir es continuado en la conciencia y discontinuo en la ejecución.

Permanente.- Algunos autores encuentran en el delito permanente dos fases. La primera de naturaleza activa, consistente en la realización del hecho previsto por la ley, la segunda, de naturaleza omisiva es el no hacer del agente, con lo que impide la cesación de la comprensión del bien jurídico. Lo que requiere es esencialmente, la facultad, por parte del agente activo, de remover o hacer cesar el estado antijurídico creado con su conducta.

2.4.6 POR EL ELEMENTO INTERNO O CULPABILIDAD

Teniendo como base la culpabilidad, los delitos se clasifican en dolosos, culposos y preterintencionales:

Dolosos, cuando se dirige la voluntad consciente a la realización del hecho típico y antijurídico, como en el robo por nombrar alguno, en donde el sujeto decide apoderarse y se apodera sin derecho del bien mueble ajeno.

Culposos, no se requiere el resultado penalmente tipificado, mas surge por el obrar sin las cautelas y precauciones exigidas por el Estado para asegurar la vida en común y los Preterintencionales, que es cuando el resultado sobrepasa a la intención.

2.4.7 DELITOS SIMPLES Y COMPLEJOS

En función de su estructura o composición, los delitos se clasifican en simples y complejos. Son simples, aquellos en los cuáles la lesión jurídica es única, y son delitos complejos, aquellos en los cuáles la figura jurídica consta de la unificación de dos infracciones, cuya fusión da nacimiento a una figura delictiva nueva, superior en gravedad a las que la componen, tomadas aisladamente.

2.4.8 DELITOS UNISUBSISTENTES Y PLURISUBSISTENTES

Por el número de actos integrantes de la acción típica, los delitos se denominan de dos formas; los llamados unisubsistentes, los cuales se forman por un solo acto; y por otro lado tenemos a los plurisubsistentes, los cuales constan de varios actos.

2.4.9 DELITOS UNISUBJETIVOS Y PLURISUBJETIVOS

Esta clasificación atiende a la unidad o pluralidad de sujetos que intervienen para ejecutar el hecho descrito por el tipo. Por lo tanto se llamaran unisubjetivos los delitos para cuya realización sólo basta la intervención de un solo sujeto, y los plurisubjetivos son aquellos delitos para los cuales se requiere de dos o más sujetos, como por ejemplo la asociación delictuosa, entre otros.

2.4.10 POR LA FORMA DE PERSECUCIÓN

Por esta forma se encuentra los delitos llamados de querella de la parte ofendida y que una vez formulada ésta, la autoridad está obligada a perseguir; y los delitos perseguibles de oficio, que son todos aquellos en que la autoridad está obligada a actuar, por mandato legal, persiguiendo y castigando a los responsables, con independencia de la voluntad de los ofendidos por lo que en estos no se considerará el perdón del ofendido como en los de querella.

2.4.11 DELITOS COMUNES, FEDERALES, OFICIALES, MILITARES Y POLÍTICOS

Esta clasificación es en función de la materia, por lo que daremos un breve significado a cada uno de ellos. Y en ese mismo orden tenemos a los delitos comunes, los cuáles constituyen la regla general, es decir, son aquellos que se formulan en leyes dictados por las legislaturas locales, en cambio los delitos federales se establecen en leyes expedidas por el Congreso de la Unión.

Por otro lado los delitos oficiales, son los que comete un empleado o funcionario público en el ejercicio de sus funciones. Ahora bien, por lo que toca a los delitos militares, la Constitución en su artículo 13 prohíbe a los Tribunales Militares extender su jurisdicción sobre personas que no pertenezcan al ejército, por lo que se concluye que estos delitos afectan la disciplina del ejército, generalmente se incluyen todos los hechos que lesionan la organización del Estado en sí misma o en sus órganos o representantes.

Y por último los delitos políticos los cuáles no han podido ser definidos de manera satisfactoria, pero generalmente se incluyen todos los hechos que lesionan la organización del Estado en sí misma o en sus órganos o representantes.

Ahora bien el artículo 144 del código penal vigente considera delitos de carácter político, a los de rebelión, sedición, motín y el de conspiración para cometerlos. Por lo anterior se puede concluir que el delito político se caracteriza por el dolo específico, es decir, el propósito de parte de quien lo comete y esto es en función de que altera la estructura fundamental del Estado.[41]

[41] Cfr. CASTELLANOS TENA, Fernando., Ob. Cit. pp. 135-146

2.5 CLASIFICACIÓN LEGAL DEL DELITO

2.5.1 INTRODUCCIÓN AL *ITER CRIMINIS*

Así como la clasificación anterior en atención a la doctrina, la siguiente clasificación legal establece el punto de partida de éste trabajo que no es otra cosa que abordar los temas esenciales del título primero referente a la Responsabilidad Penal del Código Penal Federal.

En un orden cronológico, a fin de verificar al delito en dicho ordenamiento, es necesario mencionar que todos lo delitos tienen un desenvolvimiento propio, que se compone de una serie de actos que constituyen las etapas del *proceso* criminoso, al que se le ha llamado *iter criminis;* periodo en el cual sólo puede darse en los delitos donde el sujeto decide, piensa, y resuelve cometer un ilícito, esto es en los delitos intencionales o dolosos.

El *iter criminis* es el camino recorrido por el delito que va desde su ideación en la mente del agente hasta su ejecución, es decir, el delito tiene dos fases: una interna la cuál está compuesta por una idea criminosa, deliberación y resolución del delito, actos no punibles; y la fase externa en la cual encontramos a la comunicación o exteriorización, preparación y ejecución. La primera fase es subjetiva ya que únicamente se desarrolla en el sujeto (el pensamiento delictivo no está penado) y por lo tanto no es importante para nuestro Derecho Penal, en virtud de que éste tipifica únicamente conductas que son hechos externos; es decir, la fase objetiva en donde el hecho puede ser punible cuando el delito se encuentra en su fase externa.[42]

La fase externa comprende:

a) Comunicación o exteriorización; la cual es la manifestación del pensamiento criminoso, "sale del pensamiento interno y se proyecta en el mundo exterior".[43]

Una vez que se exteriorizó el pensamiento, se inicia la preparación del delito. Así, de la resolución de delinquir, continúa la obtención de los medios o búsqueda de las condiciones adecuadas para delinquir, y así tenemos;

b) Preparación; "que es aquella forma de actuar que crea las condiciones previas adecuadas para la realización de un delito planeado".[44]

---

[42] Cfr. LÓPEZ BETANCOURT, Eduardo, *Introducción al Derecho Penal*, Ed. Porrúa, México, 2001 pp. 147-155.

[43] MAGGIORE, Giusseppe, *Derecho Penal*, Tomo II, Ed. Temis, Bogotá, 1989, p. 70

[44] Maurach, Tratado de Derecho Penal, Tomo II, Ed. Ariel, Barcelona, 1972, p. 168.

El acto preparatorio está encauzado a reunir los elementos necesarios para cometer el delito. En esta etapa se puede decir que no hay todavía violación del tipo penal, mas bien son acciones iniciales, que por regla general no son punibles.

c) La ejecución, es la tercera etapa de la fase externa en la cual se contemplan a la tentativa y a la consumación, ahora bien a diferencia de la preparación, la ejecución tiene que iniciar la acción principal descrita en la norma penal, y los actos preparatorios como su nombre lo indica, están encaminados a realizar todas las operaciones necesarias para la ejecución del delito; generalmente el acto preparatorio no afecta derecho de terceros, se desenvuelve únicamente en la esfera del agente, mientras que el acto ejecutorio invade derechos de terceros al adecuarse su conducta a la acción descrita en la norma penal, como delito, al afectar el bien jurídico protegido por dicha norma.

En esta etapa ejecutoria, puede no consumarse el delito (tentativa), o bien, llegar éste a dicha consumación, términos que mas adelante trataremos.

Una vez analizada esta fase externa de manera breve, pasaremos al análisis de nuestro ordenamiento legal referente a la responsabilidad penal.

2.5.2 LA ACCIÓN U OMISIÓN

Sólo la conducta humana tiene relevancia para el Derecho Penal. El acto y la omisión deben corresponder al hombre, porque únicamente es posible ser sujeto activo de las infracciones penales, es decir, es el único ser capaz de voluntariedad.

Como ya mencionamos anteriormente la consumación es la última etapa del iter criminis; implica la realización del delito, es el elemento externo y objetivo. Esto es, una vez que se han ejecutado todos los actos propios y característicos de delito y se ha obtenido el resultado que en conjunto configuran el hecho delictivo, se produce la consumación.

La consumación del delito no es otra cosa que la acción o la omisión plena y totalmente realizada y penalmente castigada, por lo tanto el artículo 7 del Código Penal Federal vigente define en el primer párrafo al delito como "el acto u omisión que sancionan las leyes penales". Esto implica, simplemente, la acción y la omisión, que en ciertos casos bastan, asociados a los demás aspectos positivos, para el perfeccionamiento del delito.

En dicha definición encontramos que el primer elemento es el acto u omisión, es decir, el elemento objetivo del que se manifiesta por medio de la voluntad, ya sea violando una prohibición penal, o absteniéndose de un acto cuya ejecución impone la ley.

El siguiente elemento es que el acto u omisión lo sancionen las leyes penales y por lo mismo, no puede haber delito si no hay una ley previa que califique el hecho relacionado como tal.

Con el fin de concluir con éste tema, se mencionaran a continuación los elementos de la acción y de la omisión.

Elementos de la Acción.

La voluntad constituye el elemento subjetivo de la acción. Petroccelli citado por Pavón Vasconcelos, menciona que "...el denominador común de todas las formas de conducta es el factor psíquico, es decir la voluntad...".[45]

El otro elemento de la acción, es la actividad o movimiento corporal. La actividad en sí no constituye la acción, pues ésta va aunada a la voluntad.
Y por último tenemos al siguiente elemento que así como con relación a los delitos de omisión hay un deber jurídico de obrar, en la acción, existe un deber jurídico de abstenerse de no obrar.

Elementos de la Omisión.

Como primer elemento de la omisión tenemos a la voluntad o culpa, en el entendido de que la omisión consiste en querer no realizar la acción esperada y exigida, es decir, en querer la inactividad, o realizarla culposamente. El siguiente elemento es la inactividad o no hacer, esto en función de que dicha omisión estriba en una abstención o inactividad voluntaria o culposa, violando una norma prohibitiva y finalmente el deber jurídico de obrar, elemento consistente en una acción esperada y exigida en los delitos de omisión simple, debe de estar contenida en una norma penal, es decir, estar tipificada, pues de otra manera su no realización, el no cumplimiento del deber, sería irrelevante penalmente".[46]

Pese a lo anterior, este mismo artículo alude a tres especies de delitos en función de su duración o bien según el tiempo que tarde su consumación, el delito puede ser instantáneo, permanente o continuo lo cual lo consideramos otro tipo de clasificación y detallamos a continuación.

---

[45]- PAVÓN VACSONCELOS, Francisco., Ob. Cit. p. 193.

[46] Ibidem., p. 246.

2.5.3 INSTANTÁNEO

El artículo 7 establece que el delito puede ser:

I. "Instantáneo, es cuando la consumación se agota en el mismo momento en que se han realizado todos sus elementos constitutivos".

En este tipo de delitos, se realiza el hecho delictivo a través de una sola acción que produce en un mismo momento el resultado, es decir, la consumación del delito. Entonces se puede entender a los delitos instantáneos como aquellos en los que su duración concluye en el momento mismo de realizarse o consumarse, por que son actos que en cuanto son ejecutados configuran el delito, sin prolongarse en el tiempo.
Maggiore establece, "el delito seguirá siendo instantáneo, aunque sus efectos dañosos y peligrosos permanezcan después de la consumación"[47] por lo tanto, este criterio enfoca la instantaneidad a la acción que se extingue en un solo momento coincidiendo con la consumación, independientemente de que sus efectos pudieran ser permanentes.

Finalmente, el maestro Porte Petit señala que, "...los requisitos que se desprende del delito instantáneo son: una conducta, una consumación y el agotamiento de la misma de forma instantánea...".[48]

2.5.4 PERMANENTE O CONTINUO

Asimismo, el mismo artículo establece que el delito:

II. "Permanente o continuo, es cuando la consumación se prolonga en el tiempo".

En el delito permanente, la consumación es indefinida, es decir, se prolonga en el tiempo esa acción delictiva, que por las características del delito, el agente puede prolongar voluntariamente en el tiempo; cabe mencionar, que este periodo consumatorio es ininterrumpido, lo cual quiere decir que es un solo momento prolongado en el tiempo, creándose un estado antijurídico duradero de la acción u omisión según se trate la figura delictiva.[49]

---

[47] MAGGIORE, Giusseppe, Ob Cit. p. 295.

[48] PORTE PETIT, Celestino.. Ob. Cit. p.381.

[49] Cfr. LÓPEZ BETANCOURT, Eduardo., Ob. Cit. p. 190.

"En los delitos permanentes, el mantenimiento del estado antijurídico cerrado por la acción punible, depende de la voluntad del autor, de manera que, en cierto modo, el hecho se renueva continuamente".[50] Es decir, la conducta prolongada en el tiempo, debe ser voluntariamente desplegada por el agente.

Ante esta situación el maestro Porte Petit señala que, "los elementos del delito permanente es una conducta o hecho y una consumación mas o menos duradera".[51]Asimismo, precisa que "la consumación duradera comprende los siguientes momentos; un momento inicial, que es la comprensión del bien jurídico protegido por la ley, un periodo intermedio, entre la comprensión del bien hasta antes de la cesación del estado antijurídico y un momento final, que es la cesación del estado antijurídico".[52]

Por lo tanto la característica distintiva del delito permanente es la prolongación de la consumación entre el momento inicial que constituye el contener en el tiempo el bien protegido por la norma, y la cesación del estado antijurídico. El estado delictivo derivado de la conducta voluntaria del agente, no debe terminarse en un instante, sino perdurar algún tiempo sin ser interrumpida, después del hecho que constituye el delito.

2.5.5 CONTINUADO

Por último el ya mencionado artículo describe su última clasificación que a la letra dice:

III. "Continuado, cuando con unidad de propósito delictivo, pluralidad de conductas y unidad de sujeto pasivo, se viola el mismo precepto legal".

Lo anterior no significa que haya pluralidad de delitos, sino de acciones iguales, tendientes a una misma y única resolución; estas acciones deben ser idénticamente violatorias del Derecho.

"El delito continuado se agota cuando una misma persona es responsable de varios hechos que realizan el mismo tipo de delito y cuya determinación y tratamiento procesales individualizados carecen de sentido y resultan imposibles".[53]

---

[50] JESCHECK, HANS Heinrich, *Tratado de Derecho Penal*, Ed. Bla, Tomo I tercera ed. Barcelona 1978 p. 357
[51] PORTE PETIT, Celestino., Ob. Cit. p. 356.
[52] Ibidem., p. 388
[53] CUELLO CALÓN, Eugenio, *Derecho Penal*, Ed. Bosch, Tomo I, cuarta ed, Barcelona, 1937 p. 262.

De acuerdo a lo anterior, para que se presente el delito continuado, son necesarias la homogeneidad de la forma de comisión, el mismo bien jurídico, y la unidad del dolo. La homogeneidad de la forma de la comisión quiere decir que los elementos comisivos deben ser de igual naturaleza, los hechos delictivos deben colmarse en una misma norma jurídico penal, es decir, deben violar la misma disposición legal y el desarrollo de conductas debe ser el mismo en lo esencial como consta en la descripción legal.

Estos actos parciales deben lesionar un mismo bien jurídico, tutelado por la misma ley penal, ya que si lesionara uno de estos actos otro bien jurídico, estaríamos en presencia de otra figura delictiva; y por último al referirnos a la unidad del dolo, se refiere a que la intención del agente debe ser solo una, debe abarcar el resultado total y final de aquellos actos parciales que coinciden en sus elementos comisivos esenciales, en el lugar, en el tiempo, y en la persona a quien se dirige el hecho delictivo, es decir, el agente se coloca en una misma situación de hecho en varios actos, para llegar a un resultado final.[54] Para concretar afirmamos que en el delito continuado son precisas: la unidad del precepto penal violado, la pluralidad de acciones y la unidad de resolución y de propósito.

Atendiendo a la consumación del delito continuado, ésta se forma con un periodo consumativo interrumpido, porque se forma en tiempos distintos, este periodo consumativo comprende desde que se inicia la pluralidad de conductas hasta la última de ellas, es decir, la consumación del delito se prolonga en el tiempo interrumpidamente.

2.5.6 DOLO

De conformidad al artículo 8 del Código Penal Federal, "las acciones y omisiones solamente pueden realizarse dolosa y culposamente". Asimismo el artículo 9 de la multicitada ley, define que "Obra dolosamente el que, conociendo los elementos del tipo penal, o previendo como posible el resultado típico, quiere o acepta la realización del hecho descrito por la Ley..."

Teniendo como base el elemento de la culpabilidad (como ya vimos anteriormente), encontramos al dolo y la culpa por lo que nos ocuparemos del primero en sus diferentes clasificaciones.

[54] Cfr. JESCHECK, HANS Heinrich., Ob. Cit. pp 1000-1002.

El dolo, podemos definirlo como "el conocimiento y voluntad de realizar el tipo objetivo."[55] Hablamos de delito doloso cuando se dirige la voluntad consciente a la realización del hecho típico y antijurídico. El dolo está conformado por dos elementos, el intelectual y el emocional, el primero de ellos consiste en que el sujeto conozca las circunstancias pertenecientes al tipo, es decir, que tenga conocimiento del hecho que realiza, y el segundo consiste en querer o aceptar la realización de dicho hecho. De la tipicidad legal se desprende que el dolo se puede dividir a su vez en dolo directo y dolo eventual, distinguiéndose a su vez el dolo directo de primer grado y dolo directo de segundo grado.

Dolo Directo.

Por dolo directo de primer grado se entiende que es "la forma de actuar, en cuyo caso el elemento volitivo que se presenta de modo más intenso, ya que supone claramente el propósito, intención o finalidad que persigue el agente. En cambio, si el autor del delito tiene que realizar el tipo como medio no deseado (que lamenta o al menos le es indiferente) pero necesario para una ulterior finalidad o propósito, habrá solo dolo directo de segundo grado."[56]

Dolo Eventual.

El análisis de la conducta es un proceso psicológico en que se entremezclan elementos volitivos e intelectuales de manera consciente o inconsciente, de tal suerte que el dolo eventual se ha fijado como la frontera entre el dolo y la culpa. En la actualidad tiende a imponerse el punto de vista en que se estima que deberá apreciarse el dolo eventual si el autor a tomado seriamente en cuenta la posibilidad de la lesión del bien jurídico y se conforma con ella. Si en el dolo directo de segundo grado el autor se representa en el delito como consecuencia inevitable, en el dolo eventual se le aparece como resultado posible.

En conclusión podemos decir que, en el dolo directo, el autor quiere realizar precisamente el resultado (en los delitos de resultado) o quiere la acción típica (en los delitos de actividad), en tanto que, en el dolo eventual el querer del sujeto no está referido directamente al resultado producido por lo que aunque no quiera que surja sigue actuando, admitiendo su eventual realización. En este supuesto el sujeto no quiere el resultado, pero cuenta con él, admite su producción o acepta el riesgo.

---

[55] DE LA CUESTA AGUADO, Paz. *Tipicidad e imputación objetiva*, Ed. Tirant lo Blanch. Valencia. 1996. Cita referida por ZAMORA JIMÉNEZ, Arturo., Ob. Cit. p. 147.

[56] Ibidem., P.150.

2.5.7 CULPA

El mismo artículo 9 en su segundo párrafo contempla a la culpa estableciendo que obra culposamente el que produce el resultado típico, que no previó siendo previsible, o previó confiando en que no se produciá, en virtud de la violación a un deber de cuidado, que debía y podía observar según sus circunstancias y condiciones personales.

Obviamente no podemos dejar a un lado el estudio de los delitos culposos, mismos en los que no se quiere el resultado tipificado, mas éste surge por el obrar sin cautela y precauciones exigidas por el Estado, es decir, el sujeto obra con falta de cuidado o negligencia y en virtud de ello viola una norma penal.

La culpa según la doctrina puede dividirse en culpa consciente o inconsciente. Por culpa consciente entendemos cuando el autor ha representado la posible realización del tipo y ha obrado en la creencia de poder evitarlo, suponiendo que ello ocurrirá. La culpa es inconsciente cuando el autor no representa la posible realización. De aquí que la culpa consciente ofrece problemas para su delimitación frente al dolo eventual.

Si el dolo es el conocimiento y voluntad de la realización del tipo objetivo, en consecuencia, obra con dolo, el que sabe lo que hace y hace lo que quiere, en tanto que, obra culposamente el que sin tener una finalidad determinada respecto de lo resultado lleva a cabo una conducta que infringe el deber de cuidado. Debe quedar claro que el tipo penal de los delitos dolosos contiene básicamente una acción dirigida por el autor a la producción del resultado, en cambio en los delitos culposos contiene una acción que se dirige por el autor al resultado.[57]

Antes de empezar con nuestro siguiente tema que corresponde a la tentativa, es importante mencionar brevemente lo que establece el artículo 10 del Código Penal sobre la responsabilidad penal de los delincuentes y que textualmente dice: "La responsabilidad penal no pasa de la persona y bienes de los delincuentes, excepto en los casos especificados por la ley".

[57] Cfr. ABARCA, Ricardo, *Derecho Penal*, Ed. Jus Tomo I sexta ed. México. 1947 p.506.

Asimismo el artículo 11 contempla lo siguiente: "Cuando algún miembro o representante de una persona jurídica, o de una sociedad, corporación, o empresa de cualquier clase, con excepción de las Instituciones del Estado, cometa un delito con los medios que para tal objeto las mismas entidades le proporcionen, de modo que resulte cometido a nombre o bajo el amparo de la representación social o en beneficio de ella, el juez podrá, en los casos exclusivamente especificados por la ley, decretar en la sentencia la suspensión de la agrupación o su disolución, cuando lo estime necesario para la seguridad pública".

Del propio precepto se desprende claramente que quien comete el delito es un miembro o representante, es decir una persona física, y no la moral. Por otra parte, si varios o todos los socios convienen en ejecutar el delito o intervienen en él en alguna forma, se estará en presencia de un caso de participación o co-delincuencia organizada. Ahora bien las personas morales no pueden delinquir; sin embargo, indiscutiblemente constituyen sujetos pasivos del delito como las personas físicas, en especial tratándose de infracciones penales de tipo patrimonial y contra el honor.[58]

2.5.8 TENTATIVA

Al estudiar la vida del delito, se dijo que el ilícito podía terminar en consumación o en tentativa; la primera se logra cuando el delito se ejecuta plenamente, y la segunda ocurre al existir plena voluntad del sujeto para consumar el delito, y éste no se logra por causas ajenas a su voluntad.

Existen varias definiciones de tentativa para lo cual sólo analizaremos la que nos proporciona Jiménez de Asúa, en los siguientes términos; "Cuando la voluntad criminal se traduce en un caso externo que entra en la esfera de la consumación de delito, sin llegar a llenarla, y va dirigido claramente a conseguir la objetividad jurídica del delito, pero sin llegar a lesionarla, el acto se llama ejecutivo y la figura a la que da lugar se denomina tentativa. Ésta puede definirse sintéticamente como la ejecución incompleta de un delito".[59]

En ese contexto, la tentativa aparece cuando el sujeto ha realizado todos los actos encaminados para la consumación del delito, y éste no se presenta por causas ajenas a su voluntad.

---

[58] Cfr. CASTELLANOS TENA, Fernando., Ob. Cit. p.151.
[59] JIMÉNEZ DE ASÚA, Luis, *La Ley y el Delito*, Ed. Hermes, México, 1986, p. 474.

La tentativa tiene un inicio, un comienzo en la ejecución, donde se utilizan los actos idóneos; pero en el transcurso de los actos necesarios o al final de los mismos, el resultado deseado no llega a presentarse.

La naturaleza de ésta figura se encuentra íntimamente ligada con los aspectos punitivos; esto es, tanto en el delito consumado como en la tentativa tiene que darse un dolo plenamente, pero su diferencia estriba en que en un caso, cuando se consuma el ilícito, la transgresión a la norma se dio en toda su forma; en cambio, en la tentativa, su punición será menor que en el delito consumado. Por lo tanto, la tentativa es de naturaleza imperfecta, si se compara con el delito consumado.

Maggiore establece tres elementos de la tentativa y son: "la intención dirigida a cometer un delito, un acto idóneo, y una acción no realizada o un resultado no verificado".[60]

Analizando estos elementos, encontramos que, la intención dirigida a cometer un delito es indispensable, por que al no haber intención delictuosa tampoco puede existir la tentativa, dicha intención por lo tanto no acepta interpretaciones, es inequívoca.

Para que exista la tentativa, tiene que darse por lo menos un acto idóneo, éste acto puede ser de cualquier naturaleza, lo cual resulta indispensable ya que la idoneidad debe concretarse, es decir, ser capaz de producir el resultado que se ha propuesto el activo, sin que lo pueda conseguir por causas ajenas a su voluntad. Por último el tercer elemento, nos permite ver con claridad que el acto delictivo estuvo incompleto.

El Código Penal en su artículo 12, regula a la tentativa en los siguientes términos:

"Existe tentativa punible, cuando la resolución de cometer un delito se exterioriza realizando en parte o totalmente los actos ejecutivos que deberían producir el resultado, u omitiendo los que deberían evitarlo, si aquél no se consuma por causas ajenas a la voluntad del agente.

Para imponer la pena de la tentativa el juez tomará en cuenta, además de lo previsto en el artículo 52, el mayor o menor grado de aproximación al momento consumativo del delito.

[60] MAGGIORE, Giuseppe, Ob. Cit. pp. 77-82.

Si el sujeto desiste espontáneamente de la ejecución o impide la consumación del delito, no se impondrá pena o medida de seguridad alguna por lo que a éste se refiere, sin perjuicio de aplicar la que corresponda a actos ejecutados u omitidos que constituyan por sí mismos delitos".

Del análisis de dicho artículo, observamos que son elementos básicos y esenciales de la tentativa; la resolución delictiva, y el principio de la ejecución. La resolución delictiva es un elemento subjetivo, íntimamente relacionado con la decisión tomada por el sujeto activo. El principio de ejecución, sin lugar a dudas es un elemento objetivo, comprobable y de evidente existencia.

Existen dos clases de tentativa, que son: la tentativa acabada y la tentativa inacabada; en la primera, la ejecución que realiza el sujeto activo es completa ya que va encaminada a un resultado delictivo, pero éste no acontece por causas ajenas a su voluntad, y la segunda consiste en la omisión del sujeto de uno o varios actos tendientes a la verificación del delito. En este caso, la ejecución es incompleta, por lo que el resultado como consecuencia de tal omisión no se produce.

Nuestro Código Penal vigente, para evitarse el conflicto, de explicar la tentativa acabada e inacabada, sólo señala la existencia de tentativas punibles; pero al hablar de la no consumación por causas ajenas a la voluntad del agente, está dando pauta y reconociendo la existencia de ambas formas de tentativa.[61]

2.5.9 SUJETOS

Existen diversas formas de intervención y cada una de ellas recibe un tratamiento especial, todo depende del modo en que cada sujeto participa en la comisión del hecho delictuoso.

En nuestra Ley Penal no se habla de autoría y participación en sentido literal, es por eso que enuncia las figuras delictivas en las ocho fracciones del artículo 13 del Código Penal, determinando que estos serán los responsables del delito.

[61] Cfr. LÓPEZ BETANCOURT, Eduardo., Ob. Cit. pp.166-172.

"Son autores o partícipes de delito:

I. Los que acuerden o preparen su realización

II. Los que lo realicen por sí

III. Los que lo realicen conjuntamente

IV. Los que lo lleven a cabo sirviéndose de otro

V. Los que determinen dolosamente a otro a cometerlo

VI. Los que dolosamente presten ayuda o auxilien a otro para su comisión

VII. Los que con posterioridad a su ejecución auxilien al delincuente, en cumplimiento de una promesa anterior al delito, y

VIII. Los que sin acuerdo previo, intervengan con otros en su comisión, cuando no se pueda precisar el resultado que cada quien produjo".

Cabe mencionar que dicho artículo en comento, fue reformado en 1984 y 1994; y con estas reformas se dio mayor precisión en cuanto a los sujetos, cuya conducta produce la violación de la norma penal; esto es importante, sobre todo para la aplicación correcta de las penas.

Al considerar dicho artículo, vamos hacer referencia a la intervención de cada una de las figuras de autoría y participación en el hecho delictivo y son:

Autor Material.
Para Abarca, el autor material es "el que por sí mismo ejecuta los actos externos descritos por la ley como elemento del delito".[62] Y en relación con esta expresión vemos que se encuentra contemplado en la fracción II, pues al definir "los que lo realicen por sí", quiere decir que son los sujetos que de manera directa y materialmente lo ejecutan.

Como podemos ver ésta figura concurrente al hecho delictivo no tiene mayor problema, ni provoca confusión alguna, en virtud de que siempre será el que realice la conducta típica, es decir es una figura principal y tradicional, de la que parten las demás modalidades. Dicha autoría puede darse por acción u omisión (positiva o negativamente), de un hacer respectivamente, según requiera la norma jurídico penal.

[62] ABARCA, Ricardo, *El Derecho Penal en México*. Ed. Jus, primera ed. México, 1989 p.159.

Coautor.
Son coautores, "los que lo realizan conjuntamente y de mutuo acuerdo un hecho delictivo".[63]

En la fracción III al establecer "Los que lo realicen conjuntamente", hace referencia a la coautoría; al ser ésta una forma de participación en el delito, el coautor es quien en unión de otro u otros autores responsables, ejecutan el delito, realizando conductas señaladas en la descripción penal, por lo que todos los coautores son punibles.

Autor Mediato.
El autor mediato no realiza el hecho delictivo directa ni personalmente, acude a otra persona extraña que utiliza como instrumento para su realización. La fracción IV del artículo 13, alude al autor mediato al referirse a los que son responsables del delito, preceptúa: "Los que lo lleven a cabo sirviéndose de otro".

El autor mediato tiene el control del hecho y utiliza como instrumento a otro individuo, quien no realiza ninguna conducta típica ni culpable; puede darse el caso que el autor mediato se valga del error esencial de hecho, en que se encuentre el sujeto que será utilizado como instrumento para la comisión del delito; en este caso, el sujeto al realizar la conducta ignora lo que hace. De esta manera, el sujeto que aparece con el autor mediato no puede actuar para impedir la ejecución del hecho delictivo; así el autor mediato mantendrá el control de la ejecución del delito.[64]

Autor Intelectual.
El autor intelectual se consigna en la fracción V de nuestro artículo 13, al decir que son responsables del delito: "Los que determinen dolosamente a otro a cometerlo."

En efecto, el autor intelectual es el que prepara la realización del delito; cuando al proyectarlo provoca o induce a otro a la ejecución de un delito, se convierte en instigador.

La instigación requiere de dos sujetos, uno que provoca o induce a otro a la ejecución del delito, que será el autor intelectual; y una persona que ejecute materialmente el delito, que será el autor material.

[63] JESCHECK, HANS Heinrich., Ob. Cit. p. 941.
[64] LÓPEZ BETANCOURT, Eduardo., Ob. Cit. pp. 211-212.

El autor intelectual va a provocar que otro realice la comisión del ilícito penal mediante inducción, que no es sino el influjo que lleva a efecto una persona intencionalmente sobre otro, para que cometa un hecho delictivo. Es importante distinguir el elemento intencional, el autor intelectual debe tener conocimiento de las circunstancias y del hecho delictivo al que induce.

A diferencia del autor mediato, el instigador no utiliza a otro para cometer el delito, sino que lo convence para que realice el hecho delictivo, lo induce a la comisión del delito.[65]

Cómplice.
Nuestro Código Penal en su artículo 13 fracción VI señala al cómplice como "Los que dolosamente presten ayuda o auxilien a otro para su comisión". Este precepto no habla de los medios que deberá emplear el cómplice cuando preste ayuda o auxilio; dadas esas circunstancias, se dice que el cómplice es el que realiza acciones secundarias encaminadas a la realización del hecho delictivo; puede participar moralmente, instruyendo al autor material, indicándole la forma en que debe ejecutar el delito, ofreciendo su ayuda para su interpretación, o impunidad.

Por lo tanto no hay que confundir la coautoría con la complicidad; ya que la primera se presenta cuando varios sujetos intervienen en la realización del hecho delictuoso, y cada uno de ellos reúne la calidad de autor para los efectos del delito, ya sea que cada uno realice la totalidad de los hechos o una parte de ellos. En el cómplice se presenta la intención de ayudar, auxiliando para que el otro cometa el delito. El coautor tiene el dominio del hecho lo que no sucede con el cómplice.

Encubrimiento.
En nuestra legislación penal, el encubrimiento tiene una doble vertiente; como forma de participación, y como delito autónomo, tal como lo establece la fracción VII del artículo 13, cuando dice que son responsables del delito "Los que con posterioridad a su ejecución auxilien al delincuente, en cumplimiento de una promesa anterior al delito".

Será en forma de participación, cuando el encubridor, antes de cometer el ilícito, tiene pleno conocimiento y está de acuerdo en guardar al autor material una vez que éste cometa su ilícito.

[65] Cfr. Ibidem. P. 210.

Como delito autónomo, el encubridor se presentará cuando se ignore lo referente a la realización del hecho delictivo y una vez que éste ha pasado, se oculte al delincuente.[46]

Causas de Exclusión del Delito.
Con relación a lo anterior concluimos que, para que se pueda dar una acción u omisión ya sea como autores o partícipes es necesario que exista una conducta, por lo que entonces nos preguntaremos ¿cuándo hay una ausencia de conducta?. La respuesta es lógica, cuando la acción u omisión, o bien, cuando el movimiento corporal o la inactividad no pueden atribuirse al sujeto por faltar en ellos la voluntad.

Lo cual trae como consecuencia una excluyente del delito, tal como lo menciona el artículo 15 fracción I del mismo ordenamiento que a la letra dice:

El delito se excluye cuando:

I. "El hecho se realice sin intervención de la voluntad del agente".

Los casos en que se puede dar una ausencia de conducta son los siguientes:

Fuerza irresistible
Fuerza mayor
Movimientos Reflejos
Movimientos Fisiológicos
Movimientos Automáticos
Sonambulismo
Hipnotismo
Sueño

Como se puede apreciar no es necesario que la legislación positiva enumere todas las excluyentes por falta de conducta; cualquier causa capaz de eliminar ese elemento básico del delito, será suficiente para impedir la formación de éste.

[46] Cfr. Ibidem. P. 216.

CAPÍTULO III

DELITOS INFORMÁTICOS

3.1 INTRODUCCIÓN A LOS DELITOS INFORMÁTICOS

En la actualidad a través del Internet se están dando conductas que están extralimitando los modos tradicionales en la Comisión de Delitos revelándose así nuevas formas de ejecución. El objetivo de este capítulo es analizar, las conductas delictivas que puede generar el gran avance tecnológico, sobre todo en el campo de la informática.

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo que está abriendo la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

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

3.2 TERMINOLOGÍA DE LOS DELITOS INFORMÁTICOS

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, para indicar las conductas ilícitas en las que se usa la computadora, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas. Por lo que es necesario, en base a lo anterior, y para mayor abundamiento acerca del tema, establecer de manera muy breve las principales definiciones que la doctrina nos ha proporcionado, sobre que es, lo que debemos entender por delito informático, encontrándonos con la siguiente terminología.

3.2.1 DELINCUENCIA INFORMÁTICA

La define Gómez Perals como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

3.2.2 CRIMINALIDAD INFORMÁTICA

Baón Ramírez define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).

Tiedemann considera que con la expresión *criminalidad* mediante computadoras, se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos.

3.2.3 COMPUTER CRIMEN

En el ámbito anglosajón se ha popularizado la denominación de "*Computer Crime*" y en el germano la expresión "*Computerkriminalität*"

Para Carlos Sarzana, en su obra *Criminalità* e tecnología, los crímenes por computadora comprenden cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo.

3.2.4 DELINCUENCIA DE CUELLO BLANCO

La doctrina, casi unánimemente, la considera inscribible en la criminalidad de cuello blanco.

Para Sutherland la delincuencia de cuello blanco es la violación de la ley penal por una persona de alto nivel socio-económico en el desarrollo de su actividad profesional.[67]

3.2.5 ABUSO INFORMÁTICO

Ruiz Vadillo recoge la definición que adopta el Consejo de Europa indicando que abuso informático es todo comportamiento ilegal o contrario a la ética o no autorizado, que concierne a un tratamiento automático de datos y/o transmisión de datos.

[67] http://tiny.uasnet.mx/prof/cln/der/silvia/inducc.htm

La misma definición aporta Correa incidiendo en la Recomendación (89) 9, del Comité de Ministros del Consejo de Europa considerando que la delincuencia informática suele tener carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es necesario llevar a cabo una armonización más intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el ordenador.[68]

3.2.6 DELITO ELECTRÓNICO

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 computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin:

Como método, se encuentran las conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como medio, tenemos a las conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

Como fin, son aquellas conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla".[69]

3.2.7 DELITOS INFORMÁTICOS

Romero Casabona se refiere a la definición propuesta por el Departamento de Justicia Norteamericana, según la cual Delito Informático "es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución".[70]

---

[68] Cfr. CORREA, Carlos, Derecho Informático, Ed. Depalma, Buenos Aires, 1987 p. 86.

[69] LIMA DE LA LUZ, María, Delitos Electrónicos Revista Criminalia, Ed. Porrúa Academia Mericana de Ciencias Penales México D. F No. 1-6 año I., enero-junio 1984 P. 100.

[70] ROMERO Casabona, Poder Informático, Ed. Tecnos, Madrid, 1994 p. 43

Para Davara Rodríguez define el Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Parker define los delitos informáticos como todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la víctima pudiera sufrir una pérdida; y cuyo autor puede obtener un beneficio.[71]

Julio Téllez Valdéz 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".[72]

Antonio Pérez Luñó dice "Es aquél conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan al funcionamiento de los sistemas informáticos".[73]

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".[74]

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 primero de la Constitución Española".[75]

3.3 CONCEPTO DE DELITO INFORMÁTICO

[71] Cfr. HANCE, Oliver, leyes y Negocios en Internet, Ed. Mc Gras Hill, México, 1986 p.56.
[72] TÉLLEZ VALDÉZ., Ob Cit. P. 103.

[73] PÉREZ LUÑÓ, Antonio Enrique, Ensayos de Informática Jurídica Fontamara-ITAM, Colección Biblioteca de Ética, Filosofía del Derecho y Política No. 46 México, 1996. p. 17.
[74] CALLEGARI, Lidia, Delitos Informáticos y Legislación Revista Facultad de Derecho y Ciencias Políticas Universidad Pontificia Bolivíana Medellín, Colombia. No. 70 julio-agosto-sep. 1985 p.115.

[75] http://www.cfl.gob.mx/html/5_est

El delito informático implica actividades que se han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Por lo que 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.

El término Delito Informático resulta especialmente problemático y ello a pesar de que es utilizado por bastantes autores de la materia dada su plasticidad.

Esta heterogeneidad de supuestos agrupados bajo la rubrica del delito informático para hacer referencia a hipótesis que, en muchas ocasiones, no son delitos en sentido estricto, ha provocado que en algunas culturas jurídicas se opte por una denominación más genérica y apropiada sobre la *criminalidad informática*.[76]

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.

Una vez analizado de manera previa el concepto de Delito Informático, se hace importante revisar los elementos que intervienen en los dichos delitos en un ámbito conductual, para que de esa manera se pueda observar el modo de operar de estos ilícitos.

3.4 ELEMENTOS QUE INTERVIENEN EN LOS DELITOS INFORMÁTICOS

[76] http://tiny.uasnet.mx/prof/cln/der/silvia/define.htm

Para que exista un delito necesariamente deben existir los presupuestos de este, es decir, "toda circunstancia, antecedente indispensable para que el delito exista",[77] entre esta circunstancia encontramos; la norma penal, dentro de la cual comprendemos el precepto y la sanción, que en nuestro caso se busca en su integración adecuada a la realidad tecnológica; la imputabilidad como la capacidad de valoración del deber y de obrar en base a ese deber, el bien jurídicamente tutelado que lo encontramos en la información como patrimonio, equipo electrónico y telecomunicaciones; el instrumento del delito que puede ser el equipo de electrónico, el software, computadoras, las mismas telecomunicaciones, los discos de almacenamiento no fijos, así como también los sujetos activo y pasivo.

3.4.1 SUJETO ACTIVO

De acuerdo con el tratadista Francisco Pavón; "Solo el hombre puede ser el sujeto activo del delito por que únicamente el se encuentra provisto de capacidad y voluntad, y puede con su acción u omisión, infringir el ordenamiento jurídico penal. Se dice que una persona es el sujeto activo cuando realiza la conducta o el hecho típico, antijurídico, culpable y punible".[78] Por esta razón se considera que los sujetos activos de los delitos informáticos, son aquellas personas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

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

[77] PORTE PETIT, Celestino.. Ob. Cit. P. 133.
[78] PAVÓN VASCONCELOS, Francisco. Ob. Cit. P.143.

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

Contrario a la mayoría de delitos que se encuentran tipificados en las Leyes Penales de diversos países del mundo, el perfil del delincuente informático posee cierta configuración y virtudes que lo hacen único dentro de este enfoque, todo ello en razón de las características siguientes:

Hasta cierto grado, se han descubierto una serie de patrones que van desde la apariencia hasta sus ámbitos de lectura. Es el sujeto típico inteligente, abstraído y apasionado por la informática y la computación.

Su conducta delictiva no tiene un alto grado de peligrosidad, como si lo hay en los delitos donde existe una violencia física o moral, ya que un delincuente informático al realizar la comisión de un delito, no utiliza la violencia. Su personalidad es original y única, es decir, poseen un inteligencia superior a la normal, y además tienen una gran preparación especial en la materia de informática.

Poseen una imaginación extraordinaria, compleja y muy exuberante, es decir, son muy audaces y aventureros. Son personas que generalmente no tienen antecedentes penales, y que llevan una vida laboral estable. La gran mayoría de ellos son personas de un nivel económico muy elevado.

Es difícil elaborar estadísticas sobre este tipo de delitos. La "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad.

Estas aseveraciones pueden y deben ser objeto de un estudio más profundo, que dada la naturaleza de nuestro objeto de estudio nos vemos en la necesidad de limitar.[79]

[79] http://finy.uasnet.mx/prof/cln/der/silvio/activo.htm

3.4.2 SUJETO PASIVO

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

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

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada *cifra oculta* o *cifra negra*.[80]

[80] http://iny.uasnet.mx/prof/cln/der/silvia/pasivo.htm

3.5 CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS

Según TELLEZ VALDEZ, este tipo de acciones presentan las siguientes características principales:

a) Son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas. A esto habría que agregar que pocos son los llegan a obtener dichos conocimientos, convirtiéndose en un elemento de una comunidad reducida, alejada claro está, de los individuos con bajo poder adquisitivo.

b) Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se encuentra trabajando, sin embargo, tal acierto no puede ser tomado como absoluto, ya que actualmente en México existe una densidad en cuánto al número de usuarios de Internet de los rubros como son: el hogar, los negocios, educación, gobierno, entre otros y es por eso que muchas veces el hogar tiene una presencia de suma importancia, la cual debe ser tomada en cuenta como preponderante ya que permite una clandestinidad en el actuar, que la mayoría de las veces no sería posible en una fuente de trabajo, y esto aunado al hecho de que en el hogar la disposición del tiempo para navegar dentro del Internet es mucho mayor, por lo que podría pensarse entonces de que si bien es una acción ocupacional no se podría especificar el momento de operar (trabajando), si no que son acciones que se actualizan en la clandestinidad del lugar donde se encuentra el equipo conectado en la red.

c) Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico, efectivamente la conducta delictiva la encontramos en el momento idóneo que busca el delincuente informático para poder de esta manera tener acceso ilícito a la información de terceros; pero el acceso no sólo se da en un ámbito económico, sino también privado, social, político y cultural.

d) Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan, dichas pérdidas pueden ser de carácter pecuniario o moral y no solamente económico, como lo es en el caso de los Derechos de Autor.

e) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse, los adelantos tecnológicos en el mundo de la telemática permite que cada día surjan equipos de cómputo con una velocidad mayor de respuesta en el acceso a las telecomunicaciones. así mismo las redes se implementan con avances como la fibra óptica, o la tecnología celular, esto permite que la conducta delictiva se ejecute en periodos de tiempo extraordinariamente cortos, lo que por consecuencia hace difícil su persecución.

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho, lo que lleva a que el gobernado al recurrir ante el órgano persecutor del ilícito, se encuentre con que no existe la conducta como un delito, y por ende no es posible perseguirla como tal.

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, esta posición no concuerda con tal extremo, ya que el conocimiento en Internet y lo amplios conocimientos en informática de quien lo utilice, hace difícil que el usuario no se de cuenta de que esta cometiendo un acto que necesariamente perjudicara a un tercero, pero la culpa no puede descartarse, puesto que muchas conductas se generan sin pensar en la consecuencia.

j) Ofrecen facilidades para su comisión a los menores de edad, ya que para el acceso a Internet solo es necesario que la computadora se encuentre conectada a la red, y con la clave de acceso se puede ingresar al basto mundo del ciberespacio. cuestión de suma facilidad para un menor que sepa escribir, y de nada servirá que se instalen restricciones de acceso a determinados sitios de la red. pues estos pueden ser manipulados.

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. la técnica siempre es un arma y cada avance es explotado criminalmente, en forma tal, que el criminal está más tecnificado que la prevención del crimen.

l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la Ley.[81]

[81] Cfr. TÉLLEZ VALDÉZ, Julio, Ob. Cit. pp. 104-105.

Haciendo un análisis concreto de las características que acabo de enunciar, es importante señalar que se debe de actuar de la manera más eficaz para evitar este tipo de delitos y que no se sigan cometiendo con tanta impunidad, se debe de legislar de una manera seria y honesta, recurriendo a las diferentes personalidades que tiene el conocimiento, tanto técnico en materia de computación, como en lo legal (el Derecho), ya que si no se conoce de la materia, difícilmente se podrán aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular.

3.6 CLASIFICACIÓN DE DELITOS INFORMÁTICOS

La red Internet nos permite dar algunas clasificaciones según las actividades o conductas con las que operan los sujetos para la comisión de otro tipo de delitos.

3.6.1 CLASIFICACIÓN SEGÚN ACTIVIDADES DELICTIVAS GRAVES

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

-Narcotráfico. Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas. Tanto el FBI como el Fiscal General de los Estados Unidos han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles.

-Espionaje. Se han dado casos de acceso no autorizado a sistemas informáticos gubernamentales e intercepción de correo electrónico del servicio secreto de los Estados Unidos, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera. Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

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

3.6.2 CLASIFICACIÓN SEGÚN LA ACTIVIDAD INFORMÁTICA

Sabotaje informático.

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección. Básicamente, se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

Conductas dirigidas a causar daños físicos.

El primer grupo comprende todo tipo de conductas destinadas a la destrucción «física» del hardware y el software de un sistema (por ejemplo, causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc). En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

Conductas dirigidas a causar daños lógicos.

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

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

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

-*Bombas lógicas (time bombs)*. En esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (por ejemplo a los dos meses o en una fecha o a una hora determinada), o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar actuar.

Por ejemplo la jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa.

-Cáncer de rutinas (cancerroutine). Otra modalidad que actúa sobre los programas de aplicaciones. En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos.

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

Fraude a través de computadoras.

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

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

-Estafas electrónicas. La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el *animus defraudandi* existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

-Pesca u Olfateo de claves secretas. Los delincuentes suelen engañar a los usuarios nuevos e incautos de la Internet para que revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio. Los «sabuesos» utilizan programas para identificar claves de usuarios, que más tarde se pueden usar para esconder su verdadera identidad y cometer otras fechorías, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

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

-Juegos de azar. El juego electrónico de azar se ha incrementado a medida que el comercio brinda facilidades de crédito y transferencia de fondos en la Red. Los problemas ocurren en países donde ese juego es un delito o las autoridades nacionales exigen licencias. Además, no se puede garantizar un juego limpio, dadas las inconveniencias técnicas y jurisdiccionales que entraña su supervisión.

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

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

-Copia ilegal de software y espionaje informático. Se engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información. Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apoderamiento es el mismo programa de computación (software) que suele tener un importante valor económico.

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

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

-Uso ilegítimo de sistemas informáticos ajenos. Esta modalidad consiste en la utilización sin autorización de los ordenadores y los programas de un sistema informático ajeno. Este tipo de conductas es comúnmente cometida por empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias a su trabajo. En estos supuestos, sólo se produce un perjuicio económico importante para las empresas en los casos de abuso en el ámbito del teleproceso o en los casos en que las empresas deben pagar alquiler por el tiempo de uso del sistema.

-Interceptación de e-mail. Lectura de un mensaje electrónico ajeno.

-Acceso no autorizado. La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.[82]

3.6.3 CLASIFICACIÓN SEGÚN EL INSTRUMENTO, MEDIO O FIN U OBJETIVO

En todo delito de los llamados informáticos, hay que distinguir el medio y el fin. Para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática y la telemática, y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito; una finalidad deseada que causa un perjuicio a otro, o a un tercero, y así tenemos:

De esta manera, el autor mexicano Julio Téllez Valdez clasifica a estos delitos, de acuerdo a dos criterios.

[82] http://www.monografias.com/trabajos/legisdelint/legisdelint.shtml

1.-Como instrumento o medio.

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

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

-Variación de los activos y pasivos en la situación contable de las empresas.

-Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)

-Lectura, sustracción o copiado de información confidencial.

-Modificación de datos tanto en la entrada como en la salida.

-Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

-Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

-Uso no autorizado de programas de cómputo.

-Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

-Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

-Obtención de información residual impresa en papel luego de la ejecución de trabajos.

-Acceso a áreas informatizadas en forma no autorizada.

-Intervención en las líneas de comunicación de datos o teleproceso.

2.-Como fin u objetivo.

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

-Programación de instrucciones que producen un bloqueo total al sistema.

-Destrucción de programas por cualquier método.

-Daño a la memoria.

-Atentado físico contra la máquina o sus accesorios.

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

-Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc).[83]

[83] Cfr. TÉLLEZ VALDÉZ, Julio., Ob. Cit. pp.105-106.

3.7 SITUACIÓN INTERNACIONAL Y ORGANIZACIONES

3.7.1 LEGISLACIÓN EN OTROS PAÍSES

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

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

Son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España y Chile.

Alemania.

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

Espionaje de datos (Art.202)

Estafa Informática (Art. 263)

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

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

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

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

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

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

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

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

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

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

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

Austria.

La Ley de reforma del Código Penal de 22 de diciembre de 1987 promulgada en dicho país; contempla los siguientes delitos:

Destrucción de datos (Art.126), en este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

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

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

Francia.

La Ley francesa número 88-19 de 5 de enero de 1988 relativa al fraude informático.

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

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

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

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

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

Estados Unidos.

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

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

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

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

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

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

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita, a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

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.

En Estados Unidos ya florecen los investigadores privados que han sustituido el arma de fuego por el arma electrónica y que, en vez de "pies planos", empiezan a ser denominados "colas planas", pues casi toda la investigación la realizan a través de Internet, cómodamente sentados frente a su computadora.[64]

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.

[64] http://tiny.dasnet.mx/prof/cm

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.

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 intención dolosa y cuando el hecho es cometido por parte de 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.

La Guardia Civil Española es pionera en la investigación de delitos informáticos tendientes a su prevención. Allí, los guardia civiles virtuales se encuentran con colegas de similares departamentos de las mejores policías del mundo tales como La Scotland Yard Británica, el FBI norteamericano, la Policía Francesa o los herederos del KGB soviético, y otros agentes undercover de los servicios secretos de las potencias.[85]

[85] http://www.kriptopolis.com

Chile.

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

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

Esta ley prevé en el Art. 1°, el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta 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.

Argentina.

Aunque no existe legislación especifica sobre los llamados delitos informáticos y 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 por el Decreto N° 165/94 del 8 de febrero de 1994; es importante mencionar los proyectos de ley de los Senadores nacionales Eduardo Bauza y Antonio Berhongaray.

Como punto de partida se encuentra el contenido de dicho Decreto en el que se define como obras de software las producciones que se ajusten a las siguientes definiciones:

Los diseños, tanto generales como detallados, del flujo lógico de los datos en un sistema de computación.

Los programas de computadoras, tanto en versión "fuente", principalmente destinada al lector humano, como en su versión "objeto", destinada a ser ejecutada por la computadora.

La documentación técnica, con fines tales como explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento de software.

En segundo lugar se encuentran las obras de base de datos las cuales se incluyen 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.[85]

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 que son los presentados por los Senadores Eduardo Bauza y Antonio Berhongaray, respectivamente.

A) Proyecto de Ley Penal y de Protección de la Informática (Senador Eduardo Bauza).

El Senador Eduardo Bauza, señala en el artículo 24 de su proyecto, que la alteración, daño o destrucción de datos en una computadora, base de datos o sistema de redes, se realiza exclusivamente mediante el uso de virus u otros programas destinados a tal modalidad delictiva, y aunque existen otros medios de comisión del delito, estos no fueron incorporados al tipo legal por el legislador.

En cuanto al tipo penal de violación de secretos y divulgación indebida se circunscribe al correo electrónico, dejando de lado la figura de la información obtenida de cualquier computadora o sistema de redes. Asimismo, el Senador Bauza, incluye la apología del delito y agrava la conducta en caso de ilícitos de atentados contra la Seguridad de la Nación.

En materia de los accesos no autorizados, el proyecto Bauzá, en el artículo 20 prevé, para que se configure el tipo penal, que la conducta vulnere la confianza depositada en él por un tercero (ingreso indebido), o mediante maquinaciones maliciosas (dolo) que ingresare a un sistema o computadora utilizando un *password* ajeno. Asimismo, este artículo, por su parte, prevé el agravante para aquellos profesionales de la informática.

En materia de uso indebido, este Proyecto en su Artículo 21, incluye en el tipo legal a aquel que vulnerando la confianza depositada en él por un tercero (abuso de confianza), o bien por maquinaciones maliciosas (conducta dolosa), ingresare a un sistema o computadora utilizando un *password* ajeno, con la finalidad de apoderarse, usar o conocer indebidamente la información contenida en un sistema informático ajeno (no incluye la revelación).

[86] www.argentinajuridica.com

En tanto en el artículo 38 pena a toda persona física o jurídica, de carácter privado, que manipule datos de un tercero con el fin de obtener su perfil, etc. y vulnere el honor y la intimidad personal o familiar del mismo.

En materia de Sabotaje y daños, este Proyecto, en el artículo 23, prevé prisión de uno a tres años para aquél que en forma maliciosa, destruya o inutilice una computadora o sistema de redes o sus partes, o impida, obstaculice o modifique su funcionamiento. Se agrava la pena en caso de afectarse los datos contenidos en la computadora o en el sistema de redes.

Se resalta que el tipo legal propuesto requiere malicia en el actuar. El artículo 24 también incluye malicia (en el actuar) para alterar, dañar o destruir los datos contenidos en una computadora, base de datos, o sistemas de redes, con o si salida externa. El medio utilizado, segun la propuesta, es mediante el uso de virus u otros programas destinados a tal modalidad delictiva.

En cuanto a la Intercepción ilegal/apoderamiento, este proyecto aplica penas de prisión.

En materia de Violación de secretos (Espionaje/Divulgación), este Proyecto propone gradualismo en la aplicación de la pena, agravamiento por cargo e inhabilitación para funcionarios públicos. Además, impone multas por divulgación.

En lo relacionado con Estafa y defraudación, este Proyecto reprime con pena de prisión al responsable de una estafa mediante el uso de una computadora.

B) Proyecto de Ley Régimen Penal del Uso Indebido de la Computación (Senador Antonio Berhongaray).

Este Proyecto de Ley, es abarcativo de muchas conductas delictivas, agravando especialmente la pena, cuando la destrucción fuera cometida contra datos pertenecientes a organismos de defensa nacional, seguridad interior o Inteligencia (Art. 3° inc. 2), contemplando especificamente el espionaje.

En cuanto a la Violación de secretos (espionaje/divulgación), el Proyecto Berhongaray, penaliza las violaciones a la defensa nacional, a la seguridad interior y agravado por el resultado si ocurre un conflicto internacional. Además contempla el agravante por espionaje. También pena la imprudencia, negligencia, impericia o inobservancia de los reglamentos en la comisión de delitos por parte de terceros.

El Proyecto del Senador Berhongaray, en su artículo 2, requiere el acceso a una computadora o sistema de computación, o almacenamiento de datos que no le pertenezcan directamente o a través de otra computadora, sin autorización del propietario o de un tercero facultado para otorgarla o si estando autorizado, excediere los límites de la misma. Basta para que se configure el tipo legal el ingreso sin autorización o teniéndola, que se exceda del marco de la misma.

En materia de Sabotajes y daños, Berhongaray, introduce agravamiento cuando se afecte a organismos de la defensa nacional, seguridad interior e Inteligencia, coinciden en aplicar penas de prisión para este tipo de delitos.

En el artículo 5, pena a quien a través del acceso no autorizado, o de cualquier otro modo, voluntariamente y por cualquier medio, destruyere, alterare en cualquier forma, hiciere inutilizables o inaccesibles o produjera o diera lugar a la pérdida de datos informáticos. Aclara qué se entiende por acción voluntaria, expresando que es aquello que hubiera consistido en la introducción de programas de computación aptos para destruir, alterar, hacer inutilizables o inaccesibles los datos, de cuya acción proviniera el daño, ya fuera por computadora o sistema de computación en lo que se hallaban los datos dañados, o en cualquier otro.

El artículo 6, pena la destrucción o inutilización intencional de los equipos de computación donde se encontraban los datos afectados. Agravando la pena, cuando la destrucción, alteración o pérdida de datos trajera aparejadas pérdidas económicas; o cuando fuera cometida contra datos pertenecientes a organismos de defensa nacional, seguridad interior o inteligencia.

Referente a usos indebidos, en el artículo 11, se propone como tipo legal el acceso no autorizado y el uso indebido, incorporando un móvil que es la ventaja económica.

Finalmente, cabe destacar que en materia de los accesos no autorizados, los Proyectos Bauza y Berhongaray, son coincidentes en cuanto a la aplicación de solamente penas de prisión con agravantes por los accesos no autorizados. En tanto, en lo relacionado con la Interceptación ilegal/apoderamiento, estos proyectos, coinciden en aplicar penas de prisión.[87]

[87] http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml

3.7.2 ORGANIZACIONES EN MATERIA DE PREVENCIÓN DE DELITOS INFORMÁTICOS

En distintas latitudes del globo terráqueo se pueden encontrar distintas organizaciones que buscan la reducción de los Delitos Informáticos, debido al gran auge que han tenido en los últimos años, por lo que se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

Organización de Cooperación y Desarrollo Económico (OCDE).

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

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

Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

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

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

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

La lista mínima preparada por la Organización se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité especial de expertos sobre delitos relacionados con el empleo de las computadoras del Comité Europeo para los problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras y en particular las directrices para los legisladores nacionales. Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

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

Adicionalmente, en 1992, la Organización elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos el mismo año.[88]

Organización de las Naciones Unidas (ONU).

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

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal - hasta ese entonces -era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.
En general, se supuso que habría un gran número de casos de delitos informáticos no registrados.

Por todo ello, en vista de que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró, que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

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

[88] http://tiny.uasnet.mx/prof/cln/der/silvia/lexis.htm

Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición.
A continuación haré una breve síntesis de los posibles tipos delictivos que la Organización de las Naciones Unidas ha reconocido como delitos informáticos, con independencia del análisis que se haga en los descritos por la legislación mexicana.

Tipos de delitos informáticos reconocidos por las Naciones Unidas.

a) Fraudes cometidos mediante manipulación de computadoras. Estos pueden suceder al interior de Instituciones Bancarias o cualquier empresa en su nómina, ya que la gente de sistemas puede accesar a todo tipo de registros y programas.

-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 tienen conocimientos especializados en programación e 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 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. Aprovecha las repeticiones automáticas de los procesos de cómputo accesando a los programas establecidos en un sistema de información, y manipulándolos para obtener una ganancia monetaria. Es una técnica especializada que se denomina *técnica del salchichón* en la que en rodajas muy finas apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

b) Falsificaciones informáticas. Manipulando información arrojada por una operación de consulta en una base de datos.

-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.

c) 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. Programas contenidos en programas que afectan directamente a la maquina que se infecta y causa daños muy graves.

-Gusanos. Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno.

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

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

-Acceso no autorizado a servicios y 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. Por lo tanto Hackers y Crackers dispuestos a conseguir todo lo que se les ofrezca en la red, tienen gran conocimiento de las técnicas de cómputo y pueden causar graves daños a las empresas.

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

Es la copia indiscriminada de programas con licencias de uso para copias de una sola persona, se le conoce también como piratería.[89]

Por su parte, el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada.

Asimismo, la Organización de las Naciones Unidas resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

-Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.

-Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

-Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

-No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

-Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

-Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.[90]

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, 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.

[89] http://iiny.uasnet.mx/prof/cln/der/silvia/tipos.htm
[90] http://www.delitosinformaticos.com.mx/ y http://www.delitosinformaticos.com/estafas/

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

CAPÍTULO IV

PROPUESTA JURÍDICA PARA ACLARAR EL CONTENIDO DEL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL

4.1 CÓDIGOS PENALES DE LAS ENTIDADES FEDERATIVAS QUE SANCIONAN DICHASCONDUCTAS ILÍCITAS

Gracias a los grandes avances tecnológicos, y a la falta de trabajo Legislativo a nivel Federal y Local, no existen grandes avances en materia de Delitos Informáticos, en estos últimos años se han realizado esfuerzos por realizar un trabajo legislativo que tutele estas conductas que cada vez más afectan las relaciones cotidianas de toda la Nación.

Como se puede apreciar en el capítulo anterior, son diversas las legislaciones extranjeras que ya se han preocupado por legislar en materia de delitos informáticos, sin embargo, en el caso de México, se ha empezado a tratar de manera incipiente.

En México es necesario analizar las normas que regulan penalmente las conductas ilícitas relacionadas con la informática. Al respecto analizaremos los delitos aplicables o que pudiesen ser aplicables a la normatividad, como son: el Código Penal para el Estado de Sinaloa, Morelos, Tabasco, Nuevo León y el Código Penal Federal mismos que a continuación se detallan.

4.1.1 CÓDIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA

Empezaremos diciendo que el antecedente primario de los llamados delitos informáticos en México, se encuentra legislado en el Código Penal de Sinaloa, el cual contempla la denominación de delitos informáticos cuyo congreso local dio importancia a que se legislara en esta materia, por lo que considero pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo
Delitos contra el patrimonio

Capítulo V
Delito Informático.

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

I. Use o entre a una base de datos, 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".

En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio de las personas por encontrarse dentro del título correspondiente a los delitos patrimoniales, por lo cual, desde su colocación estructural en el Código se está limitando, ya que el objeto o el bien jurídico tutelado no sólo es el patrimonio de las personas; por lo que consideramos que se ubicó al delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad y a la información.

El delito informático en ésta legislación, es determinado unisubjetivo, ya que de igual forma que otros basta de un solo individuo que perpetre la conducta para que se agote el elemento llamado sujeto activo, esto en razón de su redacción la cual dice: "...la persona..." "...al que cometa...".
En su aspecto subjetivo, el agente al desplegar su conducta de acción la debe realizar conociendo y queriendo el resultado, ya que al estar redactando precisando; "...la persona que dolosamente...", no admite la culpa en la comisión del ilícito, por lo que solo será punible el actuar doloso.

En la fracción primera se contempla la conducta de usar o entrar a una base de datos contenida mediante archivos en un disco fijo de almacenamiento de datos informáticos, o a un sistema de computadoras mismas que se encuentran conectadas entre sí en red, pero dicha conducta se entenderá sólo si se tiene como propósito el diseñar, ejecutar o alterar un esquema o artificio; un esquema debe de entenderse como una diagramación que servirá como base para la realización de un programa informático; y el artificio puede ser un desencriptador o decodificador de señales de telecomunicaciones; por lo que el agente al tener acceso a la información podrá diseñar, altera y/o ejecutar un esquema o artificio que sea capaz de defraudar para su provecho, proporcionarle dinero de manera ilícita o información no autorizada.

En la fracción segunda, nos encontramos que no establece un fin o propósito buscado por el delincuente informático, basta que la conducta se efectúe sin importar la causa que motivó su realización, así encontramos las conductas de interceptar, interferir, recibir, usar, alterar, dañar o destruir, sea por los medios que fueren y sus formas de ejecución, a un soporte lógico mediante el cual trabaja una base de datos, o a un programa de computadora, o a los datos (no a la base de datos o conjunto de datos que trabajan sobre un mismo sistema o soporte lógico), ya sea que se encuentren en una computadora, base de datos, en un sistema o en una red.

De esta manera, creemos de que aún y cuando se encuentra tipificado en el Código Penal del Estado de Sinaloa y cumple con el elemento de tipicidad, también es cierto que no satisface el resto de los elementos como podría ser el establecer de manera clara cual es el sujeto activo y pasivo, la naturaleza del ilícito, es decir si se trata de un delito continuado, permanente, o instantáneo.

Todos estos aspectos son considerados de gran importancia en materia penal, y ante esta afirmación concluimos que se trata de un tipo penal tradicional como lo es el fraude al obtener un lucro indebido, por lo que la única variante es el utilizar medios o sistemas informáticos. Por lo tanto hay que recordar que este tipo de delitos informáticos no siempre tienen el propósito de obtener un lucro, ya que en muchas ocasiones muchas de esas conductas se realizan por gusto o reto intelectual.

4.1.2 ESTADO DE MORELOS

La legislación local del Estado de Morelos otorga protección a la intimidad, por lo que cubren ciertas conductas que encuadran en los posibles delitos informáticos.

Delitos Contra la Intimidad Personal o Familiar

Capítulo I
Violación de la Intimidad Personal

ARTÍCULO 150.- "Se impondrán de seis meses a cuatro años de prisión, a quien sin consentimiento de otro o sin autorización judicial, en su caso, y para conocer asuntos relacionados con la intimidad de aquél:
I. Se apodere de documentos u objetos de cualquier clase;
II. Reproduzca dichos documentos u objetos; o
III. Utilice medios técnicos para escuchar, observar, transmitir, grabar o reproducir la imagen o el sonido".

4.1.3 ESTADO DE TABASCO

Al igual que Morelos, este Estado solo otorga protección a la intimidad por lo que se tipifica la misma conducta con la única diferencia de que en el Estado de Tabasco la sanción es de cinco años como se establece a continuación de manera textual.

Delitos Contra la Intimidad Personal

Capítulo Único
Violación de la Intimidad Personal

Artículo 163. "Se impondrá prisión de seis meses a cinco años, a quien sin consentimiento de otro o sin autorización judicial, en su caso, y para conocer asuntos relacionados con la intimidad de aquél:

I. - Se apodere de documentos u objetos de cualquier clase;
II. - Reproduzca dichos documentos u objetos,
III. - Utilice medios técnicos para escuchar u observar, transmitir, grabar o reproducir la imagen o el sonido".

Como se puede apreciar en el presente apartado, existen legislaciones donde se ha otorgado protección con fundamento en el derecho a la intimidad, sin embargo y como se desprende de los Estados de Morelos y Tabasco, la protección es muy limitada, ya que carece de tutela de cualquier información que no sea relacionada con la intimidad.

4.1.4 ESTADO DE NUEVO LEÓN

Por otro lado tenemos al Estado de Nuevo León el cual en su artículo 365, hace mención a lo que podría ser un robo informático.

Artículo 365.- "Se equipara al robo, y se castigará como tal:

IV. El apoderamiento material de los documentos que contengan datos de computadoras, o el aprovechamiento o utilización de dichos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos".

Así podríamos seguir mencionando mas al respecto, pero el objetivo de éste trabajo no es analizar las conductas de las legislaciones locales sino mas bien que sirvan como base de apoyo para que nos demos cuenta que los delitos informáticos dado a su dificultad de persecución, el atraso legislativo, circunstancias, factores etc; los convierte en un tema muy discutido por muchos autores, pero lo que si podemos afirmar como opinión personal es que tanto en el Estado de Sinaloa, como en el de Morelos, Nuevo León y Tabasco por mencionar algunos, son tipos tradicionales y que tienen como medio comisivo a las computadoras.

4.2 DELITOS QUE ESTABLECE EL CÓDIGO PENAL FEDERAL EN MATERIA DE DELITOS INFORMÁTICOS

Después del estudio de las experiencias adquiridas por diferentes Países para enfrentar el Delito Informático, es decir, en un contexto internacional, y la manera en que está siendo regulada esta problemática en México a nivel local, corresponde analizar en éste apartado sólo algunas figuras delictivas que los legisladores mexicanos han incluido en el Código Penal Federal. Esto en razón de que existen delitos como el robo, fraude, espionaje, sabotaje, por citar sólo algunos los cuales si bien corresponde a una clasificación diferente según el ordenamiento antes citado; son delitos que se han dado con una única nota en común: su vinculación con el ordenador.

De lo anterior consideramos que la protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo.

Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Por lo tanto, teniendo en cuenta la gravedad que implican los delitos informáticos, y el no poder hablar de delito informático por aludir a un comportamiento no tipificado como tal en el Código Penal, y mas aún de que en verdad no se desprende un delito con naturaleza propia, sino que puede ser cualquiera cometido por medio de la computadora afectando de diversas formas un bien jurídico tutelado como lo es la información.

4.2.1 ATAQUES A LAS VÍAS DE COMUNICACIÓN

En atención al Decreto por el que se reforman diversas disposiciones en materia penal, el cual fue publicado en el Diario Oficial de la Federación el día 17 de mayo de 1999, se reformaron las fracciones II y VI del artículo 167 del Código Penal y se adiciona un nuevo tipo penal contemplado en el artículo 168- bis, los dos numerales del Libro Segundo, Título Quinto de Delitos en Materia de Vías de Comunicación y de Correspondencia, Capítulo I "Ataques a las Vías de Comunicación y Violación de Correspondencia", del Código Penal Federal; los cuales son considerados delitos federales por ser referentes a la materia de telecomunicaciones, siendo estos los siguientes:

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

II.- Al que destruya o separe uno o más postes, aisladores, alambres, máquinas o aparatos, empleados en el servicio de telégrafos; cualquiera de los componentes de la red pública de telecomunicaciones, empleada en el servicio telefónico, de conmutación o de radiocomunicación, o cualquier componente de una instalación de producción de energía magnética o electromagnética o sus medios de transmisión".

Se trata de un tipo penal que contempla, la acción dolosa o culposa, de afectar físicamente a los componentes cuales quiera que estos sean. Como se sostuvo anteriormente, la información de una computadora se encuentra en un disco de almacenamiento de datos que se encuentra magnetizado, y la computadora sólo genera energía electromagnética para operar o transmitir su información, sin embargo podemos referir que el presente tipo penal protege solo las vías de telecomunicación por donde viaja la información, y no la información en sí, y tampoco se puede contemplar la computadora del usuario como medio de transmisión en atención a la fracción X del artículo 3ro de la Ley Federal de Telecomunicaciones que dice:

"Red pública de Comunicaciones: la red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios, ni de las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal".

Por otra parte la fracción VI del mismo artículo penaliza:

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

En esta norma punitiva nos encontramos con un grave error de redacción, ya que las comunicaciones en sí, no son alámbricas, ni inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, ya que estos son medios de transmisión, vías generales de comunicaciones, y más propiamente, redes de telecomunicación a través de las cuáles se transmiten las comunicaciones, ya sea de manera eléctrica, por ondas electromagnéticas o microondas, tal y como lo establece la fracción VIII del artículo 3ro de la Ley Federal de Telecomunicaciones.

VIII. "Red de telecomunicaciones: sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario".

Así como también establece en su artículo 4° de la última Ley citada que dispone:

"Para los efectos de esta Ley, son vías generales de comunicación el espectro radioeléctrico, las redes de telecomunicaciones y los sistemas de comunicación vía satélite".

En atención al análisis anterior consideramos que en lugar de la palabra comunicaciones debería decir "que conforme a las leyes especiales se consideren como vías generales de comunicaciones" para quedar de la siguiente manera:

Al que dolosamente o con fines de lucro, interrumpa o interfiera las que conforme a las leyes especiales se consideren como vías generales de comunicaciones, ya sean alámbricas, inalámbricas, o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos.

De esta manera la acción positiva, con o sin la intención de obtener un beneficio pecuniario, de interrumpir o interferir el espectro radioeléctrico, las redes de telecomunicaciones o los sistemas de comunicación vía satélite, se transfieran señales de audio, videos o datos, incluyendo así las redes informáticas de telecomunicaciones o Internet.

El artículo 168-bis establece que:

"Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho:

I. Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas, o

II. Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas".

En este tipo penal se castiga a la acción de descifrar o decodificar señales de telecomunicaciones distintas de las microondas, no importando el propósito delictivo del agente es punible, siendo también antijurídico la venta o renta de los aparatos, instrumentos o información que permita descifrar o decodificar, por lo que se persigue tanto el que ejecuta el delito, como el que le proporciona los medios para su ejecución. En la norma se protege así la información contenida en los programas, cuya privacidad es un derecho del titular de dicha información; es por eso que sería muy aceptable el agravar la pena contemplando la posibilidad de que el agresor venda, utilice o arriende la información que ha descifrado o decodificado.

4.2.2 VIOLACIÓN DE CORRESPONDENCIA

Artículo 177. "A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa".

Este tipo penal está estructurado de la siguiente manera:

Que la conducta de intervenir comunicaciones privadas se haga en contravención, es decir, sin la autorización de un Juez Federal en Materia Penal.

Que la norma jurídica no será aplicable cuando un particular con su conducta antijurídica afecte a otro particular, ya que el mismo artículo se contempla por el Código Penal para el Distrito Federal.

Y con referencia a los sujetos, tenemos que el Sujeto Pasivo, es un servidor público, empleado federal en ejercicio de sus funciones, funcionarios, electores federales o partidistas, o particular indeterminado

Por último el sujeto activo, quien puede ser un Servidor Público o empleado federal en ejercicio de sus funciones, funcionarios electorales o partidistas, o un particular indeterminado.

Para la integración del ilícito deben existir comunicaciones privadas, las cuales no se establece de manera precisa la clase de comunicaciones privadas a ser intervenidas, ya que pueden ser las realizadas usando el servicio de telefonía alámbrica o inalámbrica por vía satélite, por medio de radio o a través de las redes informáticas de telecomunicaciones, en razón de esto se hace necesario adecuar al presente tipo penal a la redacción que las tecnologías actuales en materia de telecomunicaciones y a la proliferación en el uso del correo electrónico.

4.2.3 PORNOGRAFÍA INFANTIL

Existen muchas definiciones acerca de lo que es pornografía, pero en un contexto general, particularmente considero que la pornografía es una industria, una cadena productiva que involucra a personas que lucran de ella, personas que trabajan directamente en ella y consumidores que pagan por ella y que obtienen a cambio una gratificación sexual.

Dicho delito se encuentra previsto dentro del titulo octavo referente a delitos contra la moral pública y las buenas costumbres en su capitulo II.
Por tanto para efectos del tema que nos ocupa, se describe textualmente el artículo 201 bis que a la letra dice:

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

Para los efectos de este artículo se entiende por pornografía infantil, la representación sexualmente explícita de imágenes de menores de dieciocho años".

El Gobierno Mexicano ha formado un Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos formado por: la Procuraduría General de la Repúbiica, la Procuraduría General de Justicia del Distrito Federal, la Policía Federal Preventiva, el Centro de Investigación y Seguridad Nacional, la Asociación Mexicana de Internet, la Secretaría del Trabajo y Previsión Social, la Secretaría de la Defensa y de la Marina, la Presidencia de la República, E-México, la Universidad Nacional Autónoma de México, Teléfonos de México, Avantel, entre otros.

Ante esta problemática, de los ya mencionados delitos informáticos, se desprende, que, de estos Grupos de Coordinación Interinstitucional de Combate a Delitos Cibernéticos en relación a la pornografía infantil es de gran relevancia resaltar el trabajo que la Policía Federal Preventiva a realizado y que a continuación se describe.

Policía Cibernética.

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

Los crímenes cometidos en agravio de menores a través de una computadora y otros medios han tenido un incremento sin precedentes, tanto en México como en el mundo. Internet ha sido ulilizado por organizaciones criminales de pedófilos que promueven y transmiten pornografía infantil; así mismo, se han detectado bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento.

Mención aparte, lo constituye el incremento de casos de niños desaparecidos en México, que son robados por extraños o sustraídos por padres en proceso de separación, lo que provoca un severo daño psicológico al menor.

En el peor de los casos, la victimización del menor apartado del seno familiar alcanza niveles de alarma cuando se observan patrones de alimentación a redes internacionales de prostitución y/o de abuso sexual.

Misión de la Policía Cibernética.

-Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.

-Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos.

-Realización de operaciones de patrullaje anti hacker, utilizando Internet como un instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.

-Análisis y desarrollo de investigaciones en campo sobre actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

Actividades de la Policía Cibernética.

-Integrar un equipo especializado en delitos cibernéticos a fin de hacer a este medio electrónico un lugar seguro para el intercambio de información.

-Analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciberespacio, así como su *modus operandi*.

-Utilizar la Internet como un instrumento para identificar a los delincuentes que cometan este tipo de delitos.

-Realizar patrullajes en la red a fin de localizar sitios que hayan podido ser vulnerados.

-Analizar y desarrollar estrategias para la identificación de los diversos delitos ocurridos en Internet.

-Ofrecer seguridad en la navegación en la Internet para los menores ya que existen peligros en ella.

-Identificar los procedimientos mediante los cuales los niños son explotados por personas mayores.

-Identificar la naturaleza, extensión y causas de los delitos cometidos en contra de mujeres y menores como son la corrupción y explotación sexuales.

-Identificar y combatir al crimen organizado dedicado al tráfico de menores.

-Establecer técnicas adecuadas para la búsqueda y localización oportuna de niños extraviados, perdidos y/o robados.

-Crear estrategias para combatir a las redes de delincuentes que se dedican a dañar a los menores de edad.

-Desintegrar y poner a disposición del ministerio público a las bandas de pedófilos dedicadas a la explotación sexual de menores y a la pornografía infantil.

-En materia de delitos cibernéticos se mantiene un patrullaje sobre sitios y atención a los llamados de la ciudadanía cuando hay ataques de hackers o fraudes a través de la Internet.

-Acciones de cooperación con autoridades locales, federales e internacionales.

-Se mantiene patrullaje en la red mediante software convencional para rastreo de hackers y sitios de Internet, comunidades y chat rooms en los que promueven la pornografía y el turismo sexual infantil. Asimismo, se utiliza Internet como un instrumento para detectar a delincuentes que organizan sus actividades en la red como los fraudes electrónicos.

-Se realiza análisis sobre actividades de organizaciones locales e internacionales de pedofilia así como de redes de prostitución infantil y redes de tráfico de menores que los explotan o prostituyen en otros países.

-Se desarrolla una Base de Datos Nacional para la identificación de patrones, rangos, preferencias y *modus operandi* de los casos reportados de menores extraviados, desaparecidos, abusados sexualmente, explotados, traficados y prostituídos, además de la integración de un Banco Nacional de Datos sobre pedofilia y agresores sexuales.

-Se cuenta con proyectos bilaterales con el Sistema Nacional para el Desarrollo Integral de la Familia (DIF), además se tienen convenios con Organizaciones Gubernamentales Nacionales que reportan casos de niños robados como son la Asociación Pro Recuperación de Niños Extraviados y Orientación a la Juventud de México, la Asociación Mexicana de Niños Robados y Desaparecidos, y la Fundación Nacional de Investigación de Niños Robados y Desaparecidos.

-Se tienen proyectos bilaterales con "International Center for Missing & Exploited Children", "National Center for Missing & Exploited Children", "U.S. Customs Cybersmuggling Center", "Oficina de Asuntos de Menores del Departamento de Estado de Estados Unidos" e Interpol.

-Se tienen contactos con otras instituciones que están ayudando a combatir los delitos que se cometen contra menores: Tecnológico de Monterrey, Casa Alianza, Unicef, Adivac, México Ciudad Humana, y Espacios de Desarrollo Integral.

-Promover la seguridad en los sistemas de computo de usuarios y empresas para evitar robo de información, espionaje y sabotaje de sitios en Internet.[91]

[91] http://www.ssp.gob.mx/cprogramas/p_cibernetica/INDEX.htm

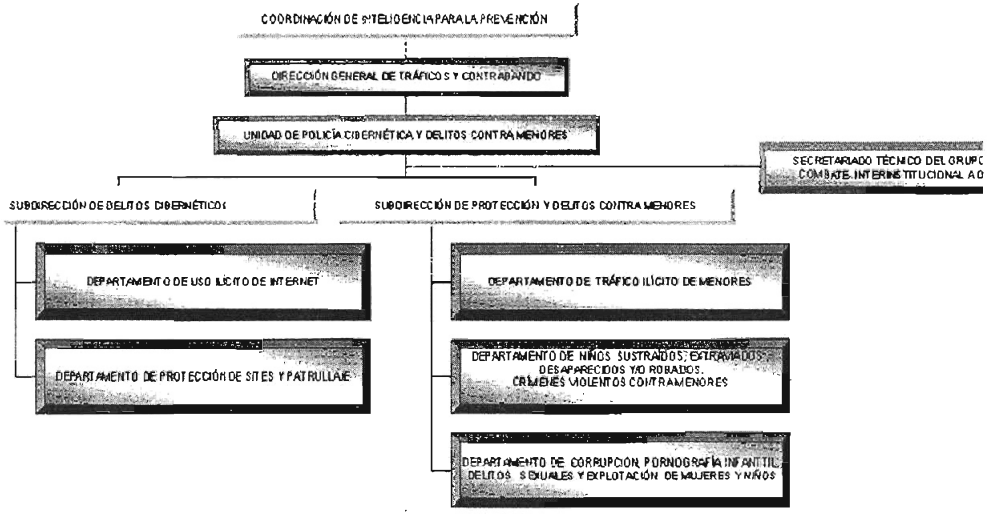
Organigrama de la Policía Cibernética.

En atención a lo anterior es importante destacar como esta estructurada la Policía Cibernética en donde los departamentos de ésta cumplen con una función muy importante para la cual cuentan con dos subdirecciones, la primera es la Subdirección de Delitos Cibernéticos, y la segunda es la Subdirección de Protección y Delitos contra menores.

En la primera se encuentran dos departamentos de suma importancia como son el de uso ilícito de Internet y el departamento de protección de sitios y patrullaje.

En la segunda se encuentran tres departamentos que al igual que la anterior son sumamente importantes para esta Unidad de Policía y estos son; los departamentos de tráfico ilícito de menores, el departamento de niños extraviados, desaparecidos y/o robados, y por último tenemos al departamento de corrupción, pornografía infantil, delitos sexuales y explotación de mujeres y niños.

La Unidad de Policía Cibernética está adscrita a la Coordinación General de Inteligencia para la Prevención de la Policía Federal Preventiva, como a continuación lo muestra el organigrama.



4.2.4 DELITOS EN MATERIA DE DERECHOS DE AUTOR

En el Interior del Código Penal Federal de su libro Segundo Título Vigésimo sexto, "De los Delitos en Materia de Derechos de Autor" encontramos una posible aplicabilidad del delito informático en sus artículos 424 fracción III, 424-bis fracción II y 426 fracciones I y II, mismos que señalan lo siguiente:

Artículo 424.-"Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa:

III. A quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor".

En el presente tipo penal existe la prevención de que se ejecute una conducta con el elemento llamado dolo como un aspecto subjetivo del activo, no admite la culpa, quien con un fin de lucro y sin haber obtenido la autorización de quien deba darla, use, de cualquier forma, obras protegidas por la Ley Federal del Derecho de Autor, teniendo como bien jurídico tutelado tanto los derechos morales como patrimoniales de su titular; el uso de dichas obras se puede realizar a través de las redes informáticas de telecomunicaciones, ya que existen páginas en Internet que usan obras protegidas para atraer publicidad a suscriptores, o como una simple imagen de la página de la red, no escapando la posibilidad de que alguna de estas páginas o sitios usen la obra protegida sabiendo que se requiere de una autorización para ello y que con su actuar se provoca un resultado en detrimento del titular de la obra, así el tipo penal podría ser más específico y señalar los medios para la comisión, ya que no refiere de manera expresa la utilización de medios electrónicos o de las telecomunicaciones.

Artículo 424- bis. "Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

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

De la fracción primera se desprende, la producción, reproducción, introducción al país, el almacenamiento, la venta o renta de obras, fonogramas o videogramas, que en la actualidad a través del Internet se puede tener acceso a obras, fonogramas y videogramas mediante el pago de cierta cantidad de dinero otorgada por medio de tarjetas de crédito, con ello se obtiene un número que permitirá dicho acceso, pudiendo copiar y transmitir posteriormente a terceros los archivos, algunas empresas trabajan con la debida autorización, pero también existen algunas que no la tienen; además existen sitios que permiten su acceso de manera gratuita a una base de datos informáticos que contienen obras, videogramas y fonogramas.

Esta conducta se actualiza sin la finalidad de la especulación de quien deba darla, e indudablemente causa un perjuicio en el titular de la obra, por que se hace necesario que dicha observación se incluya en el tipo penal, además de la especificación concreta de los medios que puede emplear el activo para cometer el delito.

Por otro lado, la fabricación de dispositivos o sistemas, se hacen a través de la creación de programas informáticos (software) capaces de decodificar datos de tal manera que se acceda a sistemas protegidos. Existen programas capaces de buscar un millón de combinaciones por minuto, los más potentes logran violar cualquier sistema protegido en un tiempo inferior a los 10 minutos, de ahí la seguridad que se busca con la redacción del presente tipo penal, y evitar la proliferación de estos programas.

Artículo 426. "Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes:

I. A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, y

II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal".

En estos casos se pretende que el tipo penal desestime la actividad conocida como robo de señales, ya que las microondas emitidas por los sistemas satelitales contienen información que al llegar a un decodificador genera imágenes y sonidos, los cuales se encuentran restringidos ya sea para la distribución comercial al público o de carácter confidencial al Gobierno Federal.

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

A continuación se presentan algunos comentarios pertinentes respecto a los elementos que deben contemplarse en atención a la problemática de los derechos de autor en nuestro país.

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

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

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

Esta ley en su artículo 215 hace una remisión al establecer que corresponde a los Tribunales de la Federación de los delitos relacionados con el derecho de autor previsto en el Título Vigésimo Sexto del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal.

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

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

En la redacción de estas fracciones se trata de evitar la llamada piratería de programas en el área del comercio, permite la regulación administrativa antes de acudir a la penal.

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

Tal y como hemos sostenido, México no está exento de formar parte de los países que se enfrentan a la proliferación de estas conductas ilícitas. Recientemente, esto ha traído como consecuencia desventajas para México, entre las que podemos citar, a las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que se remontaban a un valor de mil millones de dólares por concepto de piratería de estos programas.

Por tanto diremos que lo que justifica su regulación penal es la gravedad de la conducta ilícita en sí, y las implicaciones que conllevan estas.

En otro orden, el Artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información.

Asimismo, consideramos que la protección a este tipo de bases de datos es necesaria, en virtud de que la información contenida en ellas puede contener datos de carácter sensible, adicionalmente pueden ser susceptibles de chantaje, los clientes de determinadas instituciones de créditos que posean grandes sumas de dinero, en fin, la regulación de la protección de la intimidad personal es un aspecto de suma importancia que se encuentra regulado en este artículo.

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

Por otra parte, debe mencionarse que en abril de 1997 se presentó una reforma a la fracción III del artículo 231 de la Ley Federal del Derecho de Autor así como a la fracción II del artículo 424 del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal.

4.2.5 REVELACIÓN DE SECRETOS

Anteriormente el Título Noveno sólo se integraba por el delito de revelación de secretos, el cual sólo protege la confidencialidad de la información; pero con la reforma el legislador ubicó dentro de éste mismo Título al acceso ilícito a sistemas y equipos de informática por considerar que no solo se atenta con estas conductas en contra de los bienes patrimoniales, sino que pueden dar cabida a la vulneración de otros bienes, como la intimidad o la información en general.

Artículo 211 bis.- "A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicaran sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa".

El presente artículo se encuentra en el Libro Segundo del Título Noveno "Revelación de Secretos y Acceso ilícito a Sistemas y Equipos de Informática" Capítulo I "Revelación de Secretos" y de su redacción se hace lo siguiente:

Sujeto Activo.- Servidor Público o empleado federal en ejercicio de sus funciones, no pudiendo tener otra calidad ya que el mismo artículo es contemplado por el Código Penal para el Distrito Federal.

Sujeto Pasivo.- Servidor Público o empleado federal en ejercicio de sus funciones, funcionarios electorales federales o partidistas, o un particular indeterminado.

Para la integración de este delito, es necesario que el sujeto activo en ejercicio de sus funciones intervenga en alguna comunicación de carácter privado, o el que tuvo el conocimiento del contenido de dicha comunicación privada realice la acción positiva de revelar, divulgar o utilizar la información o imágenes contenidas en la comunicación intervenida, ya sea de manera indebida, es decir, fuera del propósito autorizado por la autoridad judicial para intervenir las comunicaciones privadas, o en perjuicio de otro.

Al igual que el artículo 177, del mismo Código, no se establece de manera precisa la clase de comunicaciones privadas intervenidas por lo que también se hace notoria la necesidad de adecuar el tipo penal a la redacción que las tecnologías actuales hacen en materia de comunicaciones y telecomunicaciones, esto con la finalidad de crear una mayor certeza jurídica en su aplicación.

Partiendo del supuesto de que el bien jurídico protegido por el tipo en la revelación de secretos es la confidencialidad de la información, consideramos correcta la ubicación dentro de dicho ordenamiento legal.

4.2.6 ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

Refiriéndonos al contenido del Título Noveno capítulo II Acceso Ilícito a Sistemas y Equipos de Informática. Tendremos que dichos artículos y denominaciones son realmente novedosos al incluir por vez primera dentro de la norma penal, referencias a sistemas y equipos de informática; y a éstas nuevas conductas contempladas en nuestro Código se le conoce como Delitos Informáticos, siendo los siguientes:

Artículo 211 bis1.- "Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

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

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

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

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

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

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

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

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

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

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

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

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

De lo anterior se desprende que en México en este cuerpo normativo federal se sancionan el que un sujeto tenga acceso ilegal a dichos sistemas y los altere, dañe, modifique o provoque pérdida de información contenida en tales sistemas.

En el siguiente capítulo analizaremos los elementos de acuerdo a la estructura que presentan estas conductas.

4.3 ANÁLISIS EN MATERIA DE DELITOS INFORMÁTICOS DEL TÍTULO NOVENO CAPÍTULO II DEL CÓDIGO PENAL FEDERAL

4.3.1 LA REFORMA DEL 17 DE MAYO DE 1999 DEL CÓDIGO PENAL FEDERAL.

El antiguo Código Penal, no preveía de manera alguna la regulación penal de las conductas ilícitas derivadas del uso de la computadora, hasta que fueron aprobadas una serie de reformas el 17 de mayo de 1999 publicadas en el Diario Oficial de la Federación.

El origen se remonta a la denominada Cruzada Nacional contra el Crimen y la Delincuencia, la cual presentaba una serie de iniciativas en diversas materias con el objetivo de actualizar nuestra legislación para hacer frente a la inseguridad por la que atraviesa el país.

La inclusión de estas conductas delictivas del Título Noveno del Código Penal Federal, cuyo título es Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática, evidentemente revela una concordancia exclusiva en su manejo derivado de la Ley Federal de Derecho de Autor, toda vez que el bien jurídicamente tutelado en el mismo no sólo es la propiedad intelectual, sino el derecho de privacidad o patrimonial derivado de la información contenida en los sistemas de computación con el consecuente perjuicio derivado de la conducta del agente, excluyéndose por supuesto la situación relacionada con la titularidad de los programas operativos o de software incluidos en los sistemas computacionales los cuales recaen en el ámbito de derecho de autor y cuyo tratamiento se encuentra regulado en la Ley de la Materia y en las disposiciones del Código Penal, como ya fue mencionado en el tema anterior.

Por lo tanto a raíz de estas reformas fue que se incluyeron los artículos que enunciamos ya con anterioridad respecto a los sistemas y equipos de informática, contenidos estos en los artículos 211 bis-1, 211 bis-2, 211 bis-3. 211 bis-3, 211 bis-4, 211 bis-5, 211 bis-6, y 211 bis-7 bajo la denominación "Acceso Ilícito a sistemas y equipos de informática", los cuales serán analizados posteriormente.

4.3.2 ANÁLISIS JURÍDICO SOBRE EL ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

A continuación se realizará un estudio jurídico dogmático sobre los delitos informáticos que se encuentran previstos en el Título Noveno Capítulo II del Código Penal Federal, los cuáles no tienen ciertamente tal denominación, pero que evidentemente se refieren a ellos dada la naturaleza jurídica de su tratamiento en el ámbito penal.

Delito Federal.

Es un ilícito de persecución federal, toda vez que su tipificación se encuentra regulada en el Código Penal Federal, por lo cual resulta suficiente la denuncia que se haga del mismo para que la Autoridad Investigadora se aboque a su investigación y posterior ejercicio de la acción penal.

Delito Grave.

Consideramos que las conductas delictivas transcritas en los numerales anteriores representan delitos graves, esto en atención a los resultados que pueden ocasionarle al pasivo lo que se traduciría en pérdidas económicas de muy alto índice, aún por el simple conocimiento de la información contenida en los sistemas de cómputo.

Delito de Daño.

Con estas conductas accesando ilícitamente a sistemas y equipos de informática y dadas las circunstancias y consecuencias podría considerarse un delito de daño o lesión ya que necesariamente la conducta del agente trae consigo la modificación, destrucción, o pérdida de información contenida en los sistemas de cómputo.

Delito Instantáneo.

Es un delito instantáneo, pues se consuma en el momento mismo en que el agente modifica, destruye o provoca la pérdida de la información o bien en el preciso instante en que el activo logró conocer la información objeto de la tutela penal o la copia, con la sola realización de dichas conductas el bien jurídico, en este caso, la información se destruye, modifica o simplemente deja de existir, lo cual acontece de manera instantánea. Sin embargo también puede ser un delito permanente, toda vez que los efectos de la conducta pueden prolongarse en el tiempo durante todo el lapso en que ocurra la modificación de la información o bien ésta sea recuperada.

Acción.

El tipo penal que nos ocupa, se encuentra conformado por dos párrafos, que engloban cinco conductas diferentes, tales como modificar, destruir, provocar pérdida de información, conocer o copiar información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero.

Podemos entender por modificar, el hacer algo que parezca distinto de cómo era, destruir significa deshacer o inutilizar. Por otro lado el conocer, podemos entenderlo como saber o tener una idea de algo o de alguien, y copiar quiere decir hacer algo semejante o igual a lo que ya está hecho.

Como podemos ver, todas estas conductas incluyendo la provocación de pérdida de la información, implican una acción, toda vez que para el sujeto activo modifique, destruya, conozca, copie o provoqué pérdida de información se requiere, en primer lugar del movimiento corporal consistente en encender la computadora. posteriormente introducirse al sistema o equipo de informática de una Institución Financiera rompiendo sus sistemas de seguridad para finalmente realizar cualquiera de las conductas descritas por el tipo penal.

Una vez analizado lo anterior, podemos afirmar que el delito que nos ocupa, no puede ser cometido mediante una omisión sino por una acción, ya que para la realización se requiere de la voluntad del agente así como diversos movimientos corporales encaminados a la realización de la conducta. Por lo tanto, difícilmente se podría hablar de una ausencia de conducta, sin embargo, para que dicha acción sea atribuible a la persona que la llevo a cabo, se requiere del elemento de la voluntad.

Entonces se puede decir que la ausencia de conducta es cuando la "acción o la omisión son involuntarias, o bien, cuando el movimiento corporal o la inactividad no pueden atribuirse al sujeto por faltar en ellos la voluntad".[92]

El elemento normativo "sin autorización" a nuestro entender significa el pleno conocimiento del sujeto que realiza la acción de que su conducta es contraria a derecho, motivo por el cual estimamos que difícilmente pudiesen darse algunos de los casos que ya se vieron en el capítulo segundo de este trabajo, referente al artículo 15 del Código Penal Federal.

[92] PAVON VASCONCELOS, FRANCISCO.Ob. Cit. 276.

Un ejemplo de esto sería el sonambulismo, hipnotismo, sueño, o cualquier otra causa, pues el sujeto al introducirse sin autorización (tecleando un password o la contraseña indicada) a un sistema de una institución financiera, y en ese estado modifique, destruya provoque pérdida, conozca o copie información. Es por ello que a nuestro parecer ninguna de las hipótesis señaladas como ausencia de conducta podría actualizarse en este artículo.

De lo anterior se concluye que estamos en presencia de un delito de acción, consistente en todos los movimientos corporales externos voluntarios que realiza el agente para lograr su objetivo al manipular y acceder a la información contenida en sistemas o equipos de informática, en las diversas comisión del delito.

Precisaremos que en los artículos descritos resulta omiso respecto a la forma en que puede llevarse acabo la conducta toda vez que refiere en todos los supuestos a las consecuencias de ésta, es decir a un resultado, al expresar los términos modifique, destruya o provoque pérdida de información, es decir que la conducta del agente puede llevarse acabo de cualquier manera, siempre y cuando se viole un requisito establecido en la ley.

Al establecer en los artículos ya mencionados "protegidos por un mecanismo de seguridad", es un concepto que en opinión particular es muy general y nada concreto, el cual se tratará con especial cuidado en el siguiente tema con referencia a la propuesta de este trabajo.

La conducta del agente puede llevarse a cabo de distintas maneras, por ejemplo de manera directa manipulando y venciendo los mecanismos de protección a la información accionando el propio equipo de la víctima o sujeto pasivo, introduciéndose en el sistema operativo y en el sistema informático produciendo con esto la modificación, destrucción o provocando la pérdida de la información, pudiendo realizar esto borrándola mediante el mismo sistema operativo, alterando o modificándola mediante el propio teclado, o insertándole virus o gusanos contenidos en programas de uso de este tipo de elementos dañinos en el software de la máquina, los cuáles se pueden activar inmediatamente o con el transcurso del tiempo o también, mediante la inserción de mecanismos electrónicos de activación de los virus o gusanos que va a producir la modificación, destrucción o pérdida de la información contenida en los equipos de cómputo o sistemas informáticos.

Puede también realizarse la conducta a distancia, incluso desde el extranjero a través de una computadora que conectada a un módem o sistema de acceso telefónico en computadoras logra penetrar y vencer los mecanismos electrónicos de seguridad del equipo del sujeto pasivo e introducir programas activados de virus o gusanos que van a producir la modificación, pérdida o destrucción de la información contenida en el equipo de cómputo de la víctima.

De igual manera la conducta que da lugar al resultado lesivo previsto por la Ley Penal lo puede obtener el agente mediante el conocimiento o la copia de la información contenida en los equipos de cómputo, venciendo los mecanismos de seguridad que protegen dicha información para cumplir su fin que es el acceder a ella, ya sea directamente o a distancia como se ha expresado y de este manera tener conocimiento de la misma o realizando una copia utilizando los diversos métodos que existen ya sea incorporándola directamente al disco duro de la computadora del sujeto activo o de un tercero, o bien, haciendo copias en elementos externos.

Presupuesto Jurídico.

El presupuesto jurídico existe y se encuentra regulado en el artículo 211 bis4, toda vez que es la norma penal que prevé determinada conducta que el legislador considera como delito. Sin embargo, para que el delito llegue a integrarse se requiere del sujeto activo, estos es, de la persona que con su actuar viole el precepto en comento, de un sujeto pasivo en cuyo caso sería una Institución Financiera y del bien jurídicamente tutelado mismo que sería la información guardada en sistemas o equipos de informática.

Por lo tanto en este artículo se estaría en presencia de un presupuesto especial que sería la información, misma que se debe encontrar en los sistemas o equipos de informática de las instituciones financieras, en virtud de que si éste no existiera, el delito no podría llevarse acabo, toda vez, que aún y cuando la intención del sujeto activo se dirigiera a la pérdida, destrucción, conocimiento o copia de la misma, si dicha información no existiese sería imposible llevar acabo la conducta delictiva descrita en el tipo penal de nuestro estudio.

Elemento Normativo.

Tal como lo establece el articulo 211 bis en sus numerales1,2,y 4 en los que se encuentra un elemento de valoración jurídica expresado en la Ley con el término "al que sin autorización" lo que significa que el delincuente o sujeto activo no cuente con ella, es decir sabiendo que no tiene libre acceso a la información accede a ella venciendo cualquier mecanismo de seguridad, asimismo quien cuenta con dicha autorización como lo establece el mismo articulo pero con numeral 3 y 5, viola un deber jurídico de no hacer ya que en el uso de esa autorización del sujeto pasivo realiza la conducta aún cuando le es permitido ingresar a los archivos que contiene la información protegida.

Dolo.

Solo puede presentarse de manera dolosa, sin admitir su comisión por culpa o imprudencia, toda vez que solo las personas que pueden tener cierto conocimiento técnico o empírico derivado del uso de computadoras para lograr el acceso a los sistemas o equipos de informática rebasando o venciendo los mecanismos de protección y produciendo el resultado lesivo, encaminando su voluntad a la consecución de este fin.

Sujeto Activo.

Este delito conforme al número de sujetos que intervienen en su comisión puede ser unisubjetivo, toda vez que permite su realización por una sola persona o plurisubjetivo ya que la conducta típica puede ser consumada con la participación de dos o mas personas.

De acuerdo con la descripción legal contenida en los artículos 211 bis 1 al 5, el sujeto puede ser común o indiferente, al expresarse en la descripción legal la frase "al que sin autorización" lo que denota que cualquier persona física imputable no importando su sexo, edad, condición social económica o cultural pueda acceder a cualquier sistema y produzca la conducta prevista en dichos preceptos legales.

Por otro lado al expresarse en la Ley "al que estando autorizado", es decir que para que pueda consumarse la conducta es necesario que el sujeto activo cuente con la autorización del titular del bien jurídicamente tutelado y a través de esa autorización pueda acceder a los sistemas o equipos de informática, ésta autorización puede ser tácita o expresa derivada del conocimiento ya sea por profesión o empleo de los mecanismos o claves de acceso propiedad del titular de los derechos protegidos.

Sujeto Pasivo.

Se puede afirmar que el titular de los bienes jurídicamente tutelados son:

Cualquier persona que posea información personal o reservada almacenada en un equipo de cómputo debidamente protegido por algún mecanismo de seguridad.

El Estado entendiéndose como tal cualquier Dependencia de la Administración Pública Federal o Local, el Poder Judicial y el Poder Legislativo, cuya información contenida en equipos de informática o de cómputo se encuentre protegido por algún mecanismo de seguridad.

Las Instituciones que integran el Sistema Financiero, entendiéndose estas conforme al artículo 400 bis del Código Penal Federal las siguientes: 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, administradoras de fondos de retiro y cualquier otro intermediario financiero o cambiario, que posean información contenida en los equipos de cómputo o sistemas informáticos protegidos por algún mecanismo de seguridad.

Objeto Material.

El objeto como bien no es la computadora mas bien lo constituye la información almacenada en los equipos sobre los cuales recae la modificación, destrucción o la pérdida de dicha información.

Punibilidad.

El acceso a sistemas y equipos de informática se encuentra agravado en dos supuestos que la misma ley establece. El primero lo contempla el artículo 211 bis 5 en su último párrafo que dice:

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

De acuerdo a lo anterior se entiende que el legislador previó agravar el delito y en consecuencia su penalidad para aquellas personas que cometan las conductas descritas y en el ejercicio de sus funciones como funcionarios o empleados de las instituciones del sistema financiero, entendiéndose como funcionarios o empleados a aquellas personas que se encuentran contratadas laboralmente y prestan un servicio personal subordinado a favor del patrón que en este caso puede ser cualquiera de las Instituciones que integran el sistema financiero que se han dejado precisadas y se relacionan en el artículo 400 bis del Código Penal Federal.

El segundo supuesto lo contempla el artículo 211 bis 7 el cual dispone lo siguiente: "Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno".

Al igual que el anterior, el legislador previó agravar el delito y la sanción al término "obtenga" lo que necesariamente implica que el sujeto activo obtuvo o se hizo de la información contenida en los sistemas de cómputo y esto solo lo puede hacer a través de su copia, sacando provecho de ésta, en perjuicio de su titular en beneficio propio o de un tercero, lo que implica el espionaje electrónico en cualquier forma y no importando el sujeto pasivo que sea, pues evidentemente el provecho que se puede obtener de la información copiada puede ser económico ya sea mediante su explotación directa, vendiéndola, o bien para su propio beneficio.

Imputabilidad.

Analizada la imputabilidad así como su aspecto negativo, decimos que para que un sujeto (que se introduce sin autorización a un sistema o equipo de informática de una Institución Financiera, protegido por algún mecanismo de seguridad, a fin de modificar, destruir, provocar pérdida, conocer o copiar información) se le declare como culpable, éste debe ser imputable al momento de cometer el hecho delictivo, es decir debe conocer y comprender el carácter ilícito del hecho y conducirse de acuerdo a esa comprensión.

Por lo tanto la inimputabilidad en este delito podría darse en el caso de las personas menores de edad y no así a las personas con trastorno mental ya sea permanente o transitorio, ya que para conocer el delito previsto en este artículo 211 bis4, se requiere, generalmente de amplios conocimientos en la materia de informática.

4.4 PROPUESTA DE REFORMA AL CAPÍTULO II DEL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL SOBRE DELITOS INFORMÁTICOS

El uso de la tecnología informática es un instrumento que facilita a la sociedad su desarrollo económico y cultural, mediante su empleo en todas las áreas del desarrollo nacional.

El avance logrado en los últimos años en este sector, ha permitido que un creciente número de personas tengan acceso a esta tecnología y la utilicen cotidianamente para realizar actividades de muy diversa índole, como las educativas, culturales, comerciales, industriales, financieras o de comunicación, entre muchas otras. Hoy en día tiene tal importancia, que muchas de esas actividades no podrían realizarse sin el uso de equipos y sistemas informáticos.

Paralelamente al avance tecnológico han surgido nuevas formas de conducta antisocial que han hecho de los equipos y sistemas informáticos instrumentos para delinquir. Adicionalmente, se presentan conductas en las que dichos equipos o sistemas constituyen el objeto o fin en sí mismo de la infracción.

Dentro de las conductas ilícitas más comunes que constituyen los llamados por la doctrina jurídica como "delitos informáticos", se encuentran: el acceso no autorizado a computadoras o sistemas electrónicos, la destrucción o alteración de información, el sabotaje por computadora, la intercepción de correo electrónico, el fraude electrónico y la transferencia ilícita de fondos.

A partir de que el El Código Penal Federal vigente fue reformado el 17 de mayo de 1999. El lapso de tiempo que ha transcurrido desde entonces es relativamente corto, pero los avances tecnológicos han sido vertiginosos y radicales en algunos casos.

Es por eso que la legislación mexicana en materia de delitos informáticos dista mucho de ser perfecta, por lo que esta reforma es sólo el primer paso para lograr un ambiente sano y seguro para los negocios y comunicaciones electrónicas en nuestro país.

Consecuentemente consideramos que antes de preguntarnos si estos delitos se encuentran mal ubicados dentro del ordenamiento, o si son delitos autónomos o bien si se encuentra el personal especializado para combatirlos como tal, entre otros cuestionamientos: es importante el tener bien definidos los términos a los que hace referencia el Código Penal Federal.

La intención y el objetivo que se buscó al proponer adicionar un numeral mas al artículo 211 bis del Código Penal Federal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer copiar, modificar o provocar la pérdida de información que contengan, en virtud de que el bien jurídico que se tutela es la privacidad y la integridad de la información. El problema es cuando en un tema como ya se había expresado anteriormente tan complejo y que la tecnología avanza día con día el Código Penal deja un margen muy general al no definir que debe entenderse por mecanismo de seguridad y en ese entendido tenemos lo siguiente:

El Código Penal contempla que constituye el delito sólo si se accesa a un sistema informático protegido por un *mecanismo de seguridad*. Esto es tan absurdo como si dijéramos que para que se diera el delito de *allanamiento de morada* es necesario que la casa habitada cuente con un candado, llave, portón o cadena protectora. La justicia no puede reducirse sólo a aquellos quienes tienen los medios económicos para proteger su computadora con un *mecanismo de seguridad*.

¿O qué acaso el que tu computadora esté conectada al Internet significa que cualquiera puede justificadamente entrar en ella, husmear y merodear tranquilamente, borrar o destruir archivos, sólo porque no está protegida por algún *mecanismo de seguridad*?. Aunque hay que enfatizar en este punto que no por eso se está justificando el que el usuario no este a la vanguardia en cuanto a la seguridad informática.

Por otro lado el Código Penal no define qué debe entenderse por "*mecanismo de seguridad*". ¿Qué es un mecanismo de seguridad de un sistema informático? ¿Una *password*? ¿Un candado contra robo (físico)? ¿Un *firewall*? ¿Un sistema criptográfico de llave pública?

Esta vaga redacción sin duda traerá innumerables problemas de interpretación a la hora de que le toque a un juez analizar un caso concreto.

La magnitud de los daños ocasionados por estas conductas depende de la información que se vulnere, al grado que se puede tener un fuerte impacto en el desarrollo de la economía, en la seguridad nacional o en las relaciones comerciales.

4.4.1 PROPUESTA PARA MODIFICAR EL TEXTO DEL CAPÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL SOBRE DELITOS INFORMÁTICOS

En ese mismo orden de ideas y en el entendido de que el tema de delitos informáticos nombrados así por la doctrina, es complejo, procedemos a presentar nuestra propuesta la cual propone adicionar un numeral mas al artículo 211 bis del Título Noveno capítulo II del Código Penal Federal con el fin de hacer mas específico el contenido de este, incluyendo definiciones que serán de vital importancia en el momento en que el juez llegue a decidir si el caso concreto que analiza está tipificado en la ley.

Todos son términos técnicos que se pretendió definir de la manera más amplia posible para evitar que con el avance tecnológico vertiginoso de hoy en día, queden obsoletos en un corto tiempo.

En la fracción I, se incluye dentro de la definición de "computadora", de manera indirecta o genérica, al Internet y redes privadas.

En la fracción II se copió la definición de "programa de computación" del artículo 101 de la Ley Federal del Derecho de Autor.

En la fracción III fueron incluidos elementos básicos que se busca tener tanto en los documentos electrónicos como en las comunicaciones: integridad, confidencialidad y disponibilidad.

En la fracción IV se encuentra la definición del principal bien jurídico protegido: la información. Se usó el lenguaje actualmente contemplado por las reformas publicadas en el Diario Oficial de la Federación el 29 de Mayo del año 2000.

En la fracción V se corrige uno de los principales defectos del actual Código Penal Federal, ya que no incluye una definición de "mecanismo de seguridad". Esta frase puede tener muy diversas acepciones según el especialista que la interprete, si no se cuenta con una guía o definición apropiada.

Al incluir el término "dispositivo físico y/o electrónico, programa de cómputo" se cubre la posibilidad de que el mecanismo de protección consista en un elemento de *hardware* y/o de *software*, tal como ocurre en la realidad.

Se contemplan los propósitos principales de cualquier *firewall*: proteger una computadora o red de computadoras en contra de accesos externos no autorizados, como el borrado o alteración de información, ataques informáticos diversos, etc. Además, se distingue uno de los objetivos fundamentales de un sistema criptográfico asimétrico (el cual también puede ser un "mecanismo de seguridad"): el no repudio del emisor o receptor.

Como ventaja adicional, se clarificó que también se entiende por el referido término "cualquier dispositivo para proteger programas de cómputo", lo cual es un golpe directo en contra de la piratería de *software*.

En la fracción VI se incluye un término derivado del bien jurídico protegido que hablábamos con anterioridad, la "información". De manera indirecta, la definición también busca proteger otro bien jurídico distinto, éste recae directamente en la persona: el derecho a la privacidad e intimidad.

ARTÍCULO 211 bis 1.- Para los efectos de este título se entenderá por:

I.- Computadora(s): máquina, aparato, dispositivo, sistema o equipo de informática, ya sea electrónico, óptico, magnético, o de cualquier otra tecnología, que realice funciones lógicas, aritméticas, transmisión o de almacenamiento de datos, así como para el tratamiento sistemático de la información mediante el procesamiento automático de datos electrónicos o de cualquier otra tecnología. Este término también incluye las redes públicas o privadas de computadoras.

II.- Programa(s) de cómputo o computación: la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

III.- Daño: deterioro o menoscabo a la integridad, confidencialidad y/o disponibilidad de datos, información, programas de cómputo, o computadoras.

IV.- Información: archivos o datos contenidos y/o transmitidos a través de una computadora, o por medios electrónicos, ópticos o de cualquier otra tecnología.

V.- Mecanismo de seguridad: dispositivo físico y/o electrónico, palabra clave, código de acceso, programa de cómputo o equipo informático que tenga por objetivo proteger una computadora, un programa de cómputo y/o la información contenida en una computadora, sistema o equipo informático de o contra:
a) accesos internos o externos no autorizados;
b) borrado, alteración o daño de información;
c) ataque informático de cualquier índole.
d) repudio del emisor o receptor de la información.

También se entenderá por mecanismo de seguridad, cualquier dispositivo técnico utilizado para proteger un programa de cómputo contra su copiado, distribución o uso ilícito.

VI.- Datos o información personal: Cualquier información relacionada a una persona física identificada o identificable. Los datos personales usualmente contienen información que directa o indirectamente puede ser relacionada o ligada a una persona física en particular.

Por último hay que enfatizar que al incluir en este artículo un numeral mas correspondiente al capítulo II de dicho ordenamiento, los numerales restantes sólo se recorrerían por lo que el capítulo tendría un numeral mas, quedando de la siguiente manera:

Artículo 211 bis 1 contemplaría las definiciones de los términos utilizados dentro del mismo capítulo; es decir, nuestra propuesta.

Artículo 211 bis 2 hace referencia al acceso ilícito más robo y daño de información.

Artículo 211 bis 3 hace referencia al acceso ilícito más robo y daño a la información del Estado.

Artículo 211 bis 4 hace referencia al robo y daño de información del Estado

Artículo 211 bis 5 hace referencia al acceso ilícito más robo y daño a la información del Sistema Financiero.

Artículo 211 bis 6 hace referencia al robo y daño de información del Sistema Financiero.

Artículo 211 bis 7 hace referencia acerca del Sistema Financiero.

Artículo 211 bis 8 se refiere al aumento de penas para este tipo de delitos.

CONCLUSIONES

Primera.- El panorama de este nuevo fenómeno tecnológico en las sociedades modernas como son los llamados delitos informáticos ha llegado a sostener que la Informática es hoy una forma de Poder Social.

Las facultades que este fenómeno pone a disposición de Gobiernos y de particulares, configuran un cuadro de realidades de aplicación y de posibilidad de acciones lícitas e ilícitas, en donde es necesario el derecho para regular los múltiples efectos de una situación, en el medio social.

Segunda.- Las aplicaciones de la informática no sólo tienen un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Tercera.- Esto ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables; la manipulación fraudulenta de los ordenadores con fin de lucro, en especial de carácter patrimonial, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

Cuarta.- En el desarrollo de éste tema, se refleja el Atraso de la Ley Penal Mexicana en la parte especial y en lo procesal en relación al vertiginoso avance que caracteriza a la denominada Internet (International Network) y a las diversas herramientas virtuales que son creadas para vestir y actualizar cada año a dicha invención, que se ponen a disposición y servicio de millones de usuarios a nivel mundial y por consecuencia, desafortunadamente se constata dicho atraso, si se le compara inevitablemente con las leyes penales que se están implementando a nivel internacional para describir y combatir los llamados Cyberdelitos o Delitos Informáticos.

Quinta.- Una vez que se cobre conciencia sobre la complejidad del tema y de las dificultades procesales que se presentan en México, para poder comprobar objetivamente los llamados "delitos informáticos" contenidos en la plausible pero insuficiente reforma penal del 17 de mayo de 1999, y si a esto le incluimos las muchas interpretaciones que se pueden tener por no tener bien delimitado los contenidos en dicho ordenamiento trae como consecuencia que en el momento de que se presente un caso contenido en los numerales del artículo 211 del Código Penal Federal, el juez no tenga los argumentos necesarios para poder interpretar y establecer de forma concreta lo que se debe entender por ejemplo por un mecanismo de seguridad.

Sexta.- Para que un país dictamine y penalice un delito, el gobierno de ese país debe tener la gente preparada y especializada para estos casos, por el cual si no existiera el personal adecuado, provocaría la corrupción en la leyes.

Séptima.- Indudablemente se desprende la necesidad de un mayor trabajo jurídico con relación a los Delitos Informáticos, la trascendencia y evolución constantes de los mismos requiere un estudio arduo llevado a cabo no solo por los abogados, sino por peritos en materia de informática.

Octava.- Del propio análisis se deduce que no es necesario esperar a la reforma penal para comenzar a reprimir algunas conductas delictivas relacionadas con los medios tecnológicos de la informática, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática.

Novena.- La complejidad del tema podría parecer contradictoria al enfatizar por una reforma integral. Debido a esta situación es importante considerar que para conseguir una prevención efectiva de la criminalidad informática se requiere:

En primer lugar que los términos a los que se hace referencia no sean de una gran magnitud, es decir, no tan generales como lo establece el Código Penal.

En segundo lugar que se tenga el personal apropiado encargado de la procuración, administración e impartición de justicia para atender e investigar, por lo que se estaría avanzando mucho en el camino de la lucha contra este tipo de conductas ilícitas derivadas de la informática, que cada día tiende a expandirse más.

De igual manera, es necesario el establecimiento de programas de capacitación especializados en el tema, para los Agentes del Ministerio Público y Jueces, impulsar la creación de plazas para los peritos en informática como auxiliares de las Procuradurías de Justicia Federal o Estatales, autorizaciones y certificaciones especiales para los Ingenieros en Informática o en Sistemas para que como peritos autorizados, auxilien a los abogados postulantes independientes y Jueces, así como procurar la celebración de tratados internacionales mediante los cuales, entre países, se convenga el auxilio mutuo para combatir y sancionar los comportamientos ilícitos por el ilegal aprovechamiento del Internet y sus herramientas virtuales.

Décima.- Para concluir con esta aproximación a un tema de gran interés y de preocupación, se puede señalar que las acciones generadas por el uso indebido de la Informática, están relacionadas con figuras convencionales tales como el robo, fraude, sabotaje, piratería, pornografía, falsedad, entre otros, con el auxilio de medios informáticos. Por lo que consideramos apropiado adecuar los tipos penales existentes a la posibilidad de que la comisión del ilícito sea realizado teniendo como medio la informática y las comunicaciones existentes.

Estando por consiguiente, en contra de aquellas personas que son de la opinión de tener contemplados los delitos informáticos de forma autónoma en sus leyes. Por el contrario sería conveniente agregar a las figuras delictivas existentes en los códigos, adecuaciones o figuras nuevas ubicadas a continuación de los delitos convencionales con que puedan tener relación, o bien, incluyéndolas como modalidades agravadas de las ya previstas según sea el caso.

Por último, es importante mencionar que las necesidades planteadas por esta posición de incluir un numeral mas al artículo 211 del Código Penal, no debe ser entendido a la ligera, sino por el contrario es un esfuerzo encaminado a su uso lícito y pacífico, sin dejar a un lado el que se debe poner especial atención a la vanguardia legislativa que se está impulsando a nivel internacional para el combate de los llamados delitos informáticos.

Por todo lo anterior se concluye que, la hipótesis planteada al inicio de la investigación ha sido comprobada con el sustento legal y la información obtenida dentro de la misma investigación.

GLOSARIO DE TERMINOS

- @ arroba (en inglés "at").
En las direcciones de correo electrónico separa el nombre del usuario de la identificación de su proveedor de correo electrónico.

- ADSL
Asymetric Digital Suscriber Line es una modalidad que permite conexión usando fibra óptica telefónica con una velocidad de subida de hasta 128 Kbps y una de bajada mucho mayor, de hasta 1.500

-ARPANET
Advanced Research Projects Agency Network. Red militar fundada por la agencia de investigación del gobierno norteamericano, pionera en la comunicación a través de líneas telefónicas que posteriormente generó Internet.

-Broadband
Termino utilizado para definir conexiones superiores a la máxima velocidad modem (56 Kbps) tales como ISDN 128 Kbps DSL 128 a 350 Kbps ADSL 128 de subida ya hasta 1.500 Kbps de bajada SDSL 300 a 1.500 de subida y bajada T1 1.500 Kbps dedicados T3 3.000 Kbps

-Chat
Charla. Servicio de Internet que permite que dos o más usuarios conversen online mediante el teclado.

-Ciberespacio
Denominación inventada por el escritor de ciencia ficción William Gibson que se refiere al espacio virtual en el que se reúnen las personas a través de Internet.

-Computadora
Ordenador. En Hispanoamérica se utiliza la palabra computadora, derivada del inglés computer, para designar a los ordenadores.

-Control
Ninguna persona, compañía, institución u organización es dueña de Internet, ni tampoco la gobierna, o incluso tiene interés controlante.

-Cortafuegos (FIREWALL)
Es un ordenador o un programa que conecta una red a Internet pero impide el acceso no autorizado desde Internet.

Mecanismo que permite que las comunicaciones entre una red local e Internet se realicen conforme a las políticas de seguridad de quien los instala. Estos sistemas suelen incorporar elementos que garantizan la privacidad, auntentificación, etc., con lo que se impide el acceso no autorizado desde Internet.

-Cracking / 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.

-Criptografía
Técnica orientada a proteger a la información de posibles modificaciones y usos no autorizados mediante la utilización de algoritmos matemáticos complejos para la transformación de la información en un extremo de la comunicación y la realización del proceso inverso en el otro extremo.

-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, etc. 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. Pakistán tiene un centro educacional terrorista de guerra informática, supuestamente con base en Londres. Algunos grupos árabes han denominado al Internet como "un arma a ser dominada".

-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 R.U., 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.

DNS: Domain Name System
Sistema de Nombres de Dominio. Sistema de denominación de Hosts en Internet.

-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.

-Download
Proceso que consiste en traer un archivo desde algún lugar de la red y guardarlo en la computadora del usuario

- DSL
Digital Suscriber Line es una modalidad que permite conexión usando fibra óptica telefónica a velocidades entre 128 y 358 Kbps

-DVC
Una videoconferencia en la que se comunican dos usuarios PC a PC con cámaras. Es la modalidad mas económica, puede realizarse por conexión modem a 56 Kbps, aunque la calidad de sonido e imagen hace aconsejable una conexión de broadband o alta velocidad, ISDN o DSL, a partir de 128 Kbps

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 modem, 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.

-E-mail o Correo Electrónico
Es un sistema de transmisión de mensajes escritos a través de Internet. El correo electrónico o e-mail debe estar amparado por la garantía de la libertad de expresión.

-Extranet
Unión de varias intranet para que las empresas puedan compartir información.

-Firma digital
Información añadida o transformación cifrada de los datos que permite al receptor de los mismos comprobar su fuente e integridad y protegerse de tal modo de la suplantación o falsificación.

-Fraudes informáticos
Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)

-FTP
File Transfer Protocol, una de las formas de transmitir datos a un server

-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".

-HTTP (hipertext transfer protocol)
Protocolo de transferencia de hipertexto) permite la vinculación de documentos. Y un hipertexto, es una técnica o sistema de consulta de una base de textos que permite saltar de un documento a otro según caminos preestablecidos o elaborados con ese fin.

-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.

-Información
Elemento fundamental que manejan los ordenadores en forma de datos binarios. Tras la revolución industrial, se habla de la revolución de la información, que se ha convertido en el mayor valor de las empresas y de las personas. El auge, proliferación y universalización de sistemas de interconexión global como Internet, ha llevado a hablar de la sociedad de la información como el nuevo paradigma del mundo en que vivimos.

Factor cualitativo que designa la posición de un sistema, y que eventualmente es transmitido por este sistema a otro.

-Informática
Ciencia que estudia el tratamiento automático y racional de la información, a través de los ordenadores. Este termino se refiere a lo mismo que computación, solo que informática tiene origen francés y computación origen ingles.

-Internet
Conjunto de redes de ordenadores creada a partir de redes de menos tamaño, cuyo origen reside en la cooperación de dos universidades estadounidenses. Es la red global compuesta de limes de redes de área local (LAN) y de redes de área extensa (WAN) que utiliza TCP/IP para proporcionar comunicaciones de ámbito mundiai a hogares, negocios, escuelas y gobiernos.

Red internacional que utilizan los protocolos TCP/IP y que poseen mas de diez mil redes enlazadas. Esta compuesto, por tantos, por un conjuntos de redes locales conectadas entre si por medio de un ordenador llamado GATEWAY que se encuentra en cada red.
Lo diferentes GATEWAY se encuentran interconectados entre sí por diferentes medios (fibra óptica, línea telefónica, etc.). La información que se debe mandar aun ordenador remoto es etiquetada con la dirección computarizada de dicho ordenador esta dirección puede tener diferentes formatos. Una vez que la información a sido etiquetada, esta sale de la red donde se ha creado a través de la puerta (GATEWAY). Apartir de ahí va siendo encaminada de puerta a puerta hasta llegar a la red local, donde figura el ordenador de destino. No existe ningún ordenador central que controle todo el entramado de la red y que dirija los flujos de información dentro de ella.

-Intranet
Asociación de redes dentro de una empresa, sin acceso publico. Permite a los empleados compartir datos corporativos.

Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet. Una red de equipos que es interna a una organización y es compatible con aplicaciones de Internet, especialmente el WWW. La mayoría de las intranet están configuradas de forma que sus usuarios puedan tener acceso a Internet sin permitir que los usuarios de Internet tengan acceso a los equipos de la Intranet.

- IP
La abreviatura de Internet Protocol, que es la "dirección" o "identidad" de un determinado ordenador para otros. Adicionalmente, existe una conexión por TCP que contacta a dos host y les permite intercambiar no ya paquetes sino flujos de datos. Matrícula que identifica a un ordenador de la red. A los ordenadores personales se les asigna una IP adress para que naveguen por la red, que cambia en cada sesión de acceso a Internet.

- ISDN
Integrated Services Digital Network, una modalidad de conexión que permite velocidades de transmisión de 128 Kbps (miles de bits por segundo), que funciona compartiendo las lineas de transimisión de teléfonos digitales.

-ISP
(Internet Service Provider). Proveedor de Servicios Internet.

Empresa dedicada a prestar servicios de conexión a Internet basada en una cuota mensual.

-LAN
(Local Area Network). Red de área local. El término LAN define la conexión física y lógica de ordenadores en un entorno generalmente de oficina. Su objetivo es compartir recursos (como acceder a una misma impresora o base de datos) y permite el intercambio de ficheros entre los ordenadores que componen la red. Los servidores son máquinas de alta velocidad que contienen programas y datos que comparten todos los usuarios de redes. Las estaciones de trabajo, o clientes, son los computadores personales de los usuarios, que realizan procesamiento autónomo y tienen acceso a los servidores de la red según se requiera.

- Performance
Definimos performance como: 1. El nivel de desempeño aplicado a tareas de individuos, grupos u organizaciones 2. El resultado economico de ese desempeño 3. El impacto a largo plazo de ese resultado para la organización, sus clientes y medio ambiente. La formación online puede estar asociada a la performance (eLearning centrado en desempeño), ser parte de ella (EPSS, ePerformance, FAQ, ayudas de tareas, plataformas de trabajo virtual) o estar limitada al aprendizaje.

-Phreaking / 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.

-Programa
1. Redacción de un algoritmo en un lenguaje de programación.
2. Conjunto de instrucciones ordenadas correctamente que permiten realizar una tarea o trabajo específico.
3. Toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.
4. Conjunto secuenciado de instrucciones que quedan escritas en un lenguaje determinado con unos fines específicos. Aunque en el lenguaje común con frecuencia se denomina programa al sistema operativo, la diferencia estriba, precisamente, en la especificidad de aquél frente al carácter de gestión global de éste. La palabra software engloba ambos.

-Programación
Programar es automatizar y definir una serie de procesos para resolver un problema y obtener un resultado final. Un programa es el conjunto de instrucciones que se le dan al ordenador para resolver un problema o tarea determinada. Consiste en proporcionar a un equipo un conjunto de instrucciones (o sentencias) que deben ser ejecutadas en orden, y que proporcionan una salida. Preparación de los datos previos indispensables para obtener la solución de un problema mediante las instrucciones codificadas de un ordenador. Lenguaje de Programación Se utilizan para indicar al ordenador las acciones que ha de realizar para resolver un determinado problema. Básicamente los lenguajes de programación se componen de ordenes (en adelante llamadas instrucciones) que es lo que en si mismo le dice al ordenador lo que tiene que hacer. Un conjunto de esas instrucciones forman el programa.

-Programador
Persona que diseña, escribe y/o depura programas de ordenador o computadora, es decir, quien diseña la estrategia a seguir, propone las secuencias de instrucciones y/o escribe el código correspondiente en un determinado lenguaje de programación.

-Programadores de Virus
Personas que programan códigos con la intención de:
Que se reproduzcan por sí mismos en otros sistemas sin ningún tipo de autorización.
Que tengan efectos secundarios convertidos en un mensaje para el operador del sistema, una travesura o guiño, o en el peor de los casos, daños irreparables para el sistema.

-Protocolo
Se denomina protocolo a un conjunto de normas y/o procedimientos para la transmisión de datos que ha de ser observado por los dos extremos de un proceso comunicacional (emisor y receptor). Estos protocolos «gobiernan» formatos, modos de acceso, secuencias temporales, etc.

-Proxy
Es un programa que realiza la tarea de encaminador, utilizado en redes locales, su función es similar a la de un router, pero es injustificable el gasto en redes locales.

-Sabotajes Informáticos
Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos.

-SDSL
Symmetric Digital Suscriber Line es una modalidad que permite conexión con una velocidad de subida y bajada de entre 128 y 1.500 Kbps

-T1
T1 es un circuito de alta velocidad de transmisión que transmite 1.544 Kbps (miles de bits / segundo), habitualmente sobre una línea dedicada. Es la norma de uso para grandes empresas en videoconferencias.

- TCP
Transmission Control Protocol, el código que permite a dos hosts intercambiar flujos de datos

-Videoconferencia
La comunicación entre dos puntos utilizando video y sonido La Videoconferencia se divide en diferentes variantes: DVC Desktop Videoconferencing Set Top Videoconferencing Rollabout videconferencing Meeting Rooms

-Virus
Conjunto de instrucciones, programáticas o de otro tipo que, merced a su capacidad de autoduplicarse, se propagan a través de redes y/o sistemas informáticos generando algún tipo de daño o molestia.

-Webmaster
Persona responsable de la creación, administración, programación y control técnico de un sitio web.

-Worm
Gusano. Tipo de programa, similar a un virus, que se distribuye en red y tiene como objetivo afectar el funcionamiento de las computadoras a las que ingresa.

-Web o World Wide Web
Red de alcance mundial. Subconjunto de Internet consistente en la asociación global de computadoras interconectadas que trabajan sobre una colección de documentos usando un protocolo especifico de Internet (el HTTP) para el intercambio de información.

BIBLIOGRAFÍA

ABARCA, Ricardo, *Derecho Penal,* Ed. Jus, Tomo I sexta ed. México, 1947.

ABARCA, Ricardo, *El Derecho Penal en México,* Ed. Jus, primera ed. México, 1989.

BARRIOS, Gabriela, MUÑOZ DE ALBA, Marcia, y PÉREZ BUSTILLO, Camilo. *Internet y Derecho en México*, Ed. McGraw Hill, México, 1998.

BEER, Stafford. *Cibernética y Administración*, Ed. Nacional, México, 1965.

CARRACOSA LÓPEZ, Valentín,, citado por FIX FIERRO, Héctor, *Informática y Documentación Jurídica*, UNAM, Facultad de Derecho, México, 1990.

CASTELLANOS TENA, Fernando Lineamientos elementales de Derecho Penal Ed. Porrúa decimooctava ed. México, 1986.

CISNEROS FARÍAS, German. *Teoría del derecho,* Ed. Trillas, segunda ed. México, 2000.

COROMINAS, Joan. *Breve diccionario Etimológico de la lengua castellana,* Madrid, 1983.

CORREA, Carlos, *Derecho Informático, Ed. Depalma, Buenos Aires, 1987.*

CRÍCKET LIU, Jerry Peek, RUSS Jones; BRUS Bryan y NYE Adrián, *Administración de Servicios de Información.* Ed. Prentice Hall, segunda ed. México, 1998.

CUELLO CALÓN, Eugenio, *Derecho Penal,* Ed. Bosch, Tomo I, cuarta ed, Barcelona, 1937.

DE LA CUESTA AGUADO, Paz. *Tipicidad e imputación objetiva,* Ed. Tirant lo Blanch. Valencia. 1996. Cita referida por ZAMORA JIMÉNEZ, Arturo.

FIX FIERRO, Héctor, *Informática y Documentación Jurídica,* UNAM, Facultad de Derecho, México, 1990.

FROSINI, Vittorio, *Informática y Derecho*, Ed. Temis, Colombia, 1988.

GUTIERREZ Y GONZÁLEZ, Ernesto. *Derecho Sucesorio, Inter-vivos y mortis causa,* Ed. Porrúa, tercera ed. México, 1998.

HANCE, Oliver, leyes y Negocios en Internet, Ed. Mc Gras Hill, México, 1986.

JESCHECK, HANS Heinrich, *Tratado de Derecho Penal,* Ed. Irla, Tomo I tercera ed. Barcelona 1978.

JIMÉNEZ DE ASÚA, Luis, *La Ley y el Delito,* Ed. Hermes, México, 1986.

JIMÉNEZ DE ASÚA, Luis, Lecciones de Derecho Penal, Ed. Harla, México Vol. 7 1998.

LA TORRE, Ángel, *Introducción al Derecho,* Ed. Ariel, Barcelona, 1999.

LIVAS, Javier. *Cibernética, Estado y Derecho,* Ed. Gernika, México, 1988.

LÓPEZ BETANCOURT, Eduardo, *Introducción al Derecho Penal,* Ed. Porrúa, México, 2001.

LOSANO, Mario G, *Curso de Informática Jurídica,* México, 1965.

MAGGIORE, Giusseppe, *Derecho Penal,* Tomo II, Ed. Temis, Bogotá, 1989.

MANCILLA OVANDO Jorge Alberto, Teoría Legalista del Delito, Ed. Porrúa, México 1999.

Maurach, Tratado de Derecho Penal, Tomo II, Ed. Ariel, Barcelona, 1972.

MORA, José Luis y MOLINO, Enzo. *Introducción a la Informática,* México, 1974.

MOTO SALAZAR, Efrain, *Elementos de Derecho,* Ed. Porrúa, México, 2002.

PALLARES, Jacinto, citado por RAMÍREZ SÁNCHEZ, Jacobo, *Introducción al Estudio del Derecho Civil.* Ed. Textos Universitarios UNAM, segunda ed. México, 1997.

RECASÉNS SICHES, Luis. *Introducción al Estudio del Derecho.* Ed. Porrúa, tercera ed. México, 1968.

RECASÉNS SICHES, Luis, citado por CISNEROS FARÍAS, German. *Teoría del Derecho,* Ed. Trillas, segunda ed. México, 2000.

RECASÉNS SICHES, Luis, citado por CISNEROS FARÍAS, German. *Teoría del Derecho,* Ed. Trillas, segunda ed. México, 2000.

RIOS ESTAVILLO, Juan José. *Derecho e Informática en México.* UNAM, México, 1984.

ROMERO Casabona, *Poder Informático*, Ed. Tecnos, Madrid, 1994.

SUÑÉ, Emilio, *Introducción a la Informática Jurídica y al Derecho Informático*, Ed. Monográfico, Madrid, 1986.

TÉLLEZ VALDEZ, Julio, *Derecho Informático*, Ed. Mc Graw Hill, segunda ed. México, 1996.

VILLORO TORAZO, Miguel, *Introducción al Estudio del Derecho*, Ed. Porrúa, México, 1975.

ZAMORA JIMÉNEZ, Arturo. *Cuerpo del Delito y tipo penal*, Ed. Angel México, 1999.

LEGISLACIÓN

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Instituto Federal Electoral, México 2004.

CÓDIGO PENAL FEDERAL. Agenda Penal del DF. Ed. Isef, México 2004.

LEY FEDERAL DEL DERECHO DE AUTOR. En Legislación sobre Derechos de Autor. Colección Porrúa, México, 2004.

LEY FEDERAL DE TELECOMUNICACIONES. Colección Porrúa, México 2004.

LEY DE FOMENTO Y PROTECCIÓN DE LA PROPIEDAD INDUSTRIAL. Colección Porrúa, México, 2004.

CÓDIGO PENAL PARA EL DISTRITO FEDERAL Agenda Penal del DF. Ed. Isef, México 2004.

CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEON. Ed. Sista, México 2003.

CÓDIGO PENAL PARA EL ESTADO DE SINALOA. Ed. Sista, México 2005.

CÓDIGO PENAL PARA EL ESTADO DE MORELOS. Ed. Sista, México 2004.

CÓDIGO PENAL PARA EL ESTADO DE TABASCO. Ed. Mc Graw Hill. 2004.

PÁGINAS DE INTERNET

http://geocities.com
http://www.servitel.es/atv/ayu/INTERNET/DICCIO/diccio.htm
http://www.geocities.com/teoríadeldelito/ y http://www.lexisnexis.cl/
http://tiny.uasnet.mx/prof/cln/der/silvia/inducc.htm
http://www.cft.gob.mx/html/5_est
http://tiny.uasnet.mx/prof/cln/der/silvia/define.htm
http://tiny.uasnet.mx/prof/cln/der/silvia/activo.htm
http://tiny.uasnet.mx/prof/cln/der/silvia/pasivo.htm
http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml
http://tiny.dasnet.mx/prof/cm
http://www.kriptopolis.com.
www.argentinajuridica.com
http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml
http://tiny.uasnet.mx/prof/cln/der/silvia/lexis.htm
http://tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm
http://www.ssp.gob.mx/_c_programas/p_cibernetica/INDEX.htm

HEMEROGRAFÍA

CALLEGARI, Lidia, Delitos Informáticos y Legislación Revista Facultad de Derecho y Ciencias Políticas Universidad Pontificia Boliviana Medellín, Colombia. No. 70 julio-agosto-sep, 1985 p.115.

Diccionario Jurídico Mexicano Ed. Porrúa, UNAM, México 1994
Articulo 19 de la Declaración Universal de los Derechos del Hombre de 1948.

LIMA DE LA LUZ,María, Delitos Electrónicos Revista Criminalia, Ed. Porrúa Academia Mericana de Ciencias Penales México D. F No. 1-6 año I ., enero-junio 1984 P. 100.

PÉREZ LUÑÓ, Antonio Enrique, Ensayos de Informática Jurídica Fontamara-ITAM, Colección Biblioteca de Ética, Filosofía del Derecho y Política No. 46 México, 1996. p. 17.