



UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
"ARAGÓN"

"ANÁLISIS SOBRE EL REORDENAMIENTO DE LOS
DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL
FEDERAL MEXICANO"

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

ASESOR:
DR. BERNABÉ LUNA RAMOS



BOSQUES DE ARAGÓN, ESTADO DE MÉXICO, 08 DE
AGOSTO DE 2013.



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

ÍNDICE

Exposición de motivos	1
Capítulo I. La informática en general.	4
1.1 Antecedentes y evolución.	4
1.2 Nociones y concepto.	15
1.3 Características generales de la informática.	20
1.4 Informática jurídica en general.	37
Capítulo II .Protección jurídica a los programas de computación.	54
2.1 Antecedentes y evolución del problema.	54
2.2 Nociones fundamentales.	62
Capítulo III. Delitos informáticos.	67
3.1 Orígenes.	67
3.2 Concepto.	68
3.3 Características.	73
3.4 Clasificación.	76
3.5 Riesgos informáticos.	82
3.6 Régimen Jurídico aplicable.	90
3.6.1 La vía patentaria.	90
3.6.2 La vía autoral.	92
3.6.3 La vía civil.	94
3.6.4 La vía penal.	95
3.7 Situación Internacional.	96
3.7.1 Alemania.	97
3.7.2 Austria.	97
3.7.3 Chile.	98
3.7.4 Estados Unidos.	98
3.7.5 España.	99
3.7.6 Francia.	99
3.7.7 Inglaterra.	100
3.7.8 Holanda.	100
3.7.9 Italia.	101
3.8 Organización de las Naciones Unidas.	102
3.9 Manual de la ONU para erradicar delitos informáticos.	104
Capítulo IV. Análisis jurídico de los elementos del tipo penal en los delitos informáticos.	107
4.1 Elementos generales.	108
4.1.1 Sujeto activo.	108
4.1.2 Sujeto pasivo.	108

4.1.3 Bien Jurídico.	119
4.1.4 Objeto Material.	110
4.1.5 Conducta.	110
4.1.6 Resultado.	110
4.2 Elementos especiales.	111
4.2.1 Referencias Temporales.	111
4.2.2 Referencias espaciales.	112
4.2.3 Referencias ocasionales.	112
4.2.4 Medios de comisión.	112
4.2.5 Elementos subjetivos.	113
4.2.6 Elementos normativos.	113
4.3 Elementos de calidad.	114
4.3.1 Sujeto activo.	114
4.3.2 Sujeto pasivo.	114
4.3.3 Objeto material.	115
4.4 Elementos de cantidad.	115
4.4.1 Sujeto activo.	115
4.4.2 Sujeto pasivo.	115
4.4.3 Objeto material.	116
4.5 Análisis del tipo penal en los delitos informáticos	116
4.5.1 Sujeto activo y sujeto pasivo.	116
4.5.2 Objeto material y bien jurídico.	119
4.5.3 Conducta y resultado.	120
4.5.4 Elementos normativos y subjetivos.	121
Capítulo V. Análisis sobre el reordenamiento de los delitos informáticos en el	
Código Penal Federal Mexicano.	123
5.1 Delitos informáticos en el Código Penal Federal.	123
5.2 Crítica al Capítulo II Título Noveno y Título Vigésimo Sexto del Código Penal Federal Mexicano.	127
Conclusiones	136
Fuentes de consulta	152

EXPOSICIÓN DE MOTIVOS

La exigencia de una reglamentación imperativa o coercitiva de las relaciones humanas aparece en el momento en que surgen los grupos, las familias, las tribus, entre otros. Así, el derecho, es producto de la organización social consubstancial al hombre en cuanto éste no puede prescindir de su relación con los demás cuando ha avanzado cierto grado de evolución.

Posteriormente, surge de la misma inquietud racional del hombre, "la informática", ante la cada vez más creciente necesidad de información para una adecuada toma de decisiones. A lo largo de la historia, el mundo ha sufrido diversas revoluciones tecnológicas relacionadas con la información, que ha repercutido en tal forma que han transformado y reorganizado la economía y la sociedad.

La informática es un fenómeno multifacético de la realidad contemporánea. Su difusión se ha extendido rápidamente sobre la economía, la política, la organización del trabajo y el derecho.

La amplia difusión de la tecnología informática ha llevado a la transformación de las estructuras industriales, además de sus significativos reflejos en la evolución política, económica, social y cultural, su impacto se traduce, en primer lugar, en la modificación o reemplazo de proceso y métodos de trabajo en la industria, controles más efectivos, incrementos en productividad, ahorro de energía, reducción en los ciclos de producción, mayor precisión y confiabilidad.

En la medida en que los ordenadores se han convertido en un elemento de la vida cotidiana, se advierte una multiplicación de los esfuerzos individuales y colectivos encaminados a hacer fluida la comunicación entre el mundo de las máquinas y el de los hombres. En particular se ha llevado a cabo una notable labor por parte de los sectores más actualizados de la ciencia y de la filosofía

jurídica para suscitar entre los juristas una "conciencia tecnológica", esto es, una actitud reflexiva, crítica y responsable ante los nuevos problemas que en las diversas esferas del acontecer social representa la tecnología, y ante los que el derecho no puede permanecer insensible.

Así, la difusión de la informática da origen a nuevas formas delictivas que utilizan los sistemas informáticos como medio comisivo, o bien, que tienden a aquellas en parte o en todo como su objeto. Si bien la aún incipiente difusión de la informática en América Latina no ha dado dimensión mayor a éste problema, es previsible que su importancia crecerá a medida que aquella progrese, en particular en el ámbito financiero.

El uso de las computadoras y su interconexión, ha dado lugar a un fenómeno de nuevas dimensiones: el delito instrumentado mediante el uso del computador.

La problemática de los delitos informáticos requiere un estudio especial en nuestro país, con vista a determinar un capítulo especial o único para la tipificación de éstos delitos, pues actualmente con las reformas al Código Penal Federal, específicamente en el Capítulo Segundo del Título Noveno llamado "Acceso ilícito a sistemas y equipos de informática", en mi opinión sería conveniente que se estableciera un capítulo nuevo llamado "DELITOS INFORMÁTICOS", en el que se contemplaran nuevos tipos penales y se reordenarán los ya existentes, con el fin de responder a las nuevas necesidades que la sociedad reclama, pues la informática es un fenómeno multifacético de la realidad contemporánea, que se ha extendido rápidamente sobre la economía, la política, la recreación, la organización del trabajo, y con ello además, en el derecho. De igual forma, la informática jurídica como instrumento orientado a optimizar la labor de los operadores del derecho, vive en nuestro país una intensa etapa de estudios e investigaciones.

Es por ello que en el tema a tratar en esta tesis, se propone que se reordenen los delitos informáticos en nuestra legislación penal. Los proyectos en

camino de ejecución orientados a la informatización en materia laboral, civil, comercial y penal, vinculados el primero y el último a la reforma de los pertinentes códigos de procedimientos, expresan la sostenida preocupación por incorporar efectivamente los adelantos que ofrece la informática a la administración de justicia.

CAPITULO I

LA INFORMÁTICA EN GENERAL

1.1 ANTECEDENTES Y EVOLUCIÓN

Desde épocas pasadas, el hombre ha tenido la necesidad de procesar datos y, en un principio, lo hizo de manera muy rudimentaria. La falta de elementos que le permitieran realizar los procedimientos para hacer cálculos, lo obligaban a operar mentalmente en la mayoría de los casos. Para contar, el hombre estaba limitado en un principio al número de sus dedos y después fue capaz de usar otros medios, como cuentas, granos u objetos similares.

La solución de casos de carácter cuantitativo motivó que se establecieran diversos métodos y sistemas; éstos auxiliaban al hombre para enfrentar los problemas matemáticos que él mismo se planteaba. Desarrolló sistemas abstractos tales como los numéricos y recurrió a elementos de ayuda como tablas, papel, entre otros. El manejo en conjunto de los sistemas numéricos y los medios de proceso permitieron al hombre resolver problemas matemáticos cada vez más elaborados.

La necesidad de equipos de cómputo ha existido durante siglos, las sociedades del pasado desarrollaron técnicas sencillas de cómputo sirviéndose de las tecnologías entonces disponibles. Una de las más antiguas fue el ábaco, que remonta sus orígenes a la antigua Babilonia.

“....De los antecedentes que se conocen hace 5,000 años en el Valle del Tigris-Eúfrates surgió un dispositivo, el cual consistía en una placa de arcilla con numerosas ranuras en la que se colocaban piedrecillas. Posteriormente, en el año 4,000 en Egipto se lograba el mismo dispositivo; 3,000 años a.c. los Babilonios empezaron a utilizar marcas en una tablilla cubierta de polvo en lugar de los dedos para contar. Estos dispositivos de cálculo trascendieron sus fronteras mediante

diversos procesos de difusión cultural llegando a China, Japón y Roma, en donde el ingenio de estas civilizaciones elevó el ordenador de piedrecillas a un alto nivel de desarrollo. Para ello, se perforaron las piedrecillas y se unieron en grupos de diez sobre un marco de alambre, también, utilizando hilos de diversos materiales sobre los cuales las piedras pudieran moverse con agilidad y rapidez, resultando una magnífica aceleración en las operaciones fundamentales de cálculo. Este dispositivo se conoce como ábaco, el cual aún se usa para demostrar los principios de conteo y la aritmética.

El desarrollo de una notación numérica que permitía el manejo rápido y preciso de datos constituyó un antecedente necesario de la era de las computadoras.

A medida que se fue incrementando la complejidad de los problemas, fue necesario inventar mejores sistemas y otros medios de proceso que permitieran resolverlos.

Uno de los primeros aparatos de cómputo fue inventado por el francés Blaise Pascal durante la década de 1640, conocida como Machine Arithmetique, en cuyo honor se llamó al lenguaje de programación "Pascal". Este dispositivo fue creado cuando Pascal contaba con tan sólo 19 años de edad, diseñado para ayudar a su padre, quien era recolector de impuestos del gobierno francés.

Esta máquina utilizaba una serie de ruedas de diez dientes en las que cada uno de los dientes representaba un dígito del 0 al 9. Las ruedas estaban conectadas de tal manera que podían sumar números haciéndolas avanzar el número de dientes correcto. Era una forma muy elemental de las sumadoras y constituyó otro paso en el camino para lograr los modernos aparatos de cómputo. A esta sumadora se le considera la primera máquina de cálculo construida por el hombre.

Sin embargo, la “Pascaline” (como se le conocía) fue un fracaso financiero, pues las máquinas construidas a mano eran costosas y además delicadas, Pascal era la única persona capaz de repararlas”.¹

Posteriormente, Gottfried Wilhelm Von Leibnitz, matemático alemán, perfeccionó el diseño de Pascal y creó un aparato de cálculo que podría llevar a cabo las cuatro operaciones aritméticas básicas.

Es de notar que antes de Pascal y de Leibnitz, el hombre necesitaba de lápiz y papel para realizar sus operaciones aritméticas. A través del tiempo, los adelantos tecnológicos industriales permiten la creación de nuevos mecanismos de proceso, facilitando esas tareas a los hombres.

“En 1804, Joseph Marie Jacquard perfeccionó el telar automático, construyó una máquina para tejer complicados diseños en telas. Mediante el uso de hoyos perforados en una serie de tarjetas conectadas, Jacquard pudo controlar el tejido de las telas. El telar automático “leía” el diseño codificado en las tarjetas y tejía la tela adecuadamente. Estas tarjetas codificadas fueron las antecesoras de las tarjetas perforadas que se utilizaron en las computadoras modernas. Su telar tuvo aceptación inmediata entre los propietarios de las fábricas de telas porque podían contratar trabajadores menos capacitados por menos dinero”.²

Mientras que a principios del siglo XIX en Inglaterra iba naciendo la computadora digital moderna:

“...El inventor inglés Charles Babbage preparó diseños de una calculadora mecánica automática, inventando una serie de máquinas como la de Diferencias, diseñada para solucionar problemas matemáticos complejos. Esta máquina operaba con 6 dígitos, realizando automáticamente cálculos científicos y astronómicos, mediante la solución de ecuaciones diferenciales de segundo orden

¹ Cfr. S. Tanenbaum, Andrew, “Organización de computadoras. Un enfoque estructurado”. Tercera edición. Editorial Prentice Hall. Pág. 16.

² Cfr. Long, Larry & Long, Nancy, “Introducción a las computadoras y el procesamiento de Información”. Cuarta edición, Editorial Prentice may, España, 1995, Pág. 34.

y otras operaciones complejas. Diez años más tarde inventa una máquina analítica, que resultó ser su mayor contribución a pesar de que nunca se terminó de construir por su complejidad y exigencias tecnológicas para su época. Esta máquina en su esquema general es equivalente a las computadoras modernas, pues incluía 5 recursos cruciales: un recurso de entrada de números (lectora de tarjetas perforadas), la facilidad para almacenar números (memoria), procesamiento de números (unidad de cálculo), unidad de control para dirigir la salida de números y un recurso de salida de números (salidas impresas y perforadas).

Muchos historiadores consideran a Babbage y su socia, la matemática británica Augusta Ada Byron (1815-1852), hija del poeta inglés Lord Byron, como los verdaderos inventores de la computadora digital moderna. Augusta Ada se convirtió en consejera de Babbage, tradujo sus trabajos y agregó extensas notas de pie de página propias. Sin embargo, a pesar de un trabajo de diez años, no pudo construir un modelo totalmente operativo, debido quizá a lo complicado de su diseño. Pero las ideas de Babbage fueron utilizadas por los ingenieros que construyeron las primeras computadoras.

En 1879, James Ritty inventa, junto con su hermano, la primera registradora. Su invento perforaba en el rollo de papel tantas columnas como teclas poseía. Al accionar una tecla, se hacía una perforación en el rollo; para conocer el total del dinero que había entrado a la caja, se extraía el papel de la máquina, se multiplicaba el número de perforaciones de una columna por la unidad que representaban; posteriormente se sumaban los productos para obtener los totales”.³

Enzo Molino comenta con más detalle la historia de las máquinas industriales a las de cálculo y posteriormente a las computacionales, en su libro “Introducción a la Informática”, al referir lo siguiente:

³ Cfr. Mora, José Luis y Enzo Molino. "Introducción A La Informática", 2ª impresión, Porrúa S.A., México, 1987. Pág.72.

“W.S. Burroughs exhibe públicamente, en 1884, su primera máquina sumadora impresora accionada por teclas, enfocada a realizar trabajos de contabilidad, la patenta en 1888, y, en 1889, comienza a ser explotada comercialmente.

El pionero del procesamiento de datos fue sin duda el estadístico Herman Hollerith, quien en 1888 inventó un sistema para representar diversos datos de personas o cosas específicas en tarjetas perforadas y procesadas posteriormente. Y una vez construida su máquina, el doctor Hollerith se dio a la tarea de procesar los datos del censo que se llevó a cabo en Estados Unidos en 1890; dicho censo se completó en tres años y no en once como se había estimado inicialmente.

Como se puede apreciar, a fines del siglo XIX y principios del XX, el desarrollo y mejoramiento de las máquinas calculadoras y registradoras accionadas mediante teclas, marcan un avance importante en el desarrollo del procesamiento de datos.

Jay Monroe y Baldwin construyen una máquina calculadora de teclado en 1912, siendo el resultado de la evolución de otras calculadoras creadas en años anteriores. En 1920, aparecen las máquinas de contabilidad, éstas se caracterizaron por su capacidad para realizar funciones como registrar, calcular y resumir.

El Dr. Howard Aiken desarrolló por otra parte, a principios de los años 40's, en la Universidad de Harvard y con apoyo de IBM, otros proyectos para el diseño de un equipo de cómputo, la Mark I. Construyó un enorme equipo que medía 17 metros de longitud y 2.5 de altura, contaba con una serie de calculadoras electromecánicas y en muchos aspectos similares a la máquina analítica de Babbage. Tenía 72 palabras de 23 dígitos decimales para cada una y un ciclo, es decir, el tiempo de instrucción, de 6 segundos. Para la entrada y salida utilizaba cinta de papel perforada. Cuando terminó de construir su segunda máquina, llamada Mark II, había comenzado la era de la electrónica, por lo que los relevadores ya eran obsoletos.

El alemán Konrad Zuse, en 1941, en Berlín, realizó la primera computadora puesta en condiciones de funcionamiento. Construyó una serie de calculadoras

automáticas usando relevadores (relays) electromagnéticos, Zuse no tenía el conocimiento de la tecnología de Babbage ni de Hollerith; sus máquinas fueron destruidas por el bombardeo aliado sobre Berlín en 1944. De modo que su trabajo no tuvo influencia en máquinas posteriores, sin embargo, se le considera como uno de los pioneros en este campo”.⁴

En la evolución de las computadoras, se clasifican en cuatro generaciones que se diferencian por sus componentes electrónicos. Los bulbos o tubos al vacío se usaron en la primera generación, los transistores en la segunda que podían contener cientos de componentes electrónicos, los circuitos integrados (CI) en la tercera que podían contener miles de componentes y, los chips integrados a gran escala (LSI), a muy gran escala (VLSI) en la cuarta que pueden contener hasta millones de componentes electrónicos. Estas generaciones serán explicadas a continuación.

La primera generación de computadoras (1941-1953) se caracterizó por el uso de válvulas electrónicas o tubos de vacío, los cuales eran grandes y voluminosos, y generaban tanto calor que necesitaban cuartos con aire acondicionado; sus velocidades de proceso se medían en milisegundos (milésimas de segundo), casi no disponían de programas de apoyo y sus equipos periféricos eran lentos y poco eficaces, ocasionando una elevación de costos, alto consumo de energía y bajas velocidades de operación; cuando era necesario procesar un gran volumen de datos en períodos cortos, superaban en rapidez a cualquier otro equipo de proceso de aquella época. El primer computador fue el UNIVAC que almacenaba 1000 palabras de 12 bits.

El Dr. John W. Mauchly colaboró con J. Presper Eckert, Jr. y John Von Neumann, en la Universidad de Pensilvania para desarrollar una máquina que calcularía tablas de trayectorias para el ejército de Estados Unidos. El producto final fue el primer ordenador electrónico por completo operativo, se terminó en

⁴ Mora, José Luis y Enzo Molino, Op Cit. pag. 75.

1946 y recibió el nombre de ENIAC (Electronic Numerical Integrator and Computer; computadora e integrador numérico electrónico). Un ordenador mil veces más rápido que sus predecesores electromecánicos, ocupaba una superficie de 1,400 metros cuadrados y pesaba 30 toneladas. Esta máquina elimina todas las partes mecánicas que representaban los números y los sustituye con tubos al vacío mediante innovaciones importantes en su época.

En la oficina de censos de los Estados Unidos en 1951, se instaló la UNIVAC I (Universal Automatic Computer) desarrollada por Mauchly y Eckert para la Remington Rand Corporation. Así de 1946 a 1950, en los Estados Unidos de América y en Europa se proyectan diferentes prototipos basados en la idea de John Von Neumann, como por ejemplo: EDSAC MADM, SEAC, MANIAC, entre otros.

En 1958, nació la segunda generación de computadoras, las cuales utilizaban transistores que sustituyeron a las válvulas electrónicas con que contaban las máquinas de la primera generación.

Los norteamericanos J. Bardeen, W. M. Brattain y W. Shockely de los laboratorios Bell, inventaron y desarrollaron el primer transistor, el cual es aproximadamente 10 veces más rápido, más confiable debido a que los transistores operan “en frío”, evitando así las fallas causadas por sobrecalentamiento, 200 veces más pequeño que un bulbo o tubo electrónico, con una duración promedio de 90,000 horas, requería menos electricidad y más fáciles de programar con la ayuda del nuevo lenguaje COBOL. Estas máquinas tuvieron dimensiones más reducidas que las anteriores; sus velocidades de proceso se miden en microsegundos (millonésimas de segundo) y sus circuitos son menos complicados. Junto con ellas se desarrollaron almacenamientos con grandes capacidades, impresoras de alta velocidad, se innovan los métodos para recuperación de información, dispusieron de lenguajes que facilitaron su uso, su costo fue más accesible; entre los beneficios adicionales aportados por los

transistores están: mayor confiabilidad, menos pérdidas de energía en calor, mayor velocidad de proceso y menor espacio requerido.

Una de las primeras computadoras que usó el transistor fue la IBM 1401, construida en 1958 que podía procesar simultáneamente lectura y perforación de tarjetas, cálculos y decisiones lógicas, grabar y leer información en cinta magnética. Estas computadoras tienen gran demanda a partir de 1962, sin embargo, se viene abajo con la aparición de la tercera generación que nace a mediados de la década de los sesenta.

La tercera generación (1964-1970) se caracterizó porque la base de la computadora fue el circuito integrado y el microcircuito; la invención de los circuitos integrados permitió poner docenas de transistores en una sola pastilla "Chip." Diminuto trozo de cristal semiconductor en forma de cubo, en el que se han formado diodos, transistores u otros componentes que, interconectados, constituyen un circuito integrado funcional. La velocidad de proceso de éstas computadoras se medía en nanosegundos, se hizo en una sola pastilla de silicio el núcleo de una computadora, cuyos componentes son principalmente: ALU Unidad Lógica-Aritmética, los registros, los controles de direcciones y el reloj, con muchas áreas de almacenamiento interno. Este avance logró que las computadoras se hicieran más pequeñas, desprendieran menos calor, fueran más rápidas y energéticamente más eficientes, menores costos, mayor facilidad de uso y aprovechamiento más eficiente del equipo.

La tecnología de los circuitos integrados provocó la expansión de la industria del software y del hardware. Los fabricantes de equipo de cómputo incrementaron la flexibilidad y compatibilidad de sus programas en las nuevas máquinas, e incluso en máquinas todavía en fases de desarrollo. A partir de un software evolucionado, la tarea de programar ya no es considerada como un pesado esfuerzo, y las tendencias actuales se orientan hacia la consecución de lenguajes, para darles instrucciones a los ordenadores. Un ejemplo es la IBM 360,

que realizaba tanto análisis numérico como de administración o procesamiento de archivos.

Diversos autores consideran que la cuarta generación de computadoras fue en 1971, siendo la principal característica de ésta la aparición de los circuitos integrados a muy alta escala, con lo que se logra una muy alta densidad de circuitos. El proceso de éstas computadoras se miden en un rango de 1 a 10 nanosegundos. Junto con estos adelantos en circuitos integrados se desarrollan mejores técnicas y medios de almacenamiento; se introdujo el empleo intensivo de minidisquetes y cartuchos magnéticos, y se desarrollaron sistemas de impresión de alta calidad y gran velocidad.

La evolución de las computadoras de la cuarta generación, junto con el apoyo tecnológico que se le brindó a partir de la década de los setentas, permitió un cambio en la filosofía de la computación electrónica, un mejor acceso a su uso y facilidad de adquisición. De igual forma, gracias a la reducción en tamaño de los elementos que integran una computadora y su abaratamiento, han permitido que surjan nuevos equipos pequeños destinados al uso personal.

“En la década de los 70’s se desarrollaron diversos diseños de computadoras personales como: el modelo 5100 de IBM, con 16 Kb. de memoria, un monitor interconstruido de 16 líneas por 64 caracteres, un intérprete Basic, una unidad de cinta.

Steve Wozniak diseñó en 1977 la Apple I, una simple tarjeta de computadora fijada a un pedazo de madera, no tenía fuente de poder y contaba con especificaciones manuales.

En ese mismo año, la Apple II fue un gran suceso porque contenía una tarjeta madre con circuitos impresos, un switch para el encendido, un teclado, manuales y una cinta de casete con el juego para computadora “Breakout”. También se le integró una televisión con la cual la Apple II producía brillantes gráficos a color.

En 1979 se terminó el diseño de la Atari 400 de 8 bits, esta computadora era usada principalmente para ejecutar juegos, su último diseño la Atari XE Game System de 1987 dejó de ser PC para convertirse en tan sólo un aparato para ejecutar juegos de video.”⁵

Es de notarse que hacia finales de los años 70's, el mercado de las computadoras personales estaba dominado principalmente por dos compañías: IBM y Apple.

Estas microcomputadoras son uno de los elementos característicos de la cuarta generación, surgieron a principios de los ochentas y poco a poco han ido colocándose en el mercado; su aparición ha hecho que las computadoras incursionen por primera vez en campos como la música, el diseño gráfico, la pintura, la escritura de textos y el control de máquinas de facturación. También, le simplificaron el trabajo tanto a estudiantes como a profesionistas, investigadores, ejecutivos y hasta a amas de casa.

“La quinta generación aconteció a principios de los 90's, con la aparición de los ordenadores multimedia y los sistemas operativos amigables con entornos gráficos para facilitar la utilización a usuarios no especialistas. Se redujeron los costos y el tamaño y, aumentó la capacidad de proceso, la memoria y la velocidad.

Esta quinta generación se inició con una batalla entre países industrializados, fundamentalmente con Estados Unidos y Japón, aunque después se incorporaron otros como Francia e Inglaterra, en dicha batalla se realizaron nuevos adelantos en materia de computación. Sin embargo, Estados Unidos y Japón fueron los que invirtieron sumas considerables de dinero en el desarrollo de nuevas y mejores tecnologías de cómputo.

Y fue Japón, quien propuso un proyecto de producir computadoras verdaderamente inteligentes, crear sistemas que se pudieran programar con lenguajes naturales mediante los cuales fuera posible conversar. En octubre de

⁵ Long, Larry. & Long Nancy, Op Cit. pp.34.

1981, en una conferencia internacional que tuvo lugar en Tokio, los japoneses invitaron a los países de occidente a discutir las ideas que estaban detrás de ese proyecto, e indicaron que tal colaboración era crucial para el éxito de las computadoras de esta quinta generación”.⁶

De esta forma, Estados Unidos observó a la quinta generación no sólo como un proyecto de avance, sino que se preocupó por las ventajas comerciales que ofrecía éste tipo de desarrollos. Es por ello, que tanto el gobierno estadounidense como las principales compañías manufactureras de computadoras en ese país, comenzaron una carrera competitiva, para lo cual se establecieron líneas de investigación y desarrollo que son financiadas con aportaciones tanto de empresas individuales como de grupos de éstas.

Como es de notarse, este proyecto necesitó de muchas disciplinas y tecnologías diferentes, pero finalmente se logró, y gracias a él, actualmente contamos con un sistema de computación totalmente avanzado. Sin embargo, esto no termina aquí, pues la informática y la ciencia tecnológica siempre avanzarán para brindarnos a nosotros como usuarios una mayor ventaja en cuanto a nuestra toma de decisiones se refiere.

Una situación similar sucede hoy con la Internet, lo cual explica su espectacular crecimiento y dinamismo. Es difícil creerlo, pero el primer mensaje enviado por correo electrónico tuvo lugar en 1969 y el primer navegador comercial apareció en el mercado en 1993. Ese año, apenas 1.3 millones de computadoras tenían acceso a la Internet. En los cuatro años siguientes el número se multiplicó en más de diez veces, a 16 millones.

Este inmenso crecimiento, impactó profundamente en los negocios y el comercio, se llevó a cabo en gran parte gracias a la casi total ausencia de regulaciones gubernamentales. La clave del éxito de la Internet es su total

⁶ Idem.

apertura, lo cual ha permitido tanto a los usuarios como a los que ofrecen servicios, un acceso virtualmente infinito y total libertad para desarrollar e innovar.

Es inevitable que la libertad de la Internet va a ser restringida. La historia nos demuestra que los gobiernos jamás dejan algo bueno en paz. Pero eso no quiere decir que la Internet no va a seguir creciendo y estimulando el crecimiento económico por muchos años.

1.2 NOCIONES Y CONCEPTO

Desde mediados de siglo, se ha sentido con mayor enfoque, la necesidad de mejorar la dirección en las organizaciones; esto ha dado lugar, a que el hombre realice búsquedas con objeto de encontrar medios que le ayuden a tal fin. En ésta búsqueda surge la **cibernética**, que sin duda ha venido a mejorar el entendimiento de la labor de la dirección.

“En 1948, el doctor Norbert Wiener, (personaje matemático) planteó las ideas que han servido de base para el desarrollo de la cibernética como ciencia. Escribió un libro que intituló “Cibernética”, empleando éste término para designar a la nueva ciencia de la comunicación y control entre el hombre y la máquina.

Se puede definir a la *cibernética* como *ciencia que trata de los principios generales de dirección y de su aplicación en las máquinas, las sociedades y los organismos vivos*”.⁷

Tiene por objeto controlar los sistemas dinámicos complejos. Un sistema dinámico de dirección, considerado desde el punto de vista de los procesos que en él se llevan a cabo, se denomina sistema de control.⁸

Para el profesor *Julio Téllez*, la cibernética “*es la ciencia de comunicación y control, teniendo como objeto controlar los sistemas dinámicos complejos*”.⁹

⁷ <http://es.wikipedia.org/wiki/Cibern%C3%A9tica>

⁸ Mora, Jose Luis y Enzo, Op.Cit. pp.288.

“Se podrá confirmar lo anterior si atendemos a la etimología de la palabra "cibernética" que deriva del griego "*Kybernetes*" que significa "piloto" y de "*Kybernes*" referido dicho concepto al arte de "gobernar"; con lo cual se concluye que ésta palabra alude a la función del cerebro respecto a las máquinas”.¹⁰

La computadora electrónica, también llamada máquina cibernética, ha venido a desempeñar una función de primordial importancia dentro de la cibernética, y ha permitido nuevas formas de manejo de información y de los sistemas de dirección.

El desarrollo alcanzado hoy por las organizaciones, demandan gran cantidad de información.

Por otra parte, las empresas de nuestros días están obligadas a tomar decisiones cada vez más precisas y con mucha mayor rapidez. La informática enfrenta estos problemas y los resuelve, estudiando el mejor modo de proporcionar la información necesaria para la toma de decisiones.

Así, la informática surge como una ciencia llamada a cumplir un papel relevante como esencial instrumento para la superación de las dificultades producidas por la aceleración del progreso y su natural consecuencia, la explosión informativa contemporánea. El cúmulo de conocimientos científicos filosóficos, sociales, tecnológicos, entre otros, expresa un crecimiento exponencial que hace impostergable e insustituible el auxilio de esta nueva disciplina. Es por ello que a continuación se mencionarán algunas definiciones de informática.

En el año de 1962, Philippe Dreyfus, estableció que la palabra "*informática*" era un neologismo derivado de los vocablos información y automatización. Definió a la informática, en sentido general, como "*un conjunto de técnicas destinadas al*

⁹ Téllez, Julio. "Los delitos *Informáticos*", UNAM, México, 1997. Pág. 35

¹⁰ Corominas, Joan, Breve Diccionario etimológico de la lengua castellana, Madrid, 1983.

tratamiento lógico y automático de la información para una mejor toma de decisiones".¹¹

Mora y Molino la definen como *"el estudio de las relaciones entre los medios (equipo), los datos y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado"*.¹²

La Real Academia Española señala que Informática es el *"conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores (computadoras)*. Así mismo, manifiesta que *"informática es la palabra que se usa en América para hablar de computación"*.¹³

Para la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), la informática es *"la ciencia que tiene que ver con los sistemas de procesamiento de información y sus implicaciones económicas, políticas y socioculturales"*.¹⁴

A su vez, la Academia de Ciencias Francesa en 1966, sostuvo que la informática es *"la ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas especializadas, de la información contemplada como vehículo del saber humano y no de la comunicación de los ámbitos técnico, económico y social"*.¹⁵

De dicha primera intención conceptual, aún manteniéndose la validez de la definición original, se fue evolucionando y la informática fue adquiriendo una mayor amplitud a la conceptualización originalmente concebida. Se fueron apartando nuevos conceptos que expresan con mayor facilidad la amplitud de su contenido.

¹¹ Mora, José Luis y Enzo Molino, Op.Cit. pág. 103.

¹² Idem, pp. 121.

¹³ http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=informática

¹⁴ <http://www.unesco.org/new/es/unesco/informatica/es>

¹⁵ Mora, José Luis y Enzo, Op.Cit. pág.170.

Así se le definió como *"la disciplina que estudia el fenómeno de la información y la elaboración, transmisión y utilización de la información principalmente aunque no necesariamente, con la ayuda de ordenadores y sistemas de telecomunicación como instrumentos"*.¹⁶

Una definición aún más amplia, nos dice que *"informática es la aplicación racional y sistemática de la información para el desarrollo económico, social y político"*.¹⁷

La informática "es el conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. La informática combina los aspectos teóricos y prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano. Los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica".¹⁸

Podemos citar también, la definición adoptada por un grupo de profesores uruguayos: Delpiazzo Eirin y Montano, sosteniendo que *"es la ciencia del tratamiento lógico de la información."*¹⁹

Después de razonar las anteriores definiciones debemos entender ¿qué es información? y ¿qué es procesamiento de información?

Bien, el concepto de **información** es muy reciente además de sencillo; fue desarrollado en la década de los 40's del siglo XX por el matemático norteamericano Claude Shannon, para referirse a *"todo aquello que está presente*

¹⁶ Long, Larry. & Long Nancy, Op.Cit. pag. 145

¹⁷ Idem.

¹⁸ "Informática", Enciclopedia MicrosoftR EncartaR 2000. C 1993-1999 Microsoft Corporation.

¹⁹ "Delpiazzo, Carlos, Eirin, Álvaro, Montano, Piero. "Introducción a la Informática Jurídica y al Derecho Informático", Ed. Amalio Fernández, 1984, 4º Ed, Montevideo, pág. 37

*en un mensaje o señal cuando se establece un proceso de comunicación entre un emisor y un receptor.”*²⁰

Así, cuando dos personas hablan, intercambian información, por ejemplo, cuando vemos una película, estamos recibiendo información, o, cuando comemos algo nuestro sentido del gusto recaba información sobre el sabor y la consistencia del bocado. La información puede encontrarse y enviarse, como vemos, en muchas formas, con la condición de quien la reciba pueda interpretarla.

Por otro lado, el procesar información implica el almacenamiento, la organización y, muy importante, la transmisión de la misma; para ello en la informática intervienen varias tecnologías; siendo dos los pilares de la informática: la computación y la comunicación, es decir, en la informática intervienen muchas de las técnicas y máquinas que el hombre ha desarrollado a través de la historia para apoyar e incrementar su capacidad de memoria, su capacidad de pensamiento y su capacidad de comunicarse.

Sintetizando lo anterior, se puede afirmar que la informática es el producto del encuentro de dos tipos de tecnológicas: el de las máquinas de comunicar y el de las computadoras.

A su vez, las ramas de la informática son innumerables y según el campo de estudio se extienden más y más, por lo que a continuación señalaremos las de mayor trascendencia siguiendo el estudio de Téllez Valdez:

“...a) *Cibernética*.- Rama de la informática que busca integrar las teorías y estudios de la comunicación y control en máquinas y organismos vivos. Por ejemplo el diseño de robots industriales y los simuladores espaciales.

b) *Inteligencia Artificial*.- Rama de la Ciencia de la Computación que se combina con el uso de las computadoras para resolver problemas como el cerebro humano lo haría.

²⁰ “Delpiazzo, Carlos , Eirin, Álvaro, Montano, Pero. Op. Cit. pag. 40

c) *Realidad Virtual*.- Área de la informática que trata el estudio de herramientas que combinadas con un equipo de cómputo permiten al ser humano vivir experiencias a través de imágenes y sensaciones virtuales que sin llegar a ser reales lo parecieran. Como cuando vivimos la experiencia de encontrarnos volando o nadando en el mar sin ser algo real, de ahí el nombre de realidad virtual. Compuesto por un complejo dispositivo en donde a través de unos guantes y un casco conectado al cerebro y a una computadora, la persona puede vivir una experiencia virtual.

d) *Multimedia*.- Ciencia que combina las computadoras con diversos medios de comunicación como son la radio, la televisión, el cable, el sonido, el video, instrumentos musicales, animación, entre otros, para crear diversos efectos. Esta tecnología llega con el advenimiento de los discos ópticos CD-ROM.

Los sistemas multimedia permiten a los usuarios consultar, desde la comodidad de su hogar, bases de datos para obtener respuestas a sus preguntas o conocer los servicios ofrecidos.

e) *Domótica*.- Informática aplicada a diversas viviendas y edificios. Un concepto derivado de esta rama son los edificios inteligentes. Por ejemplo, automatizar los servicios de una construcción, control de accesos, control automático de la energía eléctrica, control automático del suministro de agua a través de detención de presencia.”²¹

1.3 CARACTERÍSTICAS GENERALES DE LA INFORMÁTICA

Dentro de la historia, no podíamos encontrar mejor ejemplo de transformación que el de la COMPUTADORA.

²¹ Julio Téllez, Op Cit. pág. 12-13

Si bien es cierto que al hablar de INFORMÁTICA estamos hablando de la COMPUTADORA, es menester mencionar que la característica principal de la informática es la misma computadora.

La **computadora** se define como *“la máquina automatizada de propósito general, integrada por elementos de entrada, procesador central, dispositivo de almacenamiento y elementos de salida”*.²²

La computadora es un dispositivo electrónico capaz de recibir un conjunto de instrucciones o programas, y, a continuación lo ejecuta realizando cálculos sobre los datos numéricos, o bien, compilando y correlacionando otros tipos de información.

Las computadoras son máquinas que permiten efectuar procesos repetitivos mediante un procedimiento predefinido, a fin de efectuar cálculos complicados en forma eficaz además de ser útiles para diseñar objetos y realizar dibujos, entre otras tareas, todo esto con una alta calidad y velocidad insospechada.

El mundo moderno de la alta tecnología nunca hubiese existido de no ser por el desarrollo del ordenador o computadora. Toda la sociedad utiliza estas máquinas, en distintos tipos y tamaños, para el almacenamiento y manipulación de datos, desde archivos gubernamentales secretos y transacciones bancarias hasta las cuentas domésticas privadas. Los equipos informáticos han abierto una nueva era en la fabricación, gracias a las técnicas de automatización y han permitido mejorar los sistemas modernos de comunicación.

Son herramientas esenciales prácticamente en todos los campos de investigación y tecnología aplicada, desde la construcción de modelos del universo hasta la previsión de las condiciones meteorológicas. Los servicios de bases de datos y redes informáticas permiten acceder a una gran variedad de fuentes de

²² Julio Téllez, Op.cit. pág. 15

información, pero esas mismas técnicas avanzadas también posibilitan la invasión sobre lo privado y las fuentes de información restringidas.

Con todo, el delito informático se ha convertido en uno de los riesgos al que la sociedad deberá enfrentarse si desea gozar de las ventajas de la tecnología moderna.

Por sus características, la computadora electrónica desplaza al hombre de sus actividades que unos cuantos años atrás se consideraban exclusivas de su intelecto. Esta máquina puede llevar a cabo un sinnúmero de trabajos de muy diversas áreas y especialidades. Hay plantas completas que se manejan totalmente por cómputo electrónico; diagnósticos médicos se dan con rapidez extraordinaria con el auxilio de las computadoras, todo banco de importancia controla sus movimientos por medio de máquinas cibernéticas.

Para lograr los procesos requeridos en un sistema, la computadora se vale de una serie de mecanismos que a continuación se citarán.

Todas las computadoras tienen a la vista un monitor y un teclado, son elementos indispensables para la comunicación entre el usuario y la máquina. Éstos siempre se conectan a la Unidad Central de Proceso (CPU), y se encuentran debajo del monitor en las Computadoras Personales (PC's).

A continuación, señalaremos los tipos de computadoras (ordenadores) existentes tal y como lo establece el maestro José Luis Mora:

Actualmente se utilizan principalmente dos tipos de ordenadores: los analógicos y los digitales. Sin embargo, cabe hacer mención que el término ordenador o computadora se utiliza para referirse al tipo digital exclusivamente.

***Ordenadores Analógicos.-** Están constituidos por un dispositivo electrónico o hidráulico diseñado para manipular la entrada de datos en términos de niveles de tensión o presiones hidráulicas, por ejemplo, en lugar de hacerlo como datos numéricos. El dispositivo de cálculo analógico más sencillo es la regla

de cálculo, que utiliza longitudes de escalas especialmente calibradas para facilitar la multiplicación, la división y otras funciones. En el típico ordenador analógico electrónico, las entradas se convierten en tensiones que pueden sumarse o multiplicarse empleando elementos de circuito de diseño especial. Las respuestas se generan continuamente para su visualización o para su conversión en otra forma deseada.

Este tipo de ordenadores aprovechan la similitud matemática entre las interrelaciones físicas de determinados problemas y emplean circuitos electrónicos o hidráulicos para simular el problema físico.

***Ordenadores Digitales.-** Este tipo de ordenadores se basan en una operación: la capacidad de determinar si un conmutador, o “puerta”, está abierto o cerrado. Es decir, el ordenador puede reconocer sólo dos estados en cualquiera de sus circuitos microscópicos: abierto o cerrado, alta o baja tensión o, en el caso de números, 0 o 1. Sin embargo, es la velocidad con la cual el ordenador realiza este acto tan sencillo lo que lo convierte en una maravilla de la tecnología moderna.

Las velocidades del ordenador se miden en megahercios, o millones de ciclos por segundo. Un ordenador con una velocidad de reloj de 100 MHz, velocidad bastante representativa de un microordenador o microcomputadora, es capaz de ejecutar 100 millones de operaciones directas por segundo.

Las microcomputadoras de las compañías pueden ejecutar entre 150 y 200 millones de operaciones por segundo, mientras que las supercomputadoras utilizadas en aplicaciones de investigación y de defensa alcanzan velocidades de miles de millones de ciclos por segundo.

La potencia y la velocidad de cálculo de los ordenadores digitales se incrementan aún más por la cantidad de datos manipulados durante cada ciclo. Si un ordenador verifica sólo un conmutador cada vez, dicho conmutador puede representar solamente dos comandos o números. Así, ON simbolizaría una

operación o un número, mientras que OFF simbolizaría otra u otro. Sin embargo, al verificar grupos de conmutadores enlazados como una sola unidad, el ordenador aumenta el número de operaciones que puede reconocer en cada ciclo.

En general, los ordenadores de la década de 1970 eran capaces de verificar 8 conmutadores simultáneamente, es decir, podían verificar ocho dígitos binarios, de ahí el término bit de datos en cada ciclo. Un grupo de ocho bits se denomina byte y cada uno contiene 256 configuraciones posibles de ON y OFF (o 1 y 0). Cada configuración equivale a una instrucción, a una parte de una instrucción o a un determinado tipo de datos; éstos últimos pueden ser un número, un carácter o un símbolo gráfico.

El desarrollo de procesadores capaces de manejar simultáneamente 16, 32 y 64 bits de datos, ha permitido incrementar la velocidad de los ordenadores. La colección completa de configuraciones reconocibles, es decir, la lista total de operaciones que una computadora es capaz de procesar, se denomina conjunto ó repertorio de instrucciones. Ambos factores, el número de bits simultáneos y el tamaño de los conjuntos de instrucciones, continúa incrementándose a medida que avanza el desarrollo de los ordenadores digitales modernos.

De acuerdo a la concepción de Enzo Molino, “todos los ordenadores digitales modernos son similares conceptualmente con independencia de su tamaño. Sin embargo, las computadoras de acuerdo a su tamaño, capacidad, precio y rendimiento se dividen en tres clases:

A) Macrocomputadoras o Mainframe.- Son máquinas de alto precio. Las mayores en el mercado, las usan las grandes corporaciones, el gobierno y las universidades, entre otras grandes instituciones. Atienden a muchos usuarios simultáneamente desde las terminales que se encuentran conectadas.

Necesitan instalaciones especiales, como el aire acondicionado, grandes cuartos y complejas conexiones.

B) Minicomputadoras o Miniordenador.- Aunque menores, cubren necesidades considerables, su tamaño no es un límite porque se pueden conectar

varias entre sí para aumentar su potencia; de instalación más sencilla que las anteriores y ocupan menos espacio. Atienden a varios usuarios al mismo tiempo, quedando entre las denominadas multiusuarios. Por lo general son demasiado caras para el uso personal y son aptas para compañías, universidades o laboratorios.

C) Microcomputadoras, Microordenador o computadora personal.-

Las usa una persona a la vez, son monousuarias, por ello se llaman también computadoras personales o PC's (Personal Computer). Su capacidad es menor que las anteriores, cubren las necesidades de un departamento pequeño, un despacho o una oficina. Son máquinas de coste relativamente bajo y por lo general son de tamaño adecuado para un escritorio. (algunas de ellas, denominadas portátiles o, laptops, son lo bastante pequeñas como para caber en un maletín)".²³

Algunos autores manifiestan que dentro de ésta clasificación se encuentra también la llamada "estación de trabajo", un microordenador con gráficos mejorados y capacidades de comunicaciones que lo hacen especialmente útil para el trabajo de oficina.

Enseguida, pasaremos a desarrollar los elementos por los cuales están integrados los ordenadores o computadoras digitales según el tratado de la profesora Caroline Haliday.

A) Hardware.-"... Está constituido por las partes mecánicas y electromecánicas y electrónicas, como estructura física de las computadoras y encargadas de la captación, almacenamiento y procesamiento de información, así como la obtención de resultados. Es decir, todo lo que se puede ver y tocar.

El Hardware, es el equipo utilizado para el funcionamiento de una computadora. El hardware se refiere a los componentes materiales de un sistema informático. La función de estos componentes suele dividirse en tres categorías

²³ Mora, José Luis y Enzo Molino. Op cit pág. 33.

principales: entrada, salida y almacenamiento. Los componentes de esas categorías están conectados a través de un conjunto de cables o circuitos llamado bus con la unidad central de proceso (CPU) del ordenador, el microprocesador que controla la computadora y le proporciona capacidad de cálculo.

El hardware es la unidad del sistema, el monitor y los periféricos como el módem, el ratón o la impresora.

Ciertamente un ordenador o computadora digital no es una única máquina, en el sentido en el que la mayoría de la gente considera a los ordenadores. Es un sistema compuesto de cinco elementos diferenciados: una CPU (unidad central de proceso); dispositivos de entrada; dispositivos de almacenamiento de memoria; dispositivos de salida y una red de comunicaciones, denominada bus, que enlaza a todos los elementos del sistema y conecta a éste con el mundo exterior.

1) La Unidad Central de Proceso.- El CPU puede ser un único chip o una serie de *chips* que realizan cálculos aritméticos y lógicos y que temporizan y controlan las operaciones de los demás elementos del sistema. Las técnicas de miniaturización y de integración han posibilitado el desarrollo de un chip de CPU denominado *microprocesador*, que incorpora un sistema de circuitos y memorias adicionales. El resultado son unos ordenadores más pequeños y la reducción del sistema de circuitos soporte. Los microprocesadores se utilizan en la mayoría de los ordenadores personales de la actualidad.

La mayoría de los *chips* del CPU y de los *microprocesadores* están compuestos por:

**La Unidad Aritmética y Lógica.-* Esta proporciona al chip su capacidad de cálculo, permitiendo que se efectúen las operaciones aritméticas: suma, resta, multiplicación y división.

**Los registros.-* Son áreas de almacenamiento temporal que contienen datos, realizan un seguimiento de las instrucciones y conservan la ubicación y los resultados de dichas operaciones.

**La Unidad de Control.-* Tiene tres tareas principales: temporiza y regula las operaciones de la totalidad del sistema informático; su decodificador de instrucciones lee las configuraciones de datos en un registro designado y las convierte en una actividad, por ejemplo, sumar o comparar, y su unidad interruptora indica en qué orden utilizarán la CPU las operaciones individuales y regula la cantidad de tiempo de CPU que podrá consumir cada operación.

**El Bus Interno.-* Consiste en una red de líneas de comunicación que conecta los elementos internos del procesador y que también lleva hacia los conectores externos que enlazan al procesador con los demás elementos del sistema informático. Hay tres tipos de bus en la CPU:

-Bus de control, que consiste en una línea que detecta las señales de entrada y de otra línea que genera señales de control desde el interior de la CPU.

-Bus de dirección, que es una línea unidireccional que sale desde el procesador y que gestiona la ubicación de los datos en las direcciones de la memoria.

-Bus de datos, una línea de transmisión bidireccional que lee los datos de la memoria y escribe nuevos datos en ésta.

2) Dispositivos de entrada.- Estos dispositivos permiten al usuario del ordenador introducir datos, comandos y programas en el CPU. Dentro de éstos se encuentran: el teclado, los lápices ópticos, el ratón o mouse, el joystick, el digitalizador óptico, el micrófono y el módem.

El teclado, es el dispositivo de entrada más común similar al de las máquinas de escribir, que permite al usuario introducir textos e instrucciones. Algunos teclados tienen teclas de función especiales o dispositivos apuntadores

integrados, como trackballs (bolas para mover el cursor) o zonas sensibles al tacto que permiten que los movimientos de los dedos del usuario dirijan un cursor en la pantalla.

Los lápices ópticos, constan de un puntero con un extremo fotosensible que se emplea para dibujar directamente sobre la pantalla o para seleccionar información en la pantalla pulsando un botón en el lápiz óptico o presionando el lápiz contra la superficie de la pantalla. El lápiz contiene sensores ópticos que identifican la parte de la pantalla por la que se está pasando.

Un mouse o ratón, es un dispositivo apuntador diseñado para ser agarrado con una mano. Cuenta en su parte inferior con un dispositivo detector (generalmente una bola) que permite al usuario controlar el movimiento de un cursor en la pantalla deslizando el mouse por una superficie plana. Para seleccionar objetos o elegir instrucciones en la pantalla, el usuario pulsa un botón del mouse.

Un joystick, es un dispositivo formado por una palanca que se mueve en varias direcciones y dirige un cursor u otro objeto gráfico por la pantalla de la computadora.

Un digitalizador óptico emplea dispositivos fotosensibles para convertir imágenes (por ejemplo, una fotografía o un texto) en señales electrónicas que puedan ser manipuladas por la máquina. Por ejemplo, es posible digitalizar una fotografía, introducirla en una computadora e integrarla en un documento de texto creado en dicha computadora. Los dos digitalizadores más comunes son el *digitalizador de campo plano* (similar a una fotocopidora de oficina) y el *digitalizador manual*, que se pasa manualmente sobre la imagen que se quiere procesar.

El micrófono es un dispositivo para convertir sonidos en señales que puedan ser almacenadas, manipuladas y reproducidas por el ordenador. Un

módulo de reconocimiento de voz es un dispositivo que convierte palabras habladas en información que el ordenador puede reconocer y procesar.

Un módem es un dispositivo que conecta una computadora con una línea telefónica y permite intercambiar información con otro ordenador a través de dicha línea. Todos los ordenadores que envían o reciben información deben estar conectados a un módem. El módem del aparato emisor convierte la información enviada en una señal analógica que se transmite por las líneas telefónicas hasta el módem receptor, que a su vez convierte esta señal en información electrónica para el ordenador receptor.

3) Dispositivos de almacenamiento.- Sirven para almacenar permanentemente información y programas que el ordenador deba recuperar en algún momento. Los sistemas informáticos pueden almacenar los datos tanto interna (en la memoria) como externamente (en los dispositivos de almacenamiento). Los dos tipos principales de dispositivos de almacenamiento son las unidades de disco y la memoria. Existen varios tipos de discos: duros, flexibles, magneto-ópticos y compactos.

Cuando se habla de unidades de disco, nos referimos a las ranuras físicas del CPU (Unidad Central de Proceso), en donde se insertan los discos flexibles, disquetes o floppies.

Las unidades de disco duro almacenan información en partículas magnéticas integradas en un disco. Las unidades de disco duro, que suelen estar fijos, siendo una parte permanente de la computadora, pueden almacenar grandes cantidades de información y recuperarla muy rápidamente. Estos se diferencian por la marca y tamaño, proporcionando típicamente una capacidad de almacenamiento de 80, 100 o 120 Megabytes.

Las unidades de disco flexible conocido también como disquete o floppy, consiste en un disco magnético de plástico flexible y se encuentra protegido por una cubierta, el anverso del disco es liso y el reverso presenta unos remaches.

También almacenan información en partículas magnéticas integradas en discos intercambiables, que de hecho pueden ser flexibles o rígidos. Los discos flexibles almacenan menos información que un disco duro, y la recuperación de la misma es muchísimo más lenta.

Las unidades de disco magneto-óptico almacenan la información en discos intercambiables sensibles a la luz láser y a los campos magnéticos. Pueden almacenar tanta información como un disco duro, pero la velocidad de recuperación de la misma es algo menor.

Las unidades de disco compacto o CD-ROM, almacenan información en las cavidades grabadas en la superficie de un disco de material reflectante. La información almacenada en un CD-ROM no puede borrarse ni sustituirse por otra información. Los CD-ROM pueden almacenar aproximadamente la misma información que un disco duro, pero la velocidad de recuperación de información es menor.

La memoria está formada por chips que almacenan información que la CPU necesita recuperar rápidamente.

La memoria de acceso aleatorio (RAM, siglas en inglés, Random Access Memory) se emplea para almacenar la información e instrucciones que hacen funcionar los programas de la computadora. Contiene la información de lectura y escritura que se procesa en el instante, por lo que cambia constantemente su contenido. Generalmente, los programas se transfieren desde una unidad de disco a la RAM. La RAM también se conoce como memoria volátil, porque la información contenida en los chips de memoria se pierde cuando se desconecta el ordenador.

La memoria de lectura exclusiva (ROM, siglas en inglés, Read Only Memory) contiene información y *software* cruciales que deben estar permanentemente disponibles para el funcionamiento de la computadora, por ejemplo el sistema operativo, que dirige las acciones de la máquina desde el

arranque hasta la desconexión. Consta de circuitos integrados con programas especialmente grabados que debe seguir la computadora cada vez que se enciende, siendo no modificable. La ROM se denomina memoria no volátil porque los chips de memoria ROM no pierden su información cuando se desconecta el ordenador.

Algunos dispositivos se utilizan para varios fines diferentes. Por ejemplo, los discos flexibles también pueden emplearse como dispositivos de entrada si contienen información que el usuario informático desea utilizar y procesar. También pueden utilizarse como dispositivos de salida si el usuario quiere almacenar en ellos los resultados de su computadora.

Los chips de RAM son como pedazos de papel en los que se puede escribir, borrar y volver a utilizar; los chips de ROM son como un libro, con las palabras ya escritas en cada página. Tanto los primeros como los segundos están enlazados a la CPU a través de circuitos.

4) Dispositivos de Salida.- Estos dispositivos permiten al usuario ver los resultados de los cálculos o de las manipulaciones de datos de la computadora. El dispositivo de salida más común es la unidad de visualización (VDU, Acrónimo de Video Display Unit), que consiste en un *monitor* que presenta los caracteres y gráficos en una pantalla similar a la del televisor. La pantalla convierte la información generada por el ordenador en información visual. Por lo general, las VDU tienen un tubo de rayos catódicos como el de cualquier televisor, aunque los ordenadores pequeños y portátiles utilizan hoy pantallas de cristal líquido (LCD, Acrónimo de Liquid Cristal Displays) o electroluminiscentes. Otros dispositivos de salida más comunes son las *impresoras* y los *módems*. Un módem enlaza dos ordenadores transformando las señales digitales en analógicas para que los datos puedan transmitirse a través de las telecomunicaciones.

5) Bus o red de comunicaciones.- Para funcionar, el hardware necesita unas conexiones materiales que permitan a los componentes comunicarse entre sí e interactuar. Un bus constituye un sistema común interconectado, compuesto

por un grupo de cables o circuitos que coordina y transporta información entre las partes internas de la computadora. El bus de una computadora consta de dos canales: uno que la CPU emplea para localizar datos, llamado bus de direcciones, y otro que se utiliza para enviar datos a una dirección determinada, llamado bus de datos. Un bus se caracteriza por dos propiedades: la cantidad de información que puede manipular simultáneamente (la llamada 'anchura de bus') y la rapidez con que puede transferir dichos datos.

Una *conexión en serie* es un cable o grupo de cables utilizado para transferir información entre la CPU y un dispositivo externo como un *mouse*, un teclado, un módem, un digitalizador y algunos tipos de impresora. Este tipo de conexión sólo transfiere un dato de cada vez, por lo que resulta lento. La ventaja de una conexión en serie es que resulta eficaz a distancias largas.

Una *conexión en paralelo* utiliza varios grupos de cables para transferir simultáneamente más de un bloque de información. La mayoría de los digitalizadores e impresoras emplean este tipo de conexión. Las conexiones en paralelo son mucho más rápidas que las conexiones en serie, pero están limitadas a distancias menores de 3 m entre la CPU y el dispositivo externo.

B) Software (capacidad de almacenamiento).- Constituye la estructura lógica que permite a la computadora la ejecución del trabajo a realizarse, es decir, son las instrucciones responsables de que el hardware realice su tarea. El conjunto de programas es un paquete; al conjunto de elementos relacionados se le denomina sistema; al conjunto de los programas de computación se le denomina Software. Este puede dividirse en varias categorías basadas en el tipo de trabajo realizado. Las dos categorías primarias de *software* son:

1.- Los sistemas operativos (*software del sistema*), que controlan los trabajos del ordenador o computadora. El sistema operativo tiene tres grandes funciones: coordina y manipula el *hardware* de la computadora, como la memoria, las impresoras, las unidades de disco, el teclado o el *mouse*; organiza los archivos en diversos dispositivos de almacenamiento, como discos flexibles, discos duros,

discos compactos o cintas magnéticas, y gestiona los errores de *hardware* y la pérdida de datos.

Los sistemas operativos controlan diferentes procesos de la computadora. Un proceso importante es la interpretación de los comandos que permiten al usuario comunicarse con el ordenador. Algunos intérpretes de instrucciones están basados en texto y exigen que las instrucciones sean tecleadas. Otros están basados en gráficos, y permiten al usuario comunicarse señalando y haciendo clic en un icono. Por lo general, los intérpretes basados en gráficos son más sencillos de utilizar.

Los sistemas operativos pueden ser de tarea única o multitarea. Los sistemas operativos de *tarea única*, más primitivos, sólo pueden manejar un proceso en cada momento. Por ejemplo, cuando la computadora está imprimiendo un documento, no puede iniciar otro proceso ni responder a nuevas instrucciones hasta que se termine la impresión. Todos los sistemas operativos modernos son *multitarea* y pueden ejecutar varios procesos simultáneamente.

En la mayoría de los ordenadores sólo hay una UCP; un sistema operativo multitarea crea la ilusión de que varios procesos se ejecutan simultáneamente en la UCP. El mecanismo que se emplea más a menudo para lograr esta ilusión es la multitarea por segmentación de tiempos, en la que cada proceso se ejecuta individualmente durante un periodo de tiempo determinado. Si el proceso no finaliza en el tiempo asignado, se suspende y se ejecuta otro proceso. Este intercambio de procesos se denomina *conmutación de contexto*. El sistema operativo se encarga de controlar el estado de los procesos suspendidos.

También cuenta con un mecanismo llamado *planificador* que determina el siguiente proceso que debe ejecutarse. El planificador ejecuta los procesos basándose en su prioridad para minimizar el retraso percibido por el usuario. Con esta técnica se emplea espacio en el disco duro para simular la memoria adicional necesaria.

Dentro de los sistemas operativos multiusuarios se encuentran: el UNIX, el OS/2, el Windows-NT y el Macintosh OS.

Y en los sistemas operativos monousuarios están: el DOS y su sucesor, el MS-DOS.

2.- El software de aplicación, que dirige las distintas tareas para las que se utilizan las computadoras. Lleva a cabo tareas de tratamiento de textos, gestión de bases de datos y similares.

Constituyen dos categorías separadas el *software de red*, que permite comunicarse a grupos de usuarios, y el *software de lenguaje* utilizado para escribir programas.”²⁴

Hay autores que consideran que el Software es muy variado debido a sus constantes innovaciones y lo clasifican en: Sistemas Operativos, Lenguajes y Compiladores, Sistemas de Información y Programas de Aplicación.

Para aclarar el tema dentro de esta clasificación el Dr. Larry Long nos define estos últimos señalando lo siguiente:

“- **Programas de Aplicación.**- Un **programa** es una secuencia de instrucciones que indican al *hardware* de un ordenador qué operaciones debe realizar con los datos. Los programas pueden estar incorporados al propio *hardware*, o bien pueden existir de manera independiente en forma de *software*. En algunas computadoras especializadas las instrucciones operativas están incorporadas en el sistema de circuitos; entre los ejemplos más comunes pueden citarse los microordenadores de las calculadoras, relojes de pulsera, motores de coches y hornos microondas. Por otro lado, un ordenador universal, o de uso general, contiene algunos programas incorporados (en la ROM) o instrucciones (en el chip del procesador), pero depende de programas externos para ejecutar

²⁴ Haliday Caroline M. Secretos de los Sistemas de PC. Edit. Limusa S.A. de C.V., México 1994. pág. 42.

tareas útiles. Una vez programado, podrá hacer tanto o tan poco como le permita el *software* que lo controla en determinado momento. El *software* de uso más generalizado incluye una amplia variedad de programas de aplicaciones, es decir, instrucciones al ordenador acerca de cómo realizar diversas tareas.

- **Lenguajes y Compiladores.**- Los lenguajes son el medio de comunicación entre las personas y la máquina, con ellos le decimos qué hacer y cómo; igual que cualquier otro lenguaje tiene una gramática que incluye una sintaxis con una lógica a través de reglas de uso y una ortografía. A través de la historia se han inventado varios lenguajes informáticos, algunos orientados hacia funciones específicas y otros centrados en la facilidad de uso.

Los compiladores traducen estos lenguajes de programación a lenguaje de máquina, cuyo código es 0 y 1 lo que lo convierte en un lenguaje muy complicado.

Dentro de estos lenguajes tenemos:

- **FORTRAN**, (Acrónimo de Formula Translator), fue el primer lenguaje exhaustivo de alto nivel de uso generalizado, caracterizado por sus fines eminentemente científicos y matemáticos.
- **ALGOL**, (Acrónimo de Algorithmic Language), lenguaje de orientación científica.
- **COBOL**, (Acrónimo de Comun Business Oriented Language), es un lenguaje de programación para uso comercial y empresarial especializado en la organización de datos y manipulación de archivos.
- **BASIC**, (Acrónimo de código de instrucciones Simbólicas de Uso General para Principiantes), se consideró hace mucho el lenguaje principal de las microcomputadoras, por lo que hubo

muchos paquetes desarrollados en él. Este lenguaje se ha actualizado generando versiones como Visual Basic de propósitos múltiples en las empresas.

- **PASCAL**, diseñado en un principio como herramienta de enseñanza, hoy es uno de los lenguajes de microordenador más populares.
- **LOGO**, fue desarrollado para que los niños pudieran acceder al mundo de la informática.
- **ADA**, utilizado fundamentalmente por el Departamento de Defensa de Estados Unidos.

Una tendencia constante en el desarrollo de los ordenadores es la microminiaturización, iniciativa que tiende a comprimir más elementos de circuitos en un espacio de chip cada vez más pequeño. Además, los investigadores intentan agilizar el funcionamiento de los circuitos mediante el uso de la superconductividad, un fenómeno de disminución de la resistencia eléctrica que se observa cuando se enfrían los objetos a temperaturas muy bajas.

Las redes informáticas se han vuelto cada vez más importantes en el desarrollo de la tecnología de computadoras. Las redes son grupos de computadoras interconectados mediante sistemas de comunicación. La red pública Internet es un ejemplo de red informática planetaria. Las redes permiten que las computadoras conectadas intercambien rápidamente información y, en algunos casos, compartan una carga de trabajo, con lo que muchas computadoras pueden cooperar en la realización de una tarea. Actualmente, se están desarrollando nuevas tecnologías de equipo físico y soporte lógico que acelerarán los dos procesos mencionados.

Otra tendencia en el desarrollo de computadoras es el esfuerzo para crear computadoras de quinta generación, capaces de resolver problemas complejos en formas que pudieran llegar a considerarse creativas. Una vía que se está explorando activamente es el ordenador de proceso paralelo, que emplea muchos chips para realizar varias tareas diferentes al mismo tiempo.

El proceso paralelo podría llegar a reproducir hasta cierto punto las complejas funciones de realimentación, aproximación y evaluación que caracterizan al pensamiento humano. Otra forma de proceso paralelo que se está investigando es el uso de computadoras moleculares.

En estas computadoras, los símbolos lógicos se expresan por unidades químicas de ADN en vez de por el flujo de electrones habitual en las computadoras corrientes. Las computadoras moleculares podrían llegar a resolver problemas complicados mucho más rápidamente que las actuales supercomputadoras y consumir mucha menos energía.”²⁵

1.4 INFORMÁTICA JURÍDICA EN GENERAL

a) ORIGENES

A través de la historia, hemos podido observar cómo los grandes inventos, como el telégrafo, el teléfono y los satélites por mencionar algunos, han llegado a formar parte de la vida cotidiana de la sociedad. Si bien es cierto que los grandes inventores jamás se imaginaron el gran auge y la suma importancia que traerían consigo sus inventos para la humanidad, también lo es que los precursores de la computación tampoco conjeturaron los avances que llegarían a realizarse hasta el día de hoy en materia de ordenadores electrónicos.

²⁵ Long, Larry y Nancy Long, Op Cit. págs 65-68.

La información de la sociedad está en plano ascendente, y por el momento nadie conoce los niveles que pueda llegar a alcanzar. Las computadoras han llegado a ser herramientas comunes en nuestra sociedad y las personas se involucran con ellas de múltiples maneras. Dentro de los numerosos ámbitos, en los que se ha visto infiltrado el ordenador electrónico tenemos:

-Las oficinas, tanto públicas como privadas, en donde las computadoras permiten un mejor y más rápido desenvolvimiento de actividades.

-Los Bancos, los cuales cuentan ahora con sistemas de pago sin cheques, autorización de crédito, transferencia de fondos, asesorías financieras, etc.

-La industria, en donde han permitido un aumento de productividad de las fábricas con reducciones de tiempo y costos.

-Los hospitales, públicos y privados, los cuales cuentan con una mejor preparación de historias clínicas, exámenes y diagnósticos más completos, mayor exactitud en las pruebas de laboratorio y mejor control en los productos farmacéuticos.

-Las empresas, quienes en su administración tienen un adecuado control de nóminas, contabilidad, inventarios, pedidos, así como con una adecuada formulación de políticas, planeación y conducción de estrategias de organización.

-El hogar, ya que las amas de casa cuentan ya con una adecuada administración del presupuesto, control de uso de energía, análisis de inversión y preparación de la declaración de impuestos en algunos casos.

En fin, son innumerables los ámbitos en donde se cuenta ya con los ordenadores digitales. De igual forma, son varias las utilidades que se les puede dar y son infinitas las tareas que se les puede asignar como por ejemplo:

*En la industria de la construcción, nos dan un mejor diseño y construcción de edificios, casas y carreteras, principalmente.

*Proporcionan una mayor y mejor comunicación de despachos noticiosos.

*Dan un mejor control en las bibliotecas.

*Proporcionan grandes desarrollos en las ideas publicitarias.

*Con ellas existe un mejor control de tráfico y contaminación.

*Sirven para localizar en forma expedita a las personas extraviadas, así como a la pronta recuperación de vehículos robados.

*Se tienen mejores y más acertadas predicciones meteorológicas.

*Se cuenta con un mejor desarrollo de la educación e investigación.

*Podemos tener fotografía y animación por computadora.

*Actualmente ya se cuenta con diversión y entretenimiento en las mismas computadoras.

Se considera actualmente que en los próximos años se darán cambios drásticos en la estructura, funcionamiento y aplicación de las computadoras.

Sin embargo, hay quienes contemplan de una manera optimista el uso futuro de las computadoras, y, también hay quienes lo consideran perjudicial para la humanidad. A ciencia cierta nadie sabe cuál de éstos dos pensamientos prevalecerá, el hombre finalmente, es quien tiene la respuesta.

Estamos en una sociedad donde las tecnologías de la información han llegado a ser la figura representativa de nuestra cultura, hasta el punto que para designar el marco de convivencia se alude reiteradamente a la expresión sociedad de la información.

Si bien es cierto que, el derecho surge de la necesidad de reglamentar las relaciones humanas, siendo producto de la organización social, también lo es que,

en esa convivencia el hombre también se relaciona con las computadoras, dada la magnitud de desarrollo de los mismos ordenadores electrónicos, por lo que el derecho informático es una forma necesaria del vivir social: donde hay hombre hay sociedad y donde hay sociedad debe haber derecho.

Actualmente, en diversas ocasiones hemos escuchado hablar acerca del *Derecho Informático y la Informática Jurídica*; sin embargo, poco sabemos respecto de éstas figuras, pues la mayoría pensaríamos que se tratara de la aplicación de las computadoras al estudio y práctica del derecho, aunque son conceptos totalmente diferentes y que a continuación ahondaremos sobre los mismos.

El Dr. Julio Téllez ahonda en el tema:

“...la importancia de la información es tal que nuestra Constitución en su reforma de 1977 reconoce el *Derecho a la Información*, por adiciones al artículo 6, que a la letra dice: [...el derecho a la información será garantizado por el Estado], y 41 fracción II: [La Ley garantizará que los partidos políticos nacionales cuenten de manera equitativa con elementos para llevar a cabo sus actividades. Por lo tanto, tendrán derecho al uso en forma permanente a los medios de comunicación social...] de tal suerte, que estructuralmente hablando se consagra como garantía individual, y también como garantía formalmente política y materialmente social.

El Derecho Informático, como una nueva rama del conocimiento jurídico, es una disciplina en continuo desarrollo. Los antecedentes que se tienen de él, se encuentran a partir del año de 1949 con la obra de Norbert Wiener, en cuyo capítulo IV consagrado al derecho y las comunicaciones nos expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico.

Lee Loevinger fue el primero que imaginó el uso de las computadoras para coadyuvar en la resolución de una problemática jurídica: la violación o no del régimen antimonopolio en el sistema jurídico norteamericano.

La reiterada interrelación derecho-informática, en los términos de un derecho informático se contempla una serie de implicaciones tanto de orden social, económico, técnico, práctico y por supuesto jurídico, suscitada por el uso de la informática.

Podemos observar en principio dicha relación, ubicando, a similitud de las relaciones existentes entre la informática y cualquier otra ciencia, a la informática como instrumento, que en el ámbito del derecho permita optimizar la labor del abogado, el jurista y el Juez.

Es, evidentemente, el ámbito de la informática al servicio del derecho, que en sus funciones diferenciadas la denominamos Informática Jurídica.

Se puede precisar que el Derecho Informático es una rama de las ciencias jurídicas que contempla a la Informática tanto como instrumento y como objeto de estudio, por lo que estaríamos ante la presencia de la Informática Jurídica y del Derecho de la Informática, respectivamente. Por lo que la clasificación del Derecho Informático será la Informática Jurídica y el Derecho de la Informática.”²⁶

La Informática Jurídica se ve plasmada en las diferentes etapas históricas que han visto el desarrollo de la tecnología, encaminada al avance de la comunicación y la forma de regular esta en beneficio de una sociedad.

Debemos precisar que las aportaciones que han realizado los diversos estudios de esta materia, han puntualizado una clara diferencia entre el Derecho Informático por un lado y la informática jurídica por otro lado. La informática jurídica es el conjunto de aplicaciones de la informática en el ámbito del derecho.

“Nace en 1959 en Estados Unidos. Y es en los años 50’s cuando se comienzan a utilizar las computadoras no sólo con fines matemáticos sino también lingüísticos. John Harty, sintió la necesidad de encontrar medios satisfactorios para tener acceso a la información legal. Para 1959, el Healt Law Center colocó

²⁶Julio Téllez Valdez, Op. Cit. pág. 36.

los ordenamientos legales de Pensilvania en cintas magnéticas. El sistema fue posteriormente demostrado, en 1960, ante la Barra de la Asociación Americana de Abogados en la reunión anual en Washington, D.C. Esta fue la primera demostración de un sistema legal automatizado de búsqueda de información.

En 1966, doce estados de la Unión Americana se propusieron desarrollar un sistema interno de recuperación de documentos legales.

En 1968, ésta compañía había computarizado los ordenamientos de cincuenta estados de aquel país, en cerca de un billón de caracteres, trabajo conocido como el Sistema 50.

Originalmente destinado para abogados y corporaciones, el Sistema 50 encontró mucho éxito en las legislaturas locales.

El segundo logro por parte del Healt Low Center fue el sistema LITE hoy llamado FLITE (Información Legal Federal a través de computadoras), que fue desarrollado por la Universidad de Pittsburg bajo contrato con la Fuerza Aérea Norteamericana en 1969.”²⁷

b) NOCIONES Y CONCEPTOS

Una vez aclarado el origen de la Informática Jurídica, pasaremos a definir cada una de estas figuras anteriormente poco conocidas, pero que son de suma importancia en la actualidad y sin duda son el tema central del presente trabajo.

La INFORMÁTICA JURÍDICA es definida como:

“...la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación”.²⁸

²⁷ S. Tanenbaum, Andrew, “Organización de computadoras. Un enfoque estructurado”. Tercera edición. Editorial Prentice Hall, 1993.pag. 54.

²⁸ Téllez Valdez Julio, Op. Cit.pag.30

“La INFORMÁTICA JURÍDICA debe entenderse como el conjunto de estudios e instrumentos derivados de la aplicación de la informática al Derecho, o más precisamente a los procesos de creación, aplicación y conocimiento del Derecho”.²⁹

“La INFORMÁTICA JURÍDICA estudia el tratamiento automatizado de las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (Informática Jurídica Documental); las fuentes de producción jurídica, a través de la elaboración informática de los factores lógico-formales que concurren en el proceso legislativo y en la decisión judicial (Informática Jurídica Decisional); y en los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho (Informática Jurídica de Gestión).

La Informática Jurídica, es la ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el derecho; es decir, la ayuda que éste uso presta al desarrollo y aplicación del derecho.

La Informática Jurídica tiene por objeto la aplicación de la tecnología de la información al derecho.

La Informática Jurídica como aplicación concreta de la informática al derecho, comprende los sistemas de archivo y documentación jurídica, de asistencia en las tareas administrativas de apoyo a las actividades jurídicas y la construcción de modelos para la comprensión del sistema jurídico”.³⁰

Es preciso señalar las diversas posturas de los especialistas en la materia quienes han analizado debidamente la naturaleza y objeto de la Informática Jurídica según Pérez Nuño:

“- Informática Jurídica como complemento de tres áreas. Fue de los primeros planteamientos hechos a la materia, entre sus precursores más representativos esta el canadiense Mackaay, quien desde 1971 se pronuncia

²⁹ Rodríguez Hernández Victor. “La informática Jurídica y su papel en el Derecho Mexicano” REDI (Revista Electrónica de Derecho Informático) pág. 2

³⁰ Pérez Nuño, Antonio Enrique. Op. Cit. Pág. 42.

sobre el tema a través de varios escritos. Siendo las tres áreas en que se basa dicha postura las siguientes:

***Jurimetría**, entendiéndose por la misma la aplicación de técnicas, estadísticas y matemáticas que permiten verificar la regulación de ciertas hipótesis interesantes en el acontecer jurídico, resolver algunos problemas concretos y elaborar a partir de dichos datos una cierta teoría del derecho. Se le dio este término a propósito de llegar a “medir”, si ello fuera posible, la conducta de los Jueces dentro de un sistema jurídico.

***Informática Jurídica**, consistiendo ésta en el tratamiento lógico y automático de la información, en éste caso jurídica, en tanto soporte del conocimiento y comunicación humana.

***Derecho de la Informática**, entendida como el conjunto de problemas jurídicos producidos por la informática.

- Informática Jurídica como relación simétrica entre elaboración electrónica y derecho, basada en la necesidad social de información. Sustentada en la tesis de Steinmuller, en 1970, para quien la informática jurídica tiene un doble objeto:

- Las aplicaciones de la computadora al derecho (Informática Jurídica propiamente dicha).
- Los problemas jurídicos derivados del impacto de estas tecnologías en la sociedad y su consecuente reglamentación jurídica (Derecho Informático).

- Informática Jurídica como teoría estructural del Derecho (Juscibernética). Siendo los representantes de ésta concepción Mario Losano y Hebert Fiedler, quienes al igual que Taddei Elmi establecen que la Informática Jurídica no es sino el último anillo de una cadena de interacciones entre las ciencias exactas o formales y la ciencia jurídica. Comprendía una aproximación cibernética al derecho, esto es, concebía al derecho como un subsistema del sistema social susceptible de ser regulado y controlado, proponiendo así mismo el desarrollo de las técnicas necesarias para poder utilizar la computadora en el ámbito jurídico, además del estudio sobre lógica y técnicas de formalización del derecho a fin de lograr un óptimo tratamiento informático.

- La Informática Jurídica y el Derecho se relacionan instrumental y sistemáticamente. Postura defendida por el francés Chouraqui en 1974, quien señala que es una relación bidireccional y de recíproco auxilio. La informática al servicio del Derecho y viceversa, el fenómeno informático para este autor, además de conferir un instrumento al Derecho, significa un factor de mutación a varios niveles de todo el que hacer jurídico y todo lo ligado a lo jurídico (social, económico, político, informativo, gestor-administrativo, etc.).

Chouraqui tomó como puntos de referencia la actividad de los tres poderes del Estado (Parlamentario, Administración y Justicia), y la Universidad, ésta, en cuenta a la enseñanza y la investigación.

- La Informática Jurídica como soporte de la decisión jurídica adoptada bajo el principio de legalidad. El noruego Bing, estableció que el principio de legalidad es de gran importancia para el derecho, ya que es el verdadero fundamento para un Estado de Derecho, apoyando su principio en elementos como la predecibilidad del sistema jurídico y sus decisiones, la objetividad de estas últimas, el principio de igualdad en cuanto a sus destinatarios y, el factor tiempo relacionado con la calidad de la decisión judicial.

- Informática Jurídica como modelo científico transdisciplinario. Para Taddei Elmi, los problemas jurídicos de la informática no entran en modo alguno en el ámbito de la informática jurídica, incluso entendida en sentido lato, sino que resultan ser aspectos “exquisitamente jurídicos”.³¹

El autor se aboca a distinguir la Informática de la Informática Jurídica, expresando que la primera, es una especie de una disciplina más basta, cual resulta la electrónica. Mientras que la segunda no pertenece ni a una ni a otra en totalidad, sino que tiene un carácter interdisciplinario y transversal.

De igual forma según Téllez Valdez existen otras denominaciones con las que se conoce a la Informática Jurídica:

³¹ Ídem. 59.

- “Computers and Law (países anglosajones).
- Informatique Juridique (Francia).
- Rechtsinformatique (antes Elektronische Datenverarbeitung and Recht, en Alemania Occidental).
- Jurismática (México).
- Rechcibernetik (países de Europa Oriental).”³²

Por lo que podemos establecer que, en términos generales, la **Informática Jurídica** es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática en general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación.

Podemos señalar de acuerdo a lo anterior, que el **Derecho Informático o Derecho de la Informática** es la otra cara de la moneda, ya que este constituye “el conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática. Ya que la informática en general es el objeto regulado por el Derecho.”³³

El Derecho Informático “es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática”.³⁴

El Derecho de la Informática, “es el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aprovechamiento y aplicación de las nuevas tecnologías de la información y de la comunicación en cualquier área, y relaciona los efectos jurídicos que de ella se desprenden en su aplicación”.³⁵

³² Julio Téllez .op cit. Pag 26

³³ Ibidem, pág. 27

³⁴ Lara Márquez Jaime. Op. Cit. Pág. 33

³⁵ Riestra Gaytán Emma. Apuntes “Los delitos Informáticos en el Derecho Positivo Mexicano” Curso Introducción a los Delitos Informáticos. Instituto Nacional de Ciencias Penales, julio del 2000. Pág. 16.

El Derecho de la Informática, “es el conjunto de normas reguladoras del objeto informático o de problemas directamente relacionadas con la misma”.³⁶

“Al referirnos al **Derecho Informático**, nos referimos a un conjunto de normas, es decir, de una normativa jurídica que en desarrollo en el mundo contemporáneo, se va plasmando en cuerpo normativo orgánico coherente. Por ejemplo, normas regulatorias de la protección de datos personales, normas relativas al régimen jurídico del software y particularmente a la problemática de su protección jurídica, sancionadas ya en un conjunto de países, y con proyectos normativos elaborados y en debate en otro conjunto aún mayor, normas relativas a la regulación jurídica de los flujos de datos transfronterizos, de los contratos informáticos, y otros aspectos, indican ya la existencia, vigencia y acelerada elaboración de un conjunto normativo específico y orgánico.

Hablamos del conjunto de *principios e instituciones* específicas regulatorias o propias de actividades vinculadas con la informática, en función de aquellos postulados emitidos por Jueces, Magistrados, tratadistas y estudiosos respecto al tema.

Por otra parte, *hechos*, como resultado de un fenómeno aparejado a la informática inimputable al hombre.

Y por último, *actos* como resultado de un fenómeno directamente vinculado a la informática y provocado por el hombre.

La Informática Jurídica y el Derecho Informático tras denotados esfuerzos por consolidarse como ramas autónomas del Derecho, constituyen dos de las más recientes áreas del Derecho que implican un punto de contacto, un lugar de encuentro, entre el Derecho y las nuevas tecnologías; en ese sentido, la Informática Jurídica y el Derecho Informático hasta cierto punto constituyen las áreas más avanzadas del Derecho”.³⁷

³⁶ Lara Márquez Jaime. Op. Cit. Pág. 39.

³⁷ Lara Márquez Jaime, Abogado. Profesor de Informática Jurídica de la Pontificia Universidad Católica del Perú. Derecho y Tecnología. “Una visión prospectiva del derecho”. 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático. Edita Derecho Org. Portal Jurídico en Internet Dirigen. Erick Iriarte y Luis Faus. (www.yahoo.com) Pág. 1.

Como podemos ver, a finales de los años setentas y hasta nuestros días, la aplicación que se hace con las computadoras en todas sus áreas, trae consigo una serie de inquietudes respecto a las repercusiones negativas que trajo el fenómeno informático y que requiere urgentemente una regulación jurídica.

c) EVOLUCIÓN

Si bien es cierto que los precursores informáticos nunca imaginaron los alcances que llegarían a tener las computadoras en general o aun en campos tan aparentemente fuera de influencia como el jurídico, todavía más difícil hubiera sido el concebir que el derecho llegaría a regular la informática.

“...De esta forma, a finales de los sesenta y luego de cerca de diez años de aplicaciones comerciales de las computadoras, empezaron a surgir las primeras inquietudes respecto a las eventuales repercusiones negativas motivadas por el fenómeno informático, por lo que se requirió de un tratamiento especial. Cabe mencionar que dichas inquietudes surgieron en un principio respecto a la influencia que venía ejerciendo la tecnología en general. Ya desde la gestación de la llamada revolución industrial se dejaba entrever las modificaciones sociales no necesariamente positivas provocadas por las máquinas.

La década de los sesenta marcó el desarrollo de varios sistemas diversos de los mencionados en los orígenes de la informática jurídica. En 1964, la Corporación Americana de Recuperación de Datos comenzó a comercializar sistemas de procesamiento de datos legislativos.

Una siguiente incursión la realizó la Corporación de Investigación Automatizada de la Barra de Ohio (OBAR) diferente de las dos primeras experiencias del Healt Law Center (HCL), enfocada hacia los abogados litigantes.

El sistema OBAR comenzó en 1967 cuando la Barra del estado de Ohio firmó un contrato con la Corporación de Datos de Dayton, Ohio. Los trabajos de este sistema continuaron en 1970 a través de la Mead Data Central que fue

constituida luego de la fusión de Data Corporation con Mead Corporation. En 1973 la Mead Data Central comenzó a comercializar el sistema LEXIS como sucesor del OBAR.

Por su parte la IBM fue creciendo en popularidad en el área de recuperación de documentos. Ya para 1969 el estado norteamericano de Washington empezó a utilizar el sistema de la IBM para procesamiento de documentos llamado IBM-TEXPAC. Posteriormente, otros estados de la Unión optaron por el sistema STAIRS, también de la IBM”.³⁸

d) CLASIFICACIÓN

En sus primeros años, la informática jurídica se presentó en los términos de una informática documentaria de carácter jurídico, es decir, creación y recuperación de información que contenían datos principalmente jurídicos (leyes, jurisprudencia, doctrina) o al menos de interés jurídico. Poco a poco se empezó a vislumbrar la idea de que de estos bancos de datos jurídicos se podían obtener no sólo informaciones sino también, mediante programas estudiados expresamente, verdaderos actos jurídicos como certificaciones, atribuciones de Juez competente, sentencias premodeladas, naciendo a fines de los años sesenta la llamada informática jurídica de gestión.

Finalmente, viendo que las informaciones y procedimientos eran fidedignos y permitían llegar a buenos resultados, es que surge la que hoy es considerada por algunos tratadistas como la informática jurídica metadocumentaria.

De esta forma, merced a la informatización en el campo del derecho, se han constituido diferentes tipos de archivos (legislativos, de jurisprudencia, doctrinales, bibliográficos, etc.), los cuales representan un potencial informativo insospechado, además de que constituyen un apoyo rápido y eficaz en la realización de actividades de gestión, así como una ayuda en la toma de decisiones en la

³⁸ Téllez, Julio Op. Cit. pág. 31.

educación e investigación, por mencionar sólo algunos campos, lo cual representa un hecho sin precedente dentro del ámbito jurídico.

Así, nos recuerda Téllez Valdez:

“...Con base en lo anterior se puede clasificar dicha interdisciplina de la siguiente forma:

- A) Informática Jurídica Documentaria.
- B) Informática Jurídica de Control y Gestión.
- C) Informática Jurídica Metadocumentaria.

A) Informática Jurídica Documentaria. (Almacenamiento y recuperación de textos jurídicos). El reciente desarrollo de los sistemas de documentación automatizada corresponde a una realidad sensible en todos los campos del conocimiento: el crecimiento del volumen documentario se ha dado en proporciones tales que los métodos tradicionales de búsqueda al día de hoy son obsoletos. En el contexto jurídico, el fenómeno de “la inflación de textos” es en parte responsable de este incremento. Los textos de la ley han dejado de ser generales para entrar en detalle y su cantidad, por lo tanto, ha ido en aumento, provocando una labor de legislación más pronunciada en los últimos veinte años.

La Informática Jurídica Documentaria es el área más antigua de la informática jurídica; sus orígenes suelen asociarse a los trabajos de John Horty en la Universidad de Pittsburg.

En los sistemas de informática jurídica documentaria se trata de crear un banco de datos jurídicos, relativo a cualquiera de las fuentes del derecho (menos la costumbre) a efecto de interrogarlo con base en criterios propios acordes a esa información y su relevancia jurídica. Los documentos que pueden almacenarse en ese banco de datos son por ejemplo: leyes, reglamentos, jurisprudencia, doctrina, acuerdos, etc., documentos que para los juristas son de suma importancia y por ende tienden a ser encontrados rápidamente.

Su finalidad consiste en encontrar lo más rápida y pertinentemente posible la información que ha sido almacenada. El conjunto de esas informaciones constituye el banco de datos o corpus. Está constituida por bases de datos de información jurídica. Se centra en el análisis del documento jurídico y está constituido por la aplicación de las técnicas documentales en el desarrollo de las técnicas informáticas.

B) *Informática Jurídica de Control y Gestión.* Un segundo aspecto es el de control y gestión el cual abarca los ámbitos jurídico-administrativo, judicial, registral, así como despachos de abogados, principalmente. Su objeto es el tratamiento de textos jurídicos mediante el uso de procesadores de la palabra y, por otra parte, las experiencias obtenidas, en materia de automatización de registros públicos, principalmente de bienes muebles. Está encaminada a organizar y controlar la información jurídica de documentos, expedientes, libros, ya sea mediante la aplicación de programas de administración que permitan crear identificadores y descriptores para la clasificación de dicha información. Su uso se da en tres sectores:

1) *En la administración pública.* Actualmente se presenta un crecimiento extraordinario en el volumen así como una gran complejidad de actividades en las dependencias gubernamentales debido al pronunciado desarrollo demográfico, económico y tecnológico, obligando así a dicho sector en sus niveles federal, estatal y municipal estar capacitado para recibir, tramitar, analizar y difundir todo tipo de información jurídica para su correcto funcionamiento. El principal beneficio en ésta área además de la agilización en la tramitación de asuntos jurídico-administrativos, es la disminución de la inercia burocrática y corrupción, lo cual alcanza niveles más significativos en el caso de la administración de la justicia, permitiendo la impartición de una justicia rápida, expedita y particularizada.

2) *En los órganos jurisdiccionales (Informática Judicial).* Se utiliza para la formulación agenda de Jueces, Magistrados, hasta la redacción automática de textos jurídicos a manera de sentencias, así como para la

aceptación, registro e indicación de competencia y seguimiento de los expedientes en Juzgados, Tribunales y Cortes. Actualmente se considera que en un futuro no muy lejano, cuando los abogados se hayan provisto de sistemas de cómputo, ya no será tan necesaria la visita a los Tribunales para conocer el estado de los asuntos, ya que todo podrá ser consultable vía telemática.

3) *En los despachos y notarías. (Ofimática Jurídica).* Considerada como la automatización de oficinas con actividades de índole jurídico, podemos observar que también se puede aplicar en las notarías, tiene tal funcionalidad que va más allá del simple tratamiento de textos, ofreciendo un menú completo de las principales actividades, con una organización, control y seguimiento verdaderamente asombrosos (agenda, estados de asuntos, registros, tarifas, cálculo de impuestos, etc.). Y, en los despachos de abogados se puede tener un control de asuntos, honorarios, redacción y verificación de escritos, etc, complemento de las funciones documentarias de orden legislativo, jurisprudencial, doctrinario y bibliográfico.

Lo más importante de esto es que dicha modernización permitirá a los abogados dedicarse a actividades jurídicas de contenido creativo, crítico e interpretativo tan olvidadas y que son afines a su profesión, motivando un enriquecimiento del derecho, el cual es tan necesario en estos tiempos.

C) *Informática Jurídica Metadocumentaria.* Como su nombre lo indica trasciende más allá de los fines documentarios propiamente dichos (constituye el acercamiento más interesante con respecto a la hoy difícilmente comprensible iuscibernética. Ayuda en la decisión, en la educación, la investigación, la previsión y la redacción.

La informática jurídica, en este ámbito denominado como decisional, está comenzando a ocuparse también del campo de la toma de decisiones de los operadores jurídicos, con el auxilio de los llamados “sistemas expertos”, no siendo

necesario “que el sistema tome la decisión”, puede ser simplemente una ayuda a la decisión que se puede dar en varios planos y en varios ámbitos”.³⁹

El profesor Martino sostiene que:

...“está compuesto por: a) una base de conocimiento en forma de banco de datos, banco de datos estructurado de tal forma que permita el cálculo lógico sobre él; b) un sistema cognitivo, motor de inferencia que contiene la mayor parte de los esquemas de razonamiento válidos de ese dominio; c) una interfase que comunica al usuario con la máquina. El motor de inferencia es un sistema capaz de tomar dos informaciones de la base de conocimiento y obtener una conclusión lógica”.⁴⁰

³⁹Téllez Julio, Op. Cit. pág. 46-49.

⁴⁰ Antonio Martino, La Informática Jurídica Hoy, en “Revista del Derecho Industrial”, n° 21, Ed. Depalma. Según señala Daniel Ricardo Altmark. Informática y Derecho, Aportes de Doctrina Internacional, Pág. 12.

CAPITULO II

PROTECCIÓN JURÍDICA A LOS PROGRAMAS DE COMPUTACIÓN

2.1 ANTECEDENTES Y EVOLUCION DEL PROBLEMA

Todas las tecnologías poseen efectos secundarios positivos y negativos. Esto se aplica también en el caso de las computadoras. Han modificado nuestra sociedad para bien y para mal. Por ejemplo, podemos manejar transacciones rápidamente para aumentar la velocidad de nuestra comprensión de datos comerciales. Sin embargo, este incremento de velocidad obliga a los individuos a trabajar más rápidamente y los coloca bajo mayor presión.

El alto grado de dispersión de las técnicas de procesamiento de datos por computadoras, ha conducido a las personas a protestar por su impersonalidad e incluso por su eliminación de puestos de trabajo. Muchas personas consideran que las computadoras convierten a todo el mundo en “solamente un número”, y que las computadoras despersonalizan todas las transacciones y borran la identidad de las personas. Temen que muy pronto todo el mundo se identificará mediante un número de la seguridad social bajo el cual los datos personales se reunirán y serán dispuestos para inspección, traduciéndose todo ello en pérdida de la vida privada.

Sin las salvaguardas adecuadas, cualquier sistema de registro de datos puede ser mal utilizado. Por ejemplo, llevar registros mediante el número de seguridad social constituye un procedimiento lógico y bien adecuado para las computadoras. Los números de la seguridad social son prácticamente universales, se ponen fácilmente en orden numérico y sólo existe uno para cada persona. Por supuesto, estos registros pueden ser impersonales o llegar inclusive a utilizarse mal. Pero los profesionales de la computación destacan de continuo que únicamente las personas utilizan mal los datos, no las computadoras.

Las computadoras son neutrales. Ofrecen un método para el procesamiento de datos que no es afectado por prejuicios raciales, religiosos o culturales. Pueden manejar grandes cantidades de datos en forma uniforme o aleatoria, sin prejuicio alguno. La computadora no lleva a cabo excepciones, debido a favores que deba, a alianzas, a alianzas políticas o a vínculos familiares. Son únicamente los seres humanos quienes pueden llevar a cabo este tipo de acciones.

Las computadoras poseen la capacidad de mantener vastas cantidades de datos. A menos que se restrinja el acceso a esa información, se puede hacer disponible para cualquier usuario de la máquina. Consideremos el amplio uso de las computadoras en nuestra sociedad. Datos que van desde informes financieros hasta los registros médicos se guardan en computadoras en todo el país, y son accesibles en términos de segundos a usuarios potencialmente no autorizados.

Consideremos los datos personales que obtienen las entidades oficiales y las organizaciones privadas. Estos datos podrían ponerse a disposición de entidades de crédito, de cualquier organización que lleve a cabo una verificación de rutina en el pasado financiero o judicial de una persona. Esta información podría potencialmente dañar la reputación de una persona y sus posibilidades futuras de empleo. Cualquier persona que tuviera acceso a estos datos sin la autorización adecuada, podría ser culpable de invasión de la vida privada de otro ser humano.

“Un área de igual delicadeza se refiere a los registros financieros que pueden obtenerse a través de las agencias nacionales de crédito. Estas agencias de crédito actúan como bancos de datos potenciales, especialmente en los casos que se relacionan con ciertos préstamos, hipotecas o referencias crediticias. Utilizando un número de seguridad social, estas agencias pueden proporcionar una historia crediticia total.

Esta historia se construye a partir de datos en los archivos computarizados de la agencia, y constituye parte rutinaria en la mayor parte de las verificaciones que se llevan a cabo cuando una persona solicita un préstamo o una tarjeta de

crédito. Las agencias de crédito tienen todo tipo de cuidados para garantizar que únicamente los usuarios autorizados tengan acceso a estos registros de crédito. Deben verificar que la privacidad de los registros personales en los archivos computarizados no se ponga en peligro.

La seguridad informática va adquiriendo una importancia creciente con el aumento del volumen de información importante que se halla en las computadoras distribuidas. En este tipo de sistemas resulta muy sencillo para un usuario experto acceder subrepticamente a datos de carácter confidencial. La norma Data Encryption System (DES) para protección de datos informáticos, implantada a finales de los años setenta, se ha visto complementada recientemente por los sistemas de clave pública que permiten a los usuarios codificar y decodificar con facilidad los mensajes sin intervención de terceras personas”.⁴¹

Así, vemos que la informática no sólo es un fenómeno tecnológico con implicaciones solo positivas, sino que también trae consigo riesgos por sus mismos avances. Las computadoras nos permiten un manejo rápido y eficiente de la información a que se tiene acceso, facilitando la concentración automática de datos referidos de las personas, constituyendo esto un verdadero factor de poder o riesgo que se tiene sobre la información.

“El uso de la informática en manos tanto del Estado como de los particulares, crea diversos riesgos que pueden sugerir una amenaza de agresión a la intimidad de los gobernados o de los usuarios del servicio. El reto de todo avance tecnológico siempre ha sido que el hombre quede al servicio de la tecnología y no al revés. El reto es, que sea el hombre el que domine a la tecnología y no ella a él”.⁴²

“En la década de los setenta comienzan a surgir numerosos archivos con informaciones de tipo personal, con un conjunto mínimo de datos como filiación,

⁴¹ "Redes de comunicación" Enciclopedia® Microsoft® Encarta 2001. © 1993-2000. Microsoft Corporation.

⁴² Cfr. Mejian C. Luis Manuel. "El Derecho a la Intimidad y la Informática". Segunda Edición. Edit. Porrúa. México. 1996. Pág. XIV.

fecha y lugar de nacimiento, domicilio, estado civil, entre otros, hasta otro tipo de datos con caracteres aún más distintivos como raza, religión, inclinaciones políticas, ingresos, cuentas bancarias, historia clínica, principalmente. Estos datos al ser recopilados en los centros censales, civiles, parroquiales, médicos, académicos, deportivos, culturales, administrativos, fiscales, bancarios y laborales, con el apoyo de medios automatizados, provocan una gran concentración sistematización y disponibilidad instantánea de ese tipo de información para diferentes fines”.⁴³

Esta recopilación de información puede ser empleada para fines publicitarios, comerciales, fiscales y policíacos principalmente. Pero también provoca que las personas corran un gran riesgo sobre dichos datos, ya que los mismos pueden ser utilizados para otras finalidades, alterando con esto los derechos fundamentales de los individuos en la sociedad, provocando discriminaciones, manipulaciones, persecuciones, presiones, asedios, entre otros. Quedando al filo de un adecuado control jurídico de dicha información.

“A la protección jurídica de las personas en lo que concierne al tratamiento automatizado de sus datos personales, o expresando en su forma más extensa, el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, en sus datos personales susceptibles de tratamiento automatizado para confeccionar una información que, identificable con él afecte a su entorno personal, social o profesional, en los límites de su intimidad, se le denomina ‘protección de datos personales’.

La Convención del Consejo de Europa para la Protección de Personas con respecto al Tratamiento automatizado de Datos de Carácter Personal, en su artículo 2, firmado en Estrasburgo el 28 de enero de 1981, define a la información de carácter personal como toda información concerniente a la persona física identificada o identificable”.⁴⁴

⁴³ Cfr. Tèllez Valdèz Julio. Op. Cit. Pág. 69.

⁴⁴ Davara Rodríguez Miguel Ángel. Manual de Derecho Informático, Edit. Aranzadi, 1999, Según cita Riestra Gaytan Emma. Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 18.

Muñoz menciona que las diversas legislaciones que han consagrado la protección sobre el uso y gestión de la información personal toman en cuenta el Derecho a la Autodeterminación Informativa. Que es la capacidad que goza toda persona de preservar su identidad controlando la revelación y el uso de los datos que le concierne y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos por los medios informáticos, también denominado “libertad informática”. Para lo cual toma diversas vertientes:

-Derecho a la Información.- en el sentido de tener el individuo la posibilidad de conocer la existencia de algún banco de datos o fichero de información personal.

-Derecho de Acceso a la Información Personal.- La aptitud que tiene el sujeto de conocer el contenido de aquellos bancos de datos automatizados cuyo objeto es el manejo y almacenamiento de información personal.

-Derecho de Actualización.- Gracias al cual, el individuo puede exigir la corrección de ciertos datos.

-Derecho de Confidencialidad.- Que concede al sujeto la exigencia a que la información que proporciona permanezca ajena al conocimiento de terceros.

-Derecho de Exclusión.- Por la naturaleza de la información puede el individuo cancelar, borrar o solicitar la destrucción de información denominada como sensible.

Davara nos indica que “podemos hablar también de los derechos de impugnación del interesado de determinados actos, cuando el fundamento sea un tratamiento automatizado de sus datos de carácter personal que ofrezca un perfil suyo obtenido de esta forma y, también, por último, del derecho de Titular de los

datos, de exigir responsabilidad por el daño que a sus bienes o derechos se le han causado, por el tratamiento de los datos erróneamente introducidos en el fichero.⁴⁵

“Dicha problemática ha sido de gran trascendencia a nivel internacional, al regular variadas figuras de índole jurídico, tales como los derechos humanos, derechos personales, derechos patrimoniales, libertades públicas y privadas en el caso de Francia, derecho de privacidad en el caso de los países anglosajones, derecho a la intimidad y al honor en las personas como en España, o, aún las garantías individuales y sociales como pudiera ser el caso de nuestro país, todas ellas, como protección eventual, han tenido hacia una sujeción apropiada en cuanto a la concentración y destinación de los datos de carácter personal.”⁴⁶

Ahora bien, el Derecho a la Intimidad o Privacidad, es un derecho fundamental que asiste a los sujetos de derecho consistente en la facultad de mantener reserva sobre diversas situaciones relacionadas con la vida privada, que debe ser reconocido y regulado por el sistema jurídico y que es oponible a todos los demás salvo en los casos en que puede ser develado por existir un derecho superior a terceros o para el bienestar común.

Observando que “la intimidad es el conjunto de circunstancias, cosas, expresiones, sentimientos y conductas que un ser humano desea mantener reservado para sí mismo, con libertad de decidir a quién le da acceso al mismo, según la finalidad que persiga, que impone a todos los demás la obligación de respetar y que solo puede ser obligado a develar en casos justificados cuando la finalidad perseguida sea lícita”.⁴⁷

“Dentro del Derecho a la Intimidad deben comprenderse el tratamiento de la información que compilan tanto los particulares, ya sea en actividades cotidianas, como en los casos de empresas que, por su objeto, realizan actividades de acumulación y uso de información, como, el Estado, a fin de que se realice el

⁴⁵ Cfr. Davara Rodriguez, Miguel Angel. La protección de datos en Europa., Op Cit. Pág. 25. Según cita Riestra Gaytan Emma, Los delitos Informáticos en el Derecho Positivo Mexicano, Pág. 19.

⁴⁶ Téllez Valdez, Julio. Op. Cit. Pág. 70.

⁴⁷ Cfr. Mejian C. Luis Manuel. Op. Cit., Pág. 87.

concepto de un Estado de Derecho en donde el papel de gobernante y gobernado, recopiladores de información y sujetos de ella tengan bien claros sus derechos y obligaciones.⁴⁸

Si bien es cierto que la Protección de Datos Personales constituye un gran problema, también lo es el Flujo de Datos Transfronterizos, pues ambos se ven reflejados en la actualidad con relación a la tecnología y comunicación que se maneja y éste último a nivel internacional.

Según el Consejo Económico de la Organización de las Naciones Unidas, el Flujo de Datos Transfronterizos es “la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y repercusión”.⁴⁹

El problema del Flujo de Datos Transfronterizos surgió a partir de la década de los setenta, con la relación entre la informática y las telecomunicaciones, dando el nacimiento con esto de la teleinformática o telemática.

El acceso rápido y eficiente con la tecnología informática ha facilitado el flujo instantáneo de actividades financieras e industriales que una vez fueron obstaculizadas por los controles de los gobiernos nacionales.

La red y el visor, liberaron a la computadora del papel, al surgir una nueva imprenta que permite a la comunidad mundial compartir conocimientos en el ciberespacio, sin limitación de tiempo ni espacio. Esas nuevas tecnologías trascendentales están cambiando nuestra forma de comprar, vender, comunicarnos y, en general, nuestra forma de vida. Vivimos en una era que no ha tenido un nombre específico, algunos la llaman “la post-guerra”, “la era atómica”, “la era cibernética e informática”, sin embargo, no cabe duda de que estamos en la Era Post-Industrial, en donde la nueva ciencia, la tecnología informática, genera

⁴⁸ *Idem. Pág. 106.*

⁴⁹ www.slideshare.net/.../flujo-de-datos-transfronterizo

constantemente herramientas digitales paradigmáticas de aceptación universal, que transforman la comunidad humana.⁵⁰

“La comercialización de las computadoras se inicia en la década de los 60’s, primeramente el 70% del capital destinado al desarrollo de la industria informática era empleado en el área de componentes físicos (hardware) mientras que el 30% restante se canalizaba al área de soporte lógico (software).

Actualmente, la creación de programas es más costosa que el soporte lógico, ya que son precisamente los programas de cómputo los que soportan en buena medida el adecuado comportamiento y el carácter efectivo de las computadoras, por ello, absorbe actualmente el 70% de los costos de la industria informática”.⁵¹

De acuerdo a los doctrinarios dicha protección corresponde a áreas del derecho; algunos consideran que la protección de los programas de computadora y de las bases de datos corresponde al derecho de propiedad intelectual específicamente en los derechos de autor, y otros doctrinarios, se inclinan por el derecho de patentes cosa que no ha tenido gran apoyo en el panorama legislativo.

“Al hablar de la protección jurídica de los programas de computación, se deben considerar dos tipos elementales: la protección del software y la de las bases de datos, ya que ambos constituyen la protección jurídica de los derechos de autor consagrados en la propiedad intelectual.”⁵²

Aunque un programa de computadora sea totalmente diferente a una base de datos consideramos que sus coincidencias y sus efectos jurídicos constituyen este tipo de protección jurídica intelectual.

⁵⁰Cfr. Perez Marallo Guillermo Augusto. Abogado y Notario. Universidad Complutense de Madrid. “Instrumentos de Pago Internacional, Tecnología Informática y Comercio Electrónico”, (Costa Rica) Derecho, Tecnología y Cambio, 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), Pág. 11.

⁵¹ <http://www.forodelderecho.blogcindario.com>

⁵² Páez Maña Jorge. La Protección de las Bases de Datos. España. 1996. Según señala Rietsra Gaytan Emma. Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág.25

2.2 NOCIONES FUNDAMENTALES

a) Concepto de programa de computación

Podemos considerar a los *Programas de Cómputo* como “el conjunto de procedimientos o reglas que integran el soporte lógico de las máquinas y que permiten la consecución del proceso de tratamiento de la información”.⁵³

“Dentro de los programas de computación podemos distinguir dos tipos:

-*Los Programas Fuente* (sistemas operativos o de explotación) están ligados al funcionamiento mismo de la máquina, guardando una relación con las memorias centrales y auxiliares de la computadora.

A su vez, el código fuente es la versión del programa de computadora escrita en uno de los diferentes lenguajes de programación usualmente utilizados para escribirlo y que permita su lectura por cualquier profesional programador. Además de que permite un enlace apropiado entre la máquina y los trabajos del usuario.

-*Los Programas Objeto*, que se realizan para satisfacer las necesidades más variadas de los usuarios, y que permiten el tratamiento de datos definidos concretamente, siendo dissociables de la máquina.

Es la versión del programa accesible únicamente a la máquina, es decir, el lenguaje comprendido por la computadora para llevar a cabo las diferentes etapas del programa”.⁵⁴

Programa de Computo, siguiendo el criterio del maestro Correa “es el conjunto de programas, procesos y reglas y eventualmente de documentación relativa al funcionamiento de un conjunto de tratamiento de la información. Conjunto o serie de instrucciones destinadas a ser utilizadas directa o indirectamente por un computador para obtener resultados”.⁵⁵

⁵³ Cfr. Téllez Valdés Julio, Op. Cit. Pág. 86.

⁵⁴ Riestra Gaytan Emma Op. Cit. Pág. 28.

⁵⁵ Carlos M. Correa “Derecho Informático” Edit. De Palma, Buenos Aires, 1987, Pag. 293

“Programa, en informática, suele ser denominado también *software*, siendo este el conjunto de instrucciones que ejecuta un ordenador o computadora.

El término puede referirse al *código fuente* original o a *la versión ejecutable* (en lenguaje máquina) de un componente de *software*. Cuando se habla de un programa se supone un cierto grado de terminación, o sea, se da por hecho que están presentes todas las instrucciones y archivos necesarios para la interpretación o compilación del programa. Por otro lado, se entiende que un programa ejecutable puede cargarse en un entorno determinado y ejecutarse independientemente de otros programas”.⁵⁶

“Programa ejecutable, en informática, programa que ha sido traducido a código máquina en un formato que puede cargarse en la memoria y ejecutarse. Sin embargo, en los lenguajes interpretados puede referirse simplemente al código fuente en su formato apropiado. La mayoría de los programas ejecutables en MS-DOS tiene la extensión de nombre de archivo .EXE. Para ejecutar el programa, el usuario sólo tiene que escribir el nombre del archivo (sin la extensión EXE) junto al símbolo del sistema y, a continuación, presionar la tecla Intro. El usuario no tiene que modificar el programa en modo alguno para poder ejecutarlo. Las aplicaciones como los programas de procesamiento de textos son programas ejecutables”.⁵⁷

PROGRAMA DE COMPUTACIÓN.- Es una secuencia de instrucciones que indican al *hardware* de un ordenador qué operaciones debe realizar con los datos. Los programas pueden estar incorporados al propio *hardware*, o bien pueden existir de manera independiente en forma de *software*. En algunas computadoras especializadas, o dedicadas, las instrucciones operativas están incorporadas en el sistema de circuitos; entre los ejemplos más comunes pueden citarse los microordenadores de las calculadoras, relojes de pulsera, motores de coches y hornos microondas.

⁵⁶ "Programa." *Enciclopedia® Microsoft® Encarta 2001*. © 1993-2000 Microsoft Corporation.

⁵⁷ "Programa ejecutable." *Enciclopedia® Microsoft® Encarta 2001*. © 1993-2000 Microsoft Corporation.
Reservados todos los derechos.

Por otro lado, un ordenador universal, o de uso general, contiene algunos programas incorporados (en la ROM) o instrucciones (en el chip del procesador), pero depende de programas externos para ejecutar tareas útiles. Una vez programado, podrá hacer tanto o tan poco como le permita el *software* que lo controla en determinado momento. El *software* de uso más generalizado incluye una amplia variedad de programas de aplicaciones, es decir, instrucciones al ordenador acerca de cómo realizar diversas tareas así, existen medios o lenguajes:

- **Lenguajes**

Las instrucciones deben darse en un lenguaje de programación que comprenda, es decir, en una determinada configuración de información digital binaria. En las primeras computadoras, la programación era una tarea difícil y laboriosa ya que los conmutadores ON-OFF de las válvulas de vacío debían configurarse a mano. Programar tareas tan sencillas como ordenar una lista de nombres requería varios días de trabajo de equipos de programadores. Desde entonces se han inventado varios lenguajes informáticos, algunos orientados hacia funciones específicas y otros centrados en la facilidad de uso.

- **Lenguaje máquina**

El lenguaje propio del ordenador, basado en el sistema binario, o código máquina, resulta difícil de utilizar para las personas. El programador debe introducir todos y cada uno de los comandos y datos en forma binaria, y una operación sencilla como comparar el contenido de un registro con los datos situados en una ubicación del chip de memoria puede tener el siguiente formato: 11001010 00010111 11110101 00101011. La programación en lenguaje máquina es una tarea tan tediosa y consume tanto tiempo que muy raras veces lo que se ahorra en la ejecución del programa justifica los días o semanas que se han necesitado para escribir el mismo.

- **Lenguaje ensamblador**

Uno de los métodos inventados por los programadores para reducir y simplificar el proceso es la denominada programación con lenguaje ensamblador. Al asignar un código mnemotécnico (por lo general de tres letras) a cada comando en lenguaje máquina, es posible escribir y depurar o eliminar los errores lógicos y de datos en los programas escritos en lenguaje ensamblador, empleando para ello sólo una fracción del tiempo necesario para programar en lenguaje máquina. En el lenguaje ensamblador, cada comando mnemotécnico y sus operadores simbólicos equivalen a una instrucción de máquina. Un programa ensamblador traduce el código fuente, una lista de códigos de operación mnemotécnicos y de operadores simbólicos, a código objeto (es decir, a lenguaje máquina) y, a continuación, ejecuta el programa.

Sin embargo, el lenguaje ensamblador puede utilizarse con un solo tipo de chip de CPU o microprocesador. Los programadores que dedicaron tanto tiempo y esfuerzo al aprendizaje de la programación de un ordenador, se veían obligados a aprender un nuevo estilo de programación cada vez que trabajaban con otra máquina. “Lo que se necesitaba era un método abreviado en el que un enunciado simbólico pudiera representar una secuencia de numerosas instrucciones en lenguaje máquina, y un método que permitiera que el mismo programa pudiera ejecutarse en varios tipos de máquinas. Estas necesidades llevaron al desarrollo de lenguajes de alto nivel”.⁵⁸

“La traducción de una serie de instrucciones en lenguaje ensamblador (el código fuente) a un código máquina (o código objeto) no es un proceso muy complicado y se realiza normalmente por un programa especial llamado compilador. La traducción de un código fuente de alto nivel a un código máquina también se realiza con un compilador, en este caso más complejo, o mediante un intérprete.

⁵⁸ www.civilizaciónwebinformática.blogspot.html

Un compilador crea una lista de instrucciones de código máquina, el código objeto, basándose en un código fuente. El código objeto resultante es un programa rápido y listo para funcionar, pero que puede hacer que falle el ordenador si no está bien diseñado. Los intérpretes, por otro lado, son más lentos que los compiladores ya que no producen un código objeto, sino que recorren el código fuente una línea cada vez. Cada línea se traduce a código máquina y se ejecuta. Cuando la línea se lee por segunda vez, como en el caso de los programas en que se reutilizan partes del código, debe compilarse de nuevo. Aunque este proceso es más lento, es menos susceptible de provocar fallos en la computadora”.⁵⁹

A todas luces nos podemos dar cuenta que los programas están relacionados de manera estrecha con los llamados lenguajes de programación, los cuales, sea de nivel de que se traten, fungen como medio de enlace entre el lenguaje natural y el lenguaje de la máquina.

Los problemas que alcanzan los programas de cómputo en la actualidad son tanto económicos como jurídicos, ya que representan pérdidas económicas, así como acciones ilícitas que trae repercusiones tanto a empresas como a los particulares cuando se ven afectados por algún delito relacionado a este tema.

⁵⁹ "Lenguaje de Programación". Enciclopedia Microsoft Encarta 2001.1993-2000 Microsoft Corporation.

CAPITULO III

DELITOS INFORMÁTICOS

3.1 ORÍGENES

En la actualidad, las computadoras se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación, y condiciona su desarrollo de la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto 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.

Los llamados *delitos informáticos* no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella. En ese entendido, nuestro trabajo se dirige al análisis de las posibles medidas preventivas, ya sean de carácter administrativo o penal que consideramos deben ser tomadas en cuenta para evitar que la comisión de este tipo de infracciones o delitos, alcance en México los niveles de peligrosidad que se han dado en otros países.

El aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

En la actualidad, la informatización se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como "criminalidad informática".

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

3.2 CONCEPTO

DELITOS INFORMÁTICOS O CIBERDELITOS (Cybercrime-Computer Crime).- "Son aquellas actividades ilícitas que se cometen mediante el uso de

computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos *per se*). También se puede definir al delito informático como la conducta típica, antijurídica, culpable y punible, en que se tiene a las computadoras como instrumento o fin.”⁶⁰

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 I de la Constitución Española”.⁶¹

Carlos M. Correa establece que es cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos.⁶²

Jijena Leiva lo define como “toda conducta típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma”.⁶³

Libano Manssur Claudio lo define como “aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátense de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose,

⁶⁰ www.informaticajuridica.com

⁶¹ Fernández Calvo, Rafael. "El Tratamiento del llamado "Delito Informático", Edit. Mérida, Extremadura, 1996, pag. 149.

⁶² Cfr. Carlos M. Correa "Derecho Informático" Edit. De palma, Buenos Aires, 1987, Pag. 293.

⁶³ Jijena Leiva, Renato Javier, Chile. La protección penal de la intimidad y el delito informático, Santiago, Ed. Jurídica de Chile, 1992. pág. 150

muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro”.⁶⁴

Núñez Ponce Julio lo define como “la realización de una acción que reuniendo las características que delimitan el concepto delito, sea llevada a cabo utilizando un elemento informático, ya sea de hardware o de software”.⁶⁵

Por último, el maestro Julio Téllez Valdez establece el concepto de delito informático en dos formas:

-*Típica*: las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin.

-*Atípica*: Son las actitudes ilícitas en que se tienen a las computadoras como instrumento o fin.

Sin embargo, dentro de las diferentes doctrinas existen diferentes términos para definir este tipo de delitos entre los que podemos destacar:

a) *Delincuencia informática*.- Gómez Perals la define 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”.⁶⁶

b) *Criminalidad informática*.- Alestuey prefiere hablar de "delincuencia o 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

⁶⁴ Huerta Miranda, Marcelo y Libano Manssur, Claudio. Delitos Informáticos. Ed. Jurídica Cono Sur. Santiago de Chile, Año 1998. Pág. 125

⁶⁵ <http://julionunezderechoinformatico.blogspot.com/>

⁶⁶ Gómez Perals, Miguel. “Delitos Informáticos en el Derecho Español” Edit. Aranzadi, Barcelona, 1994, Pag.481.

del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en este caso lo informático es finalidad)".⁶⁷

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".⁶⁸

c) *Delitos informáticos.*- Romeo 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".⁶⁹

Para Davara Rodríguez no parece adecuado hablar de delito informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito. Ni el Código Penal de 1995 introduce el delito informático, ni admite que exista como tal un delito informático, si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático. 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".⁷⁰

Determinados enfoques doctrinales subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los ordenadores.

⁶⁷ Baón Ramírez, Rogelio. "Visión General de la Informática en el Nuevo Código Penal" Cuadernos de Derecho Judicial. Madrid.1996, Pag.77.

⁶⁸ Tiedemann, Klaus. "Poder económico y delito", Barcelona, 1985.

⁶⁹ Romeo Casabona, Carlos María Los llamados delitos informáticos edit. Impactos Madrid 1987, Pag.34

⁷⁰ Davara Rodríguez, Miguel Ángel, "Manual de derecho informático" . Según cita Cuervo. Pág. 9.

Parker define los delitos informáticos como “todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio”.⁷¹

La definición anterior si no es la más exacta, sí contempla diferentes elementos del delito como son el dolo o la obtención de algún beneficio.

d) *Computer crimen*.- En el ámbito anglosajón se ha popularizado la denominación de “*Computer Crime*” y en el germano la expresión “*Computerkriminalität*”.⁷²

Esta definición hace referencia al crimen computacional, sólo en cuanto al medio utilizado para su comisión.

e) *Delincuencia 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”.⁷³

Para este autor los delitos informáticos son cometidos por personas de alto nivel económico, situación que en la actualidad no ocurre, pues pueden realizarlos personas de bajos recursos, como lo veremos más adelante.

f) *Abuso informático*.- Ruiz Vadillo recoge esta definición, 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”.⁷⁴

La misma definición aporta Correa, 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

⁷¹ http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

⁷² http://www.rae.es/rae.html/delito_informatico.es

⁷³ <http://forodelderecho.blogcindario.com/2008/05/00492-el-delito-de-cuello-blanco-edwin-sutherland.html>

⁷⁴ Ruiz Vadillo, Enrique. Falsedad y defraudaciones por abuso informático. Colección: Cuadernos de Derecho Judicial. Madrid. 1995. Pág. 77

la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el ordenador.

g) *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 desempeñaban un papel ya sea como método, medio o fin”.⁷⁵

h) *Crímenes por Computadora*.- Carlos Sarzana establece que los crímenes por computadora “comprenden cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo”.⁷⁶

En este orden de ideas, en el presente trabajo se entenderán como “*delitos informáticos*” las conductas ilícitas que tengan como finalidad o medio el uso indebido de equipos informáticos o los datos contenidos en ellos, ya que los mismos sirven como respaldos de información general, o bien como información que ejecuta las ordenes que el usuario proporciona para su funcionamiento.

3.3 CARACTERÍSTICAS

Como vemos, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan,

⁷⁵ Lima de la Luz, María. Delitos electrónicos. México D.F: Ed. Porrúa. Academia de México de Ciencias Penales. 1984, pág. 32

⁷⁶ Alestuey Dobòn, María del Carmen. “*Apuntes sobre la perspectiva criminológica de los delitos informáticos*”, Informática y Derecho n° 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi, págs.453 a 463.

con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

El estudio de los distintos métodos de destrucción y/o violación del hardware y el software es necesario en orden a determinar cuál será la dirección que deberá seguir la protección jurídica de los sistemas informáticos, ya que sólo conociendo el mecanismo de estos métodos es posible encontrar las similitudes y diferencias que existen entre ellos.

En consecuencia, la legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, provisionales y de identificación de las personas, y, si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje.

No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no está frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

De acuerdo a las características que menciona en su obra “Derecho Informático” el Dr. Julio Téllez Valdés, se observa el modo de operar en estos ilícitos:⁷⁷

- ❖ 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.
- ❖ Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.
- ❖ 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.
- ❖ Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios de más de cinco cifras a aquellos que los realizan.
- ❖ Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- ❖ Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- ❖ Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- ❖ Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- ❖ En su mayoría son imprudenciales y no necesariamente se cometen con intención.

⁷⁷ Cfr. Téllez Valdez, Op. Cit. Pag. 93.

- ❖ Ofrecen facilidades para su comisión a los menores de edad.
- ❖ Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- ❖ Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Haciendo un análisis concreto de las características enunciadas, 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.⁷⁸

3.4 CLASIFICACIÓN

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.

Así, tenemos la clasificación de los delitos informáticos del maestro Julio Téllez:

⁷⁸ Helen Peña. Silvia Palazuelos. Rosalía Alarcón. División de Estudios de Posgrado Facultad de Derecho UNAM, Cd. Universitaria, México, 1997.

***Como instrumento o medio.** Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio ó símbolo en la comisión del delito.

***Como fin u objeto.** En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.⁷⁹

Dentro de la doctrina se encuentran los siguientes autores que clasifican a los delitos informáticos como a continuación se describe:

Para Jover Padró se entendían comprendidos dentro de los delitos informáticos, con anterior al reciente Código Penal:

- a) El fraude informático, ilícitos patrimoniales que Jurisprudencia y Doctrina han calificado como hurto, apropiación indebida o estafa.
- b) Los documentos informáticos y sus falsedades.
- c) Del sabotaje informático, tipificado como delito de daños y estragos.
- d) Los ataques contra la intimidad de las personas.
- e) Las defraudaciones a la propiedad intelectual.
- f) Las faltas informáticas.

Romeo Casabona analiza las distintas facetas de lo que llama "las repercusiones de las Nuevas Tecnologías de la Información en el Derecho Penal", y de esta forma, divide su análisis en diferentes apartados bajo los títulos de:

- La protección penal de la intimidad e informática,
- La informática como factor criminógeno en el tráfico económico,
- El fraude informático,
- Implicaciones penales de las manipulaciones en cajeros automáticos mediante tarjetas provistas de banda magnética,

⁷⁹ Téllez Julio, Op. Cit. Pág. 105.

- Agresiones a los sistemas o elementos informáticos.⁸⁰

CORREA, siguiendo a UHLRICH, clasifica los delitos informáticos de la siguiente manera:

- a) fraude por manipulaciones de un ordenador contra un sistema de procesamiento de datos,
- b) espionaje informático y robo de software,
- c) sabotaje informático,
- d) robo de servicios,
- e) acceso no autorizado a sistemas de procesamiento de datos,
- f) ofensas tradicionales en los negocios asistidos por ordenador.⁸¹

Barriuso Ruiz los clasifica en:

- Delitos contra la intimidad
- De los robos
- De las estafas
- De las defraudaciones
- De los daños
- Relativo a la protección de la propiedad industrial
- Relativos al mercado y a los consumidores.⁸²

Baon Ramírez, distingue dos grandes grupos:

1.- Referente a los delitos que recaen sobre objetivos pertenecientes al mundo de la informática, dentro de los cuales destaca:

- Los relativos a la destrucción o sustracción de programas o de material.

⁸⁰ Cfr. Romeo Casabona Carlos María, "Poder informático y seguridad jurídica. La unificación tuteladora del derecho penal ante las nuevas tecnologías de la información". Fundesco, colección impactos, Madrid, 1987, Pág. 23. Según cita Cuervo Álvarez, pag. 8

⁸¹ Cfr. Cuervo Álvarez José, Op. Cit, Pag 16.

⁸² Barriuso Ruiz, Carlos, Interacción del Derecho y la Informática, Dykinson, Madrid, 1996, págs. 245-252. Según Cuervo Álvarez José, pag. 35.

-Los relativos a la alteración, destrucción o reproducción de datos almacenados.

-Los que se refieren a la utilización indebida de ordenadores.

2.- Encuadrados a la comisión de los delitos más tradicionales como los delitos en contra de:

- La intimidad

- La propiedad

- La propiedad intelectual o industrial

- La fe pública

- El buen funcionamiento de la administración

- La seguridad exterior e interior del Estado.⁸³

Pérez Nuño hace la siguiente clasificación:

-Desde el punto de vista subjetivo.- Los cuales ponen el énfasis en la pretendida peculiaridad de los delincuentes que realizan estos supuestos de criminalidad.

-Desde el punto de vista objetivo.- Considerando los daños económicos perpetrados por las conductas criminalistas sobre bienes informáticos, dentro de los cuales están:

*Los fraudes: los daños engañosos, virus informáticos, espionaje informático o hurto de software.

⁸³ Cfr. Baon Ramírez Rogelio. Visión General de la Informática en el nuevo Código Penal, según cita Cuervo Alvarez, pág. 37.

*El robo de servicios: Hurto del tiempo del ordenador, apropiación de información.

*El acceso no autorizado a servicios informáticos.

-Funcionales.- La insuficiencia de los planteamientos subjetivos han aconsejado primar otros aspectos que pueden resultar más decisivos para delimitar la criminalidad informática, como los atentados contra la fase de entrada o de salida del sistema, a su programación, elaboración, procesamiento de datos y comunicación telemática.⁸⁴

Davara Rodríguez clasifica a los delitos informáticos de acuerdo al fin que persiguen:

1.- Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos.

2.- Acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello.

3.- Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas.

4.- Utilización del ordenador y/o los programas de otras personas, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro.

5.- Utilización del ordenador con fines fraudulentos, y,

6.- Agresión a la privacidad mediante la utilización y procesamiento de datos personales con fin distinto al autorizado.⁸⁵

⁸⁴ Cfr. Pérez Nuñó, Antonio-Enrique, "Manual de informática y derecho", editorial Ariel s.a., Barcelona, 1996, pags. 69-81. Según cita de Cuervo Álvarez José, pag. 46.

⁸⁵ Cfr. Davara Rodríguez, Miguel Ángel, Op. Cit. pág. 23.

Por su parte Emma Riestra Gaytán clasifica a las conductas informáticas ilícitas en:

* Intercepción de comunicaciones sin autorización.

*Aprovechamiento de sistematización de la información contenida en bases de datos de sistemas o equipos de informática.

*Utilización de segmentos de red de sistemas o equipos informáticos. Utilización indebida del equipo informático o de los servicios de procesamiento de datos, bien sea en sitio o a través de acceso remoto del que puede resultar la obtención de la información (robo).

- ❖ Destrucción total o parcial de la información contenida en sistemas informáticos dirigidos a causar un perjuicio sobre bienes patrimoniales, tanto para el titular como al usuario del sistema.
- ❖ Difusión, distribución y reproducción mediante sistemas o equipos de informática de información relativa a la pornografía infantil (corrupción de menores) y lenocinio.
- ❖ Difusión, distribución y reproducción mediante o no sistemas informáticos, lo que actualmente se concibe como fraude informático, espionaje industrial.
- ❖ Aprovechamiento indebido o violación de un código para penetrar un sistema introduciendo instrucciones inapropiadas.
- ❖ Negación de acceso si autorizado a sistemas y equipos de informática.
- ❖ Abuso y daños de información en introducción falsa de información al sistema o equipo informático.
- ❖ Copiar y distribuir programas de cómputo en equipos o sistemas informáticos.

María de la Luz Lima, clasifica a los delitos electrónicos en tres categorías:

-Los que utilizan la tecnología electrónica como método; conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

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

-Los que utilizan la tecnología electrónica como fin; conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.⁸⁶

3.5 RIESGOS INFORMÁTICOS

En la actualidad han surgido muchos problemas relacionados con el uso de computadoras, amenazas que afectan negativamente tanto a individuos como a empresas. La proliferación de la computadora como la principal herramienta de funcionamiento en casi todos los niveles de convivencia, así como la creación de la red global Internet ha provocado que cada vez más personas se las ingenien para lucrar, hacer daño o causar perjuicios a través del uso de estos instrumentos.

Estos delitos tienen características específicas que los distinguen de los demás. Requieren de conocimientos altamente técnicos para ser realizados, se pueden consumir de manera rápida, efectiva (a veces milésimas de segundos) y sin necesidad de una presencia física.

Las estadísticas nos indican que estos delitos generalmente son realizados por personas con conocimientos técnicos de alto nivel que a veces trabajan con o a través de la entidad afectada, pero otras veces están completamente fuera de nuestro alcance ya que los realizan estando físicamente en otro país. Esto

⁸⁶ Cfr. Lima de la Luz Maria. Op. Cit. pág. 55.

conlleva que quede el agresor y la víctima en dos legislaciones distintas y sea complicado remediar las dificultades que surgen.

Qué ocurre en los siguientes casos:

- Cuando se varían datos como los activos y pasivos en la situación contable de una empresa.
- Cuando se sustrae información confidencial que se puede utilizar para causar perjuicios.
- Cuando se modifican datos tanto en su entrada como en su salida.
- Cuando se varía el destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Cuando se introduce algún virus informático que altera o paraliza el funcionamiento de los sistemas.

Todas estas actividades pueden ser extremadamente dañinas a las empresas o individuos que son afectados y altamente lucrativas para los que las realizan.

Estos delitos no pueden ser combatidos, investigados, ni castigados. Entonces, ¿qué le ocurre a quien es víctima de ellos? ¿de qué manera se puede cubrir una persona contra los riesgos que causan estas conductas?. Es muy común ver coberturas por fraudes de tarjetas de crédito. Esta póliza cubre pérdidas sufridas por el tarjetahabiente por el uso doloso de su tarjeta por un tercero sin su autorización. Esto incluye la interceptación de su número de tarjeta con el fin de retirar dinero o de hacer compras por la red. Pero, aun hay mucho por abarcar, pues cada vez se ven más casos de delitos electrónicos, a medida que nos modernizamos, nos integramos a la red global y comenzamos a depender más de tecnología computacional.

“A los sujetos que realizan estas conductas hubo de llamarles de alguna forma, por ello se les denominó, en círculos profanos, *Hackers*. Es un término inglés con el que se define a las personas dedicadas, por afición u otro interés, a

violador programas y sistemas supuestamente impenetrables, y apenas constituyen una muestra de la nueva faceta de la criminalidad: El delincuente silencioso o tecnológico. Producto de la falta de información se les nombra así a todos sin tener en cuenta la diferencia implícita que lleva su actuar y las consecuencias del mismo.

En el internet el pirateo se simplificó porque los programas fueron puestos a disposición del público en la misma red. Desde entonces, la distinción se hace por los grados de conocimiento y la esfera de su actuar. Así nos encontramos con los Hackers, los Crackers y los Phreakers, quienes son los tres grupos originarios de los que se subdividen otros tantos.”⁸⁷

A continuación distinguiremos cada uno de ellos:

HACKER.- Es una persona muy interesada en el funcionamiento de sistemas operativos; aquel curioso que simplemente le gusta husmear por todas partes, llegar a conocer el funcionamiento de cualquier sistema informático mejor que quienes lo inventaron. La palabra es un término inglés que caracteriza al delincuente silencioso o tecnológico. Ellos son capaces de crear sus propios softwares para entrar a los sistemas.

Los hackers suelen ser verdaderos expertos en el uso de las computadoras y por lo general rechazan hacer un uso delictivo de sus conocimientos, aunque no tienen reparo en intentar acceder a cualquier máquina conectada a la red, o incluso penetrar a una Intranet privada, siempre con el declarado fin de investigar las defensas de estos sistemas, sus lados débiles y "anotarse" el mérito de haber logrado burlar a sus administradores. Muchos de ellos dan a conocer a sus víctimas los "huecos" encontrados en la seguridad e incluso sugieren cómo corregirlos, otros llegan a publicar sus hallazgos en revistas o páginas Web de poder hacerlo.

⁸⁷ Jiménez Dan, Rafael Ricardo, Derecho org. R.e.d.i. (revista electrónica de derecho informático).

El Hacker es una persona experta en materias informáticas y con edad fluctuante entre los 15 y 25 años de edad es por ello que esta delincuencia se ha denominado "SHORT PANTS CRIMES", es decir, en pantalones cortos, su motivación no es la de causar daños sino de obtener personales satisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos.

CRACKER.- Personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas. El Pirata informático tiene dos variantes:

-El que penetra en un sistema informático y roba información o se produce destrozos en el mismo.

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

Cracker es aquel Hacker malicioso fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas, utiliza sus conocimientos para obtener beneficios, o simplemente por causar daños.

Para los grandes fabricantes de sistemas y la prensa este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.

En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado más adelante.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

Como su nombre indica se dedican a romper, por supuesto las protecciones y otros elementos de seguridad de los programas comerciales, en su mayoría con el fin confeso de sacar provecho de los mismos del mercado negro. Estos crean códigos para utilizarlos en la copia de archivos. Sus acciones pueden ir desde la destrucción de información ya sea a través de virus u otros medios, hasta el robo de datos y venta de ellos. Ejemplo de su actuar ilegal son los millones de CD's con software pirata que circulan por el mundo entero y de hecho, muchas personas no llegan a sospechar que parte del software que tienen en sus máquinas, incluso con certificados de garantía de procedencia, es craqueado. Esto sucede sobre todo en los países del tercer mundo; se agrupan en pequeñas compañías y contratan especialistas de alto nivel.

Aunque tratan de cubrirse con el ropaje de la aventura y el desafío tecnológico, los miles y millones de pérdidas y los cientos de casos que conocen anualmente la policía y fiscales de todo el mundo, hablan de un interés pecuniario y delictivo que científico.

Claro que la prensa, e incluso autoridades del mundo entero, diferencian al estudiante sin recursos que "craquea" un programa para su uso, de los que hacen de ello un negocio, aunque insisten que nadie debe actuar así. Lo cierto es que la principal condición para que florezca el negocio del cracking es el precio, siempre en ascenso y en algunos casos exorbitantes, de los programas de mayor utilidad en contraposición con el del hardware que ha mantenido una tendencia decreciente, por lo que no es de extrañar que con frecuencia el costo del software que soporta una máquina, aun una de última generación, sea superior al de ésta.

El Cracker desconoce los sistemas informáticos y sus retos se limitan a la vulneración del software comercial cometiendo conductas de piratería informática.

Las conductas habituales de los crackers se basan en la copia no consentida de programas informáticos vulnerando sus derechos de autor.

PHREAKER.- Es el especialista en telefonía (Cracker de teléfono).Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo, es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesamiento de datos.

Estos buscan burlar la protección de las redes públicas y corporativas de telefonía, con el declarado fin de poner a prueba conocimientos y habilidades(en la actualidad casi todas estas redes de comunicaciones son soportadas y administradas desde sistemas de computación), pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de "Hacking" a sus servidores.

Estos tipos con conocimientos de telefonía insuperables conocen a fondo los sistemas telefónicos incluso más que los propios técnicos de las compañías telefónicas.

Actualmente se preocupan más de las tarjetas prepago, ya que suelen operar desde cabinas telefónicas o móviles. Un sistema de retos, es capaz de captar los números de abonado en el aire. De esta forma es posible crear clones de tarjetas telefónicas a distancia.

LAMMERS.- Aquellos que aprovechan el conocimiento adquirido y publicado por los expertos. Si el sitio web que intentan vulnerar los detiene, su capacidad no les permite continuar mas allá. Generalmente, son despreciados por los verdaderos hackers que los miran en menos por su falta de conocimientos y

herramientas propias. Muchos de los jóvenes que hoy en día se entretienen en este asunto forman parte de esta categoría.

GURUS.- Son los maestros y enseñan a los futuros Hackers. Normalmente se trata de personas adultas, me refiero a adultas, porque la mayoría de Hackers son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma hay, para enseñar a o sacar de cualquier duda al joven iniciativo al tema. Es como una especie de profesor que tiene a sus espaldas unas cuantas medallitas que lo identifican como el mejor de su serie. El gurú no está activo, pero absorbe conocimientos ya que sigue practicando, pero para conocimientos propios y solo enseña las técnicas más básicas.

BUCANEROS.- En realidad se trata de comerciantes. Los bucaneros venden los productos crackeados como tarjetas de control de acceso de canales de pago. Por ello, los bucaneros no existen en la Red. Solo se dedican a explotar este tipo de tarjetas para canales de pago que los Hardware Crackers, crean. Suelen ser personas sin ningún tipo de conocimientos ni de electrónica ni de informática, pero si de negocios. El bucanero compra al Copy-Hacker y revende el producto bajo un nombre comercial. En realidad es un empresario con mucha afición a ganar dinero rápido y de forma sucia.

NEWBIE.- Traducción literal de novato. Es alguien que empieza a partir de una Web basada en Hacking. Inicialmente es un novato, no hace nada y aprende lentamente. A veces se introduce en un sistema fácil y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la página Web para seguir las instrucciones de nuevo. Es el típico tipo, simple y nada peligroso. Está apartado en un rincón y no es considerado.

TRASHING.- Esta conducta tiene la particularidad de haber sido considerada recientemente en relación con los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una

empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas.

Estas actividades pueden tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada. Esta minuciosa distinción de sujetos según su actuar no son útiles para tipificar el delito pues son sujetos indeterminados, no requieren condición especial; más vale realizar dicha diferenciación para ubicarnos en el marco en que se desenvuelven y las características de su actuar, favoreciendo con ello el procedimiento penal que se deberá llevar a cabo luego de producirse el delito.

“La gran mayoría de los hackers, en sentido general, copian herramientas que desarrollaron otros. Actualmente, existen alrededor de 60 mil páginas que explican con todo detalle muchos de los trucos para piratear. Sólo basta con bajar un programa y comenzar a bombardear un sitio para lograr las primeras experiencias. Incluso, hay algunas páginas que ofrecen laboratorios de virus, donde la persona puede crearlos a su medida, siguiendo instrucciones básicas. Además por medio de estos programas van aprendiendo a desarrollar sus propias herramientas...”⁸⁸

En virtud de estas transformaciones, está emergiendo una nueva economía que alternativamente también se le ha denominado “sociedad de la información o del conocimiento”. Se trata de un sistema económico y social donde la generación, procesamiento y distribución de conocimiento e información constituyen la fuente fundamental de productividad, bienestar y poder.

La revolución digital es ya una realidad que exige ser afrontada de inmediato, buscando y motivando una suficiente inversión para su desarrollo y legislando un marco jurídico seguro tanto para los proveedores de servicios como para los usuarios. Uno de los factores que ha impedido un desarrollo mayor de los servicios de la sociedad de la información, es la inseguridad al momento de

⁸⁸ <http://www.delitosinformaticos.com>

realizar transacciones electrónicas, debido a un sistema jurídico que no está adecuado para recoger las exigencias del mismo. La implantación de Internet y las nuevas tecnologías tropiezan con incertidumbres jurídicas, que es preciso aclarar con el establecimiento de un marco jurídico adecuado, que genere en todos los actores participantes la confianza necesaria para el empleo de este nuevo medio.

En la medida que nuestra sociedad va evolucionando, los problemas relacionados con la seguridad jurídica tanto de los programas de computación como del tráfico en la red presentan importancia prioritaria para el desarrollo de la misma. Los grandes principios a que está aferrada nuestra democracia deben aplicarse a esta nueva situación: libertad de expresión, protección de menores, protección de la vida privada y de la correspondencia privada, igualdad de acceso al saber, protección del derecho de autor y de la propiedad industrial, diversidad cultural, protección de los consumidores, etc.

3.6 RÉGIMEN JURÍDICO APLICABLE

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 por qué 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.

3.6.1 LA VÍA PATENTARIA

Dentro de los delitos informáticos, existe uno que muestra como la tecnología computacional y las redes informáticas van superando la realidad

legislativa, este delito se conoce como Cybersquatting, que se puede definir como la práctica de registrar furtivamente en Internet como nombres de dominio, marcas conocidas sobre las que no se tiene derecho alguno. El problema es que la mayoría de las leyes de propiedad industrial no reconocen este acto como un ilícito.

La solución que se implantó en Estados Unidos para detener y castigar estos actos fue la creación de una nueva ley denominada “The Anticybersquatting Consumer Protection Act”.

Para fines de nuestro tema exponemos la existencia de actividades delictivas que podrían afectar la información relativa a la obtención de la protección de derechos de propiedad industrial como marcas, patentes de invención o de procedimientos, diseños industriales y modelos de utilidad; como sucede en los casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y el llamado “know how” estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada. Tal vez, en estos casos, se podrían aumentar las sanciones independientemente de que sean administrativas, civiles o penales, ya que el medio utilizado para espiar y obtener la información no fue la violencia, pero sí en cambio, un medio silencioso, imperceptible, que causa un daño más grave a las empresas por no tener conocimiento de éste.

Cabe destacar, que en nuestro país, la Ley de Propiedad Industrial ha tenido que reformarse a efecto de tipificar su relación con los delitos informáticos y electrónicos, también son considerados como delitos falsificar, producir, almacenar, transportar, introducir al país, distribuir o vender en forma dolosa y con fin de especulación comercial, marcas protegidas.

Además se contempla como delito en la fracción III del artículo 223 de la citada Ley, el aportar o proveer de cualquier forma, a sabiendas, materias primas o insumos destinados a la producción de productos “piratas”. Por lo que los especialistas en sistemas informáticos que llegasen a crear los programas lógicos

para realizar los moldes o incluso dirigir la producción de tales objetos, encuadran perfectamente en tal hipótesis, aunque se debiera contemplar la calificativa en el delito, si esos insumos fueran software o programas informáticos, ya que su utilización permite que las falsificaciones alcancen un grado de perfección y sea imposible percibir la falsedad de dicho objeto para la mayoría de las personas.

3.6.2 LA VÍA AUTORAL

El problema legal más importante, por mucho, que afecta a la industria de cómputo en relación a los derechos de autor hoy en día es la piratería informática, que consiste en el copiado o uso ilegal de programas o software.

Las nuevas técnicas han dado lugar a la creación de nuevos formatos en donde están plasmadas las obras autorales. Así, por ejemplo, tenemos el mp3 para el caso de obras musicales, con todas las controversias que se han planteado y que, ahora, no vamos a comentar; las técnicas de digitalización y compresión digital se están aplicando a las obras creadas por el intelecto y estas obras han encontrado en Internet otra vía para su comercialización. Dichas técnicas ofrecen una serie de ventajas como pueden ser una mejor calidad de las obras, reducción de costos a la hora de la reproducción o mayor interactividad con el usuario, pero también se plantean algunos riesgos, siendo el principal la dificultad de los autores a la hora de controlar su obra. Así pues, la Propiedad Intelectual se encuentra ante nuevos retos.

Según estadísticas recientes, “la piratería informática cuesta a los desarrolladores de software miles de millones de dólares al año, los fabricantes de software estiman que por cada paquete vendido los piratas ya han hecho cuatro copias no autorizadas.”⁸⁹

⁸⁹ <http://www.ciencia.vanguardia.es/ciencia/portada/p351.html>

El copiado ilegal puede ser efectuado por personas o compañías que desean usar copias gratis de paquetes de software lo que provoca que éstas sean susceptibles a la acción jurídica por parte de los autores afectados.

Tal acción puede establecerse en base a la legislación sobre derechos de autor, que puede estar contemplada en leyes civiles, leyes penales, o leyes especiales. En el caso de nuestro país los derechos de autor fueron ubicados dentro de la Ley Federal del derecho de Autor, y dentro del Código Penal Federal.

Las controversias derivadas de la violación a los derechos de autor en nuestro país pueden tener como consecuencia reparación de daños y perjuicios por la vía civil, infracciones administrativas, o incluso penas corporales impuestas por jueces penales. 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.

Existen ciertas modalidades de “piratería” que deben ser tipificadas como delitos y otras no por ejemplo:

a) Copias caseras: son las fabricadas por los usuarios, no constituyen delitos porque por lo general no existe un fin de lucro

b) Copia corporativa: se adquiere un ejemplar original para asegurarse la asistencia técnica en caso de ser necesario y a partir de ésta se fabrican copias para ser instaladas en todas las computadoras existentes en una empresa. Obviamente no constituye delito, pero si puede dar lugar a una acción civil.

c) Clubes de usuarios: mediante el pago de un arancel o cuotas se pueden obtener copias en préstamo, canje o alquiler, para elaborar nuevas copias a partir de estas, aquí al haber un fin de lucro hay acción delictiva.

d) Suministro de copias como “estimulo” de venta de computadoras: los comercios o empresas que venden hardware “cargan” en el disco rígido del comprador

copias “piratas” que el usuario no tiene que comprar y así abaratan el precio final para éste, aquí hay acción delictiva.

e) Fabricación y venta de copias en comercio: si hay acción delictiva.

f) Copiado de fuentes: este consiste en que empleados de una empresa obtienen una copia de un determinado software hecho a medida de ésta, lo modifican y lo venden como si fuera un desarrollo propio. También deberá ser considerado delito.

Es conveniente que se empiece a regular con más precisión los derechos de autor en el área de las páginas web, incluyéndose con esta denominación en las leyes, considerando que también son portadoras de un espíritu de creación intelectual, para que así se puedan proteger los derechos de autor plasmados en los nuevos medios electrónicos.

3.6.3 LA VÍA CIVIL

Aun cuando cierta conducta no esté tipificada como delictuosa, puede implicar el quebrantamiento de otras normas generales como las del derecho civil, si al quebrantar dichas normas se causa un daño y se obra con culpa en sentido amplio, estaremos ante lo que la doctrina reconoce como hechos ilícitos o cuasidelitos, generadores de la obligación de responsabilidad civil. Según el maestro Bejarano Sánchez, “para que nazca la obligación de responder civilmente, debe existir como presupuesto un hecho ilícito caracterizado por ser una acción antijurídica, culpable y dañosa.”⁹⁰

Así, los actos informáticos dañosos que no puedan ser encuadrados dentro de la norma típica, pero que sí reúnan los requisitos del hecho ilícito civil, podrán ser enmendados según lo expuesto mediante la vía civil; para que se indemnicen los daños y perjuicios ocasionados; pensemos en el caso de difamación por medio

⁹⁰ Cfr. Bejarano Sánchez, Manuel. “Obligaciones Civiles” 5ª. ed., Oxford, México, 2002. p. 171.

del Internet hacia una empresa por sus competidores, si tal acción no se encuentra contemplada dentro del ordenamiento penal, ya sea por política económica o por aplicación del principio penal de “la ultima ratio”, por la vía civil se podrá tener acción para que se cumpla con la obligación de responsabilidad civil.

Dentro del área civil y comercial, se aprecia una amplia legislación en todo el planeta. La Comisión de Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL), ha promovido diversas convenciones internacionales sobre el comercio electrónico, debemos recordar, que con el boom de las nuevas tecnologías informáticas, han cambiado los viejos métodos comerciales de transacciones de bienes y servicios, por lo que una inmensa cantidad de contratos mercantiles se llevan a cabo hoy en día por vía electrónica, mediante el uso de computadoras; además, se le ha conferido al documento electrónico un valor de documento fiable, y medio de prueba en juicio, como también lo establecen en nuestro país, el Código Federal de Procedimientos Civiles o el Código de Comercio, en la búsqueda de establecer una protección integral de los derechos civiles y comerciales más trascendentes.

3.6.4 LA VÍA PENAL

En la gran mayoría de las legislaciones internacionales y en nuestro país, si se actualiza un delito informático el Estado reprimirá al autor del hecho castigándolo principalmente con una pena privativa de la libertad que es característica de la materia, o en su defecto algunas de otra índole, pero además de las anteriores, impondrá al sujeto activo del delito la obligación de indemnizar el daño causado, esto es la responsabilidad civil.

Por ello, en nuestro país, la reparación del daño proveniente de un ilícito penal se debe tramitar como un incidente de responsabilidad civil en el proceso penal instaurado contra el autor del delito: “Cuando un solo hecho es a la vez delito civil y delito penal, la víctima tiene la facultad de ejercer su acción civil ante

el tribunal represivo, que entonces conoce simultáneamente de ambas acciones, se constituye en parte civil”.⁹¹

Cuando se comete un delito informático, se puede causar un daño físico o moral que debe ser reparado por el autor del hecho delictivo, así, por decir, si se atentara contra diversas personas por medio de un ordenador, utilizando la técnica de salami, en la que se hicieran pequeños desvíos de fondos casi imperceptibles de varias cuentas hacia una nueva cuenta apócrifa, en caso de encuadrar en un tipo penal, al sujeto agente se le podrá seguir un proceso penal para que vaya a la cárcel, pero también se buscará que regrese el dinero de ser posible o lo pague, como sucedería con cualquier otra clase de delito.

De lo anterior, se desprende que la vía penal es idónea para que se cumplan los intereses públicos y los intereses privados lesionados por la actividad delictuosa en materia informática, ya que por medio de esta vía se pueden llevar a cabo los fines del derecho penal y se pueden hacer valer derechos transgredidos del orden civil.

Considerando además, que el *ius puniendi* observa como uno de sus fines la prevención general y especial, positiva o negativa del delito; aunque el tipificar algunos actos informáticos como delictuosos no resuelva en su totalidad el problema, considero que es una buena fuente de intimidación hacia las personas para no cometerlos, por lo que proponemos se legisle en esta materia adecuadamente.

3.7 SITUACIÓN INTERNACIONAL

Los delitos informáticos constituyen una gran laguna en nuestras leyes penales, así pues, el derecho comparado nos permite hacer una lista de los delitos que no están contemplados en el Código Penal y que requieren análisis urgente

⁹¹ (GAUDEMET) cit. Bejarano Sánchez. 1999.

por parte de nuestros académicos, penalistas y legisladores. Por lo tanto, en este apartado se verá las disposiciones legales que implementaron algunos países⁹² para enfrentarse con el problema en estudio:

3.7.1 ALEMANIA. Se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

1. Espionaje de datos.
2. Estafa Informática.
3. Falsificación de datos probatorios.
4. Alteración de Datos.
5. Sabotaje Informático.
6. Utilización abusiva de cheques o tarjetas de crédito.⁹³

Cabe mencionar que esta solución fue también adoptada en los Países Escandinavos y en Austria.

Alemania también cuenta con una Ley de Protección de Datos, en la cual, en su numeral primero menciona que "el cometido de la protección de datos es evitar el detrimento de los intereses dignos de protección de los afectados, mediante la protección de los datos personales contra el abuso producido con ocasión del almacenamiento, comunicación, modificación y cancelación (proceso) de tales datos. La presente ley protege los datos personales que fueren almacenados en registros informatizados, modificados, cancelados o comunidades a partir de registros informatizados".⁹⁴

3.7.2 AUSTRIA. Ley de reforma del Código Penal del 22 de diciembre de 1987, la cual contempla los siguientes delitos:⁹⁵

1.- Destrucción de Datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

⁹² <http://www.legislacionmundial.com>

⁹³ <http://wings.buffalo.edu/law/bclc/germind.htm>

⁹⁴ <http://www.germanwings.com/es/Proteccion-de-datos.htm>

⁹⁵ <http://www.loc.gov/law/help/guide/nations/austria.php#legislative>

2.- Estafa Informática.(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.

3.7.3 CHILE. Cuenta con una ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993, la cual en sus cuatro numerales menciona:⁹⁶

Art. 1.- "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento...".

Art. 2.- " El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él..".

Art. 3.- " El que maliciosamente revele o difunda los datos contenidos en un sistema de información....".

Art. 4.- " El que maliciosamente revele o difunda los datos contenidos en un sistema de información....".

3.7.4 ESTADOS UNIDOS. Cabe mencionar, la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030). Que modificó al Acta de Fraude y Abuso Computacional de 1986. Dicha 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

⁹⁶ <http://www.todoelderecho.com/SeccionInternacional/Codigos/Chile/CODIGO%20PENAL-chile.htm>

sólo de manera imprudencial la sanción fluctúa entre una multa y un año de prisión.⁹⁷

Es interesante también señalar que el Estado de California, en 1992 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 de 1994.

3.7.5 ESPAÑA. En el Nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicará pena de prisión o multa. En lo referente a:⁹⁸

a) La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

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

c) En materia de estafas electrónicas, el nuevo Código Penal de España, 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.

3.7.6 FRANCIA. Las disposiciones penales están contempladas en sus numerales del 41 al 44, los cuales contemplan lo siguiente:⁹⁹

Artículo 41. " El que hubiere procedido o mandado proceder a la realización de tratamientos automatizados de información nominativa sin que hubieran sido

⁹⁷ <http://legal.web.aol.com/resources/legislation/ecpa.html>

⁹⁸ <http://www.law.unican.es/incade/lex/cpint.htm>

⁹⁹ <http://www.legifrance.gouv.fr/citoyen/code00.ow?heure2=032030494971&code=CPENALLL.rcv&no=66>

publicados los actos reglamentarios previstos en el artículo 15 o formuladas las denuncias previstas en el artículo 16.

Artículo 43. "El que habiendo reunido, con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento, informaciones nominativas cuya divulgación tuviere como efecto atentar contra la reputación o la consideración de la persona o la intimidad de la vida privada; hubiere, sin autorización del interesado y a sabiendas, puesto tales informaciones en conocimiento de una persona que no estuviere habilitada para recibirlas.

Artículo 44. "El que, disponiendo de informaciones nominativas con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento las hubiere desviado de su finalidad.

3.7.7 INGLATERRA. 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.¹⁰⁰

3.7.8 HOLANDA. El 1º de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:¹⁰¹

a) El hacking.

b) El phreaking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).

c) La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).

d) La distribución de virus.

¹⁰⁰ <http://www.loc.gov/law/help/guide/nations/england.php>

¹⁰¹ <http://www.loc.gov/law/help/guide/nations/netherlands.php>

3.7.9 ITALIA. En un país con importante tradición criminalista, como Italia, nos encontramos tipificados en su Código Penal los siguientes delitos:¹⁰²

a) Acceso Abusivo. Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware).

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

c) Introducción de virus informáticos. Es penalmente responsable aquel que cree o introduzca a una red programas que tengan la función específica de bloquear un sistema, destruir datos o dañar el disco duro.

d) Intercepción abusiva.- Es un delito que se comete junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas.

e) Falsificación informática. Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas.

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

g) Abuso de la detención o difusión de Códigos de acceso (contraseñas).

Analizando lo anteriormente expuesto, se advierte que en diferentes países se han preocupado por el mal uso que pueda tener los grandes avances tecnológicos, el cual sin una reglamentación adecuada pueden desbordarse y salir de un control, así pues, la apremiante necesidad de que en nuestro Código Penal Federal, se contemplen de una forma u otra.

¹⁰² http://www.jus.unitn.it/cardoza/law_web/home_it.html

La legislación y regulación sobre los delitos informáticos en otros países, constituye un gran avance en la materia, pero no se va a realizar una crítica a las anteriores disposiciones legales, ya que cada país contempló dichas normas de acuerdo a sus necesidades propias; podemos observar que algunos países se enfocaron propiamente a proteger el derecho a la privacidad, y a la propiedad intelectual, o como el que disponga de informaciones nominativas y haga un mal uso de ello; otros tantos a proteger al patrimonio de las personas afectadas como en los fraudes informáticos etc. Las legislaciones de otros países nos ayudan y nos dan la pauta para que nuestros legisladores contemplen las figuras delictivas de "delitos informáticos", de acuerdo a nuestra propia realidad.

3.8 ORGANIZACIÓN DE LAS NACIONES UNIDAS

En el contexto internacional, en el marco del Décimo Congreso de Naciones Unidas sobre prevención del delito y tratamiento del delincuente celebrado en Viena, Austria, la ONU ha reconocido que los delitos por computadora constituyen un grave problema, ya que las leyes, los sistemas de impartición de justicia y la cooperación internacional no se han adecuado a los cambios tecnológicos.¹⁰³

Las conductas o acciones que considera las Naciones Unidas como delitos informáticos¹⁰⁴ son las siguientes:

1) Los fraudes cometidos mediante manipulación de computadoras: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común.

2) La manipulación de programas es un delito que consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas que tienen conocimiento especializados en programación informática.

¹⁰³ <http://www.uncjin.org/Documents/congr10/10s.pdf>

¹⁰⁴ http://www.delitosinformaticos.com.mx/pro_pc.htm

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

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

5) Falsificaciones informáticas ocurren cuando se alteran datos de los documentos almacenados en forma computarizada.

6) Como instrumentos las computadoras pueden utilizarse también para efectuar falsificación de documentos de uso comercial.

7) 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.

8) Los virus son una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.

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

10) La 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.

11) Acceso no autorizado a servicios o sistemas informáticos; realizado por motivos diversos desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

12) Piratas Informáticos o Hackers los cuales realizan accesos a menudo desde un lugar exterior, situado en la red de telecomunicaciones.

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

3.9 MANUAL DE LA ONU PARA ERRADICAR DELITOS INFORMÁTICOS

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

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, en razón de que los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada.¹⁰⁵ Asimismo, la ONU 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 qué tipo de conductas deben constituir delitos informáticos.

¹⁰⁵ <http://www.iurilex.org/man-onu/044n1soc.html>

- 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.
- Falta de 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.

La propia Organización instó a los Estados miembros a intensificar sus esfuerzos para combatir este tipo de conductas, entre otras medidas, mediante la creación de nuevos tipos penales y procedimientos de investigación, para hacer frente a estas nuevas y sofisticadas formas de actividad criminal.

Para enfrentarse a los problemas causados por todos estos delitos relacionados con la informática e Internet, numerosos países se han unido y firmado la Convención del Consejo Europeo contra el Cibercrimen¹⁰⁶, que requiere que los miembros consideren delictivas todas las actividades relacionadas con el Ciberterrorismo y otras formas de delitos informáticos. Los estados que no forman parte de esta asociación como, Estados Unidos, Canadá, Japón y Sudáfrica también se han adherido a ella, México aún no se ha adherido a dicha Convención lo cual es un error que se podría componer. Gracias a esta cooperación, las actividades como la piratería, la intervención en sistemas informáticos, el fraude, la falsificación y otros delitos relacionados se consideran ahora ilegales en todos los países firmantes del acuerdo. Este acuerdo también facilita la cooperación

¹⁰⁶ <http://www.conventions.coe.int>.

internacional para detectar, investigar y perseguir tales delitos, así como para usar medios electrónicos para reunir pruebas para delitos relacionados con el terrorismo, el crimen organizado y otros delitos que se llevan a cabo a escala global mediante la organización de ordenadores y de redes.

CAPITULO IV

ANÁLISIS JURÍDICO DE LOS ELEMENTOS DEL TIPO PENAL EN LOS DELITOS INFORMÁTICOS

Para que una conducta sea catalogada como delito, ésta debe encontrarse descrita en la ley penal para que pueda ser perseguible por el aparato de justicia social, así entonces, nace la tipificación de conductas delictivas.

La tipicidad se puede considerar como una expresión propia del Derecho Punitivo, equivalente técnico del apotegma político "*nullum crimen sine lege*", bien con el nombre con que ahora técnicamente se le designa, bien como garantía de libertad consagrada en la parte dogmática de las Constituciones políticas, la tipicidad ha sido, desde el inicio de los regímenes de derecho, el fundamento del hecho punible.

Las legislaciones de la casi totalidad de los países modernos proclaman expresamente este principio. Así, por lo que respecta a México, el artículo 14 de la Constitución Federal dispone que: "en los juicios del orden criminal queda prohibido imponer por simple analogía y aún por mayoría de razón pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata"; y el artículo 7 del Código Penal Federal estatuye que: "Delito es el acto u omisión que sancionan las leyes penales".

Así, nuestra carta magna establece que los delitos deben estar previamente establecidos en la ley, y a estas descripciones se les llama tipos penales.

El tipo penal se define como: "el injusto descrito concretamente por la ley en sus diversos artículos y a cuya realización va ligada la sanción penal".¹⁰⁷

¹⁰⁷ Mezger Edmundo "Tratado de Derecho Penal" Tomo I. Revista de Derecho Privado, Madrid España, 1955.p.190

También, “el tipo penal se puede definir como la creación legislativa, la descripción que el Estado hace una conducta en los preceptos penales”.¹⁰⁸

El tipo penal encuentra su fundamento en el “principio de legalidad”, concretamente al antes referido principio de “reserva legal”, ya que solamente el legislador puede realizar las definiciones de lo que considera como delito, encontrando su fundamento en el artículo 73, fracción XXI, de la Constitución Política de los Estados Unidos Mexicanos.

En la comisión de un delito siempre encontraremos diversos elementos que deben encuadrar dentro del tipo penal, a continuación pasaremos a analizar cada uno de ellos:

4.1 ELEMENTOS GENERALES

4.1.1 SUJETO ACTIVO. “El sujeto activo, es la persona que ejecuta la conducta típica y que en el tipo se indica por lo común con las partículas “Al que”, “El que”, “Al responsable”, “Al autor”, entre otros, es decir, se designa genéricamente a la persona”.¹⁰⁹

Es decir, el sujeto activo es quien realiza la conducta delictiva; también se le conoce con el nombre de agente, sujeto-agente, actor o autor.¹¹⁰

4.1.2 SUJETO PASIVO. Para el maestro JIMÉNEZ DE ASÚA, puede ser sujeto pasivo del delito “todo poseedor de un bien o de un interés jurídicamente protegido”.¹¹¹

¹⁰⁸ Castellanos Tena Fernando. Op Cit. Pág. 167.

¹⁰⁹ Orellana Wiarco Octavio A. “Curso de Derecho Penal” Parte General. Edit. Porrúa, México, 1999, p.223

¹¹⁰ Cfr. Cerezo M. José “Autoría y Participación en el Código Penal”, en Revista Anuario de Derecho Penal y Ciencias Penales, fascículo III, Madrid, 1979, págs. 567-581. Según cita Reyes Echandia, Alfonso, “Tipicidad”, 6° ed., Edit. Temis, Bogota, pag.26

¹¹¹ Jiménez Huerta Mariano. “Derecho Penal Mexicano: Introducción al estudio de las figuras típicas, Porrúa, México, 1977.

Los sujetos pasivos pueden ser en general personas físicas, personas morales, organismos colectivos con personalidad jurídica conforme al Derecho Público (Federación, entidad federativa, municipio) o incluso un ente colectivo desprovisto de personalidad jurídica (familia, colectividad nacional o internacional).

Por ejemplo, aunque el derecho no estructura el grupo familiar como una verdadera persona jurídica, esto es, como titular de derechos subjetivos, lo reconoce como sujeto de intereses jurídicos. Como también la comunidad social que constituye el pueblo de una nación aunque desprovista como tal de personalidad jurídica y de capacidad para ejercitar derechos subjetivos, es portadora o titular de intereses o bienes jurídicos que son lesionados o puestos en peligro por determinados delitos. Esto acontece, por ejemplo, en los delitos contra la seguridad pública, contra la salud, contra la moral pública, o bien los delitos contra el derecho internacional por ejemplo.

4.1.3 BIEN JURÍDICO. Según el maestro JIMÉNEZ HUERTA, el bien jurídico “es el interés o valor de la vida humana que específicamente la ley penal tiene por objeto tutelar y proteger”.¹¹²

Dichos bienes o intereses jurídicos que la ley penal protege son los que la colectividad considera más importantes para la subsistencia y pleno desarrollo social y humano.

“Las figuras típicas se determinan precisan y definen por imperio del bien jurídico; no hay norma penal que no esté destinada a la tutela de un valor y que no tenga por fin la protección de un bien jurídico. Así por ejemplo, la norma que incrimina el homicidio, tutela la vida; aquella que incrimina el robo, la propiedad; y aquella que incrimina la bigamia, el orden familiar”.¹¹³

¹¹² Jiménez Huerta Mariano, op. cit. P.234

¹¹³ Idem, p. 119

4.1.4 OBJETO MATERIAL. “Es aquello sobre lo cual se concreta el interés jurídico que el legislador pretende tutelar en cada tipo penal y al cual se refiere la acción u omisión del agente”.¹¹⁴

Está constituido por la persona o cosa donde recae materialmente la acción, por lo que también se conoce como *objeto de la conducta*, pudiendo coincidir en una misma persona tanto el objeto jurídico como el objeto material, cítese por ejemplo el homicidio; sin ser necesario que ocurra siempre como en el caso de robo.

4.1.5 CONDUCTA. La Suprema Corte ha considerado que dentro del significado de conducta debe entenderse “*el comportamiento corporal voluntario*”, según cita de PORTE PETIT.¹¹⁵

La conducta también llamada acto o acción, lato sensu, es la manifestación externa de la voluntad por parte del sujeto activo; en el delito y su tipificación puede manifestarse mediante haceres positivos (acciones) o negativos, es decir, por abstenciones como en el caso de la omisión o la comisión por omisión.

En estricto sensu, la acción es todo hecho humano voluntario, todo movimiento voluntario del organismo humano capaz de modificar el mundo exterior o de poner en peligro dicha modificación.

La omisión, en cambio, radica en un abstenerse de obrar, simplemente de una abstención, un dejar de hacer; en dejar de actuar; “el sujeto activo por no hacer lo que se espera que haga, deja inerte el mundo externo, cuya mutación se aguarda”.¹¹⁶

4.1.6 RESULTADO. MAGGIORE define al resultado como “la consecuencia de la acción, que la ley considera decisiva para la realización del tipo del delito, o lo que

¹¹⁴ Reyes Echandia, Alfonso, “Tipicidad”, 6° Ed, Edit. Temis, Bogotá, pág. 81 y 82.

¹¹⁵ Diccionario Jurídico 2000. Informática Jurídica Profesional.

¹¹⁶ Castellanos Tena, Fernando “Lineamientos elementales de Derecho Penal”, edit. Porrúa, México, 1989, pág.118

es lo mismo, la realización del tipo del delito fijado por la ley. El resultado es el efecto voluntario en el mundo exterior, o más precisamente, la modificación del mundo exterior como efecto de la actividad delictuosa”.

PAVÓN VASCONCELOS nos recuerda que “el resultado es un efecto de la conducta, pero no todo efecto tiene tal carácter, sino sólo aquel o aquellos relevantes para el Derecho, por cuanto éste los recoge dentro del tipo penal”, y para clarificar, cita como ejemplo un homicidio con arma de fuego; cuando el sujeto agente jala el gatillo del arma, existen resultados de dicha acción tales como la explosión de la pólvora y del cartucho, la salida del proyectil, la lesión producida al hacer impacto en el cuerpo de la víctima, todos estos solo son “efectos” importantes, por cuanto tienen un preciso valor en la serie causal iniciada por el movimiento corporal, pero solo tiene rango de resultado jurídicamente hablando la muerte de la víctima para el delito de homicidio.¹¹⁷

En los llamados delitos “formales” de simple conducta como la posesión de armas o los de “peligro” como en el contagio de enfermedad, el resultado material (externo, físico) no se da, pero siempre existirá un resultado típico que, en estos delitos se agotará al momento de ejecutarse el acto descrito en el tipo.

4.2 ELEMENTOS ESPECIALES

4.2.1 REFERENCIAS TEMPORALES. “La punibilidad de la conducta o del hecho queda a veces condicionada a determinadas referencias de tiempo que indican el momento en que el hecho se debe ejecutar para que resulte típicamente adecuado”.¹¹⁸

La temporalidad de la conducta puede ser ilimitada o circunscrita:

¹¹⁷ Cfr. Pavón Vasconcelos, Francisco “Manual de Derecho Penal Mexicano”, 10ª Ed. Porrúa, México, 1973, pag. 232

¹¹⁸ Op. Cit., p. 310

*Ilimitada; significa que la conducta puede ejecutarse en cualquier momento.

*Circunscrita; sólo es jurídicamente relevante la que se desenvuelve en el momento a que se refiere el tipo.

4.2.2 REFERENCIAS ESPACIALES. Las referencias espaciales contenidas en el tipo penal indican el lugar o espacio físico determinado para que se actualice la acción positiva o negativa delictuosa.

Tales referencias espaciales deben tomarse en cuenta en una disyuntiva de técnica legislativa-penal para la creación de tales leyes, por lo que el espacio o lugar puede servir para la integración de un tipo penal básico o fundamental, siendo un ejemplo de éste el robo que se puede cometer en cualquier parte, o bien para agravar o atenuar un tipo como lo es el robo calificado por cometerse en lugar cerrado.

4.2.3 REFERENCIAS OCASIONALES. Como en el caso de las anteriores, las referencias ocasionales pueden estar enfocadas a la plena y exacta configuración de un tipo penal específico o a las agravantes o atenuantes de la sanción.

En el caso del tipo que solo se actualiza en una determinada ocasión podemos citar como ejemplo algunas hipótesis del delito de traición a la patria, en donde debe mediar como presupuesto del delito y referencia ocasional del tipo una invasión extranjera.

En el segundo caso, donde dichas referencias ocasionales sirven para determinar una agravante de la pena, citemos por ejemplo el robo agravado por ser cometido durante una situación causada por una catástrofe.

4.2.4 MEDIOS DE COMISIÓN. Aun cuando por lo general el medio comisivo resulta indiferente, en ciertos casos la exigencia de la ley al empleo de

determinado medio lo hace esencial para integrar la conducta o para hacer operar alguna agravante de la pena como ya hemos mencionado.¹¹⁹

En la configuración de un delito el medio puede determinar el delito como lo es el caso del delito sexual de violación, en donde el acceso carnal es una función perfectamente ajena al derecho punitivo, si no va acompañada (salvo el caso del menor de edad o incapaz de comprender el significado del hecho) de violencia física o moral.

En otros casos el medio califica el delito como el homicidio o las lesiones por medio de envenenamiento, asfixia, etc.

4.2.5 ELEMENTOS SUBJETIVOS. Los tipos contienen muy frecuentemente elementos subjetivos por cuanto están referidos al motivo y al fin de la conducta descrita, o al conocimiento de alguna circunstancia, en dichos casos se incluyen frases como lo son: “proponiéndose un interés”, “con propósito de causar perjuicio”, “para fines propios o ajenos”, “propósito de lucro”, “a sabiendas”, “con conocimiento de esa relación”, entre otros.¹²⁰

Así, en la situación de un homicidio en relación de parentesco solo se configurará dicho delito o en su caso agravante (dependiendo de la ley aplicable) si el homicida tiene conocimiento de esa relación o parentesco, en caso contrario se hablará solo de homicidio.

5.2.6 ELEMENTOS NORMATIVOS. Los elementos normativos son presupuestos del injusto típico, forman parte de la descripción contenida en los tipos penales y hacen referencia a la antijuricidad, se expresan mediante formulas tales como “sin derecho”, “sin causa justificada”, “injustificadamente” o “al que indebidamente”.¹²¹

Los elementos normativos indican que el comportamiento realizado por el delincuente contraviene la norma jurídica. La propia norma lo resalta con

¹¹⁹ Idem, p. 310

¹²⁰ Amuchategui R. Irma, Villasana Ignacio. “Diccionario Jurídico: Derecho Penal, Vol. I, Edit. Oxford. México, 2002.

¹²¹ Op. cit, 2002.

expresiones como las indicadas, lo que interpretado a *contrario sensu* significa que el comportamiento no sería antijurídico. Por ejemplo si alguien toma una cosa mueble ajena “con derecho” “o bien “con consentimiento”, la conducta no es ilícita.

4.3 ELEMENTOS DE CALIDAD

4.3.1 SUJETO ACTIVO. A veces el tipo establece determinada calidad en el sujeto activo a la cual queda subordinada la punibilidad de la acción bajo un concreto tipo delictivo, ello excluye la posibilidad de ejecución de la conducta por cualquier sujeto y por tal razón se denominan los delitos propios, particulares o exclusivos, para diferenciarlos de los delitos que se pueden cometer por un sujeto común o indiferente.¹²²

Así, los delitos cometidos por servidores públicos, como pueden ser la concusión o el peculado, el sujeto activo debe contar con dicha calidad, o sea la de ser servidor público, ya que tal delito no puede encuadrar en la acción de cualquier persona civil que no posea tal calidad.

4.3.2 SUJETO PASIVO. En otras ocasiones la ley exige determinada calidad en el sujeto pasivo, operándose el fenómeno de la ausencia del elemento típico cuando el sujeto no la reúne y por ende la impunidad de la conducta o del hecho.

Por lo que la referencia de calidad hablando de sujeto pasivo puede determinar algunos delitos cometidos contra bienes jurídicos de entes de derecho público como los delitos contra el servicio público, contra la seguridad nacional, o bien ser contra intereses jurídicos de entes de derecho privado como personas físicas o morales.

La calidad del sujeto pasivo, se incluye en la hipótesis típica para delimitar y determinar quién puede ser el sujeto pasivo del delito, por lo que la calidad es una

¹²² Idem, p. 309

referencia especial para la integración de tipos que el legislador considere pertinentes a fin de que puedan ser punibles las conductas dañosas que recaen sobre determinados sujetos pasivos o bien para incidir en una agravante sobre la penalidad.

4.3.3 OBJETO MATERIAL. Como ya sabemos la distinción entre objeto jurídico y el objeto material, en este inciso hacemos referencia al segundo, sobre el cual recae la conducta, es decir, al objeto material o corporal de la acción, el cual puede tener una calidad específica, por ejemplo en el robo, se destaca que la cosa robada (sobre la que recae la acción) debe ser forzosamente mueble y ajena, de ser así, se cumplirá la calidad del objeto material para la adecuación de la conducta al tipo legal.

4.4 ELEMENTOS DE CANTIDAD

4.4.1 SUJETO ACTIVO. Los elementos de cantidad en el sujeto activo son pocas veces de importancia, debido a que por lo común el delito puede ser cometido por una o más personas indiferentemente y no afectará la naturaleza del delito, ya que la pluralidad del sujeto activo es un elemento de la autoría y formas de participación en el hecho delictivo.

4.4.2 SUJETO PASIVO. En las leyes penales, la cantidad de individuos que puedan resultar sujeto pasivo del delito algunas veces son importantes por cuanto pueden agravar la pena (lesiones u homicidio culposos a dos o mas personas en determinadas hipótesis) o bien incidir en un delito específico como lo es el genocidio donde la ley especifica que el sujeto pasivo sea un grupo de personas con determinada característica (étnica, racial o religiosa), por lo que así el sujeto pasivo debe ser el grupo humano o individuos de dicho “grupo”, y con el fin de exterminio que es un elemento subjetivo.

4.4.3 OBJETO MATERIAL. La cantidad del objeto material, entendiendo por este el objeto físico sobre el que recae la acción delictuosa, no interesa para el proceso de subsumir el hecho en un tipo legal, siempre y cuando se haya dañado o puesto en peligro un bien jurídico, por lo que muy rara vez se podrá constituir un tipo en donde se requiera una cantidad determinada de objetos materiales.

Por ejemplo siguiendo los lineamientos del maestro JIMÉNEZ DE ASÚA, en el delito de robo, el objeto jurídico afectado es el patrimonio, el sujeto pasivo es el titular de dicho patrimonio, el objeto material comprende lo robado, pero al materializarse en el mundo fáctico el delito de robo será lo mismo robar un billete de 100 pesos o robar 10 monedas de 10 pesos, por lo que se aprecia claramente que la cantidad de objetos materiales no influirán en la comisión del delito, solo en su punibilidad que será atendida en base al daño producido, en este caso patrimonial, y no a la cantidad de objetos materiales sobre los que recayó la conducta típica.¹²³

4.5 ANÁLISIS DEL TIPO PENAL EN LOS DELITOS INFORMÁTICOS

Basados en la información anteriormente expuesta procederemos al análisis de los elementos que se encuentran en los delitos de acceso ilícito a sistemas y equipos de informática que aparecen actualmente en el Código Penal Federal, contenidos específicamente en el título II del Capítulo noveno de dicho ordenamiento legal.

4.5.1 EL SUJETO ACTIVO Y SUJETO PASIVO

Como ya se ha dicho el sujeto activo del delito es aquella persona que lleva a cabo la realización de la conducta calificada como delictiva, es decir, el delincuente. Mientras que el sujeto pasivo es aquella persona en la que recae el daño.

¹²³ Jiménez de Asúa, Luis “Teoría del delito” Cursos jurídicos temáticos hispanoamericanos, Iure Editores, México, 2006. 711 p.p.

Hay que resaltar que a veces el tipo establece determinada calidad en el sujeto activo a la cual queda subordinada, por así decirlo, la punibilidad de la acción bajo un concreto tipo delictivo; ello excluye la posibilidad de ejecución de la conducta (acción u omisión) por cualquier sujeto común o indiferente.

En el tema que nos ocupa, *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 ilícitos, hoy en día cualquier persona con medianos conocimientos de informática puede llegar a ser un delincuente informático ya que la posibilidad de acceder a algún sistema informático se puede realizar desde algún lugar remoto.

En nuestro Código Penal Federal sólo en los artículos 211 bis 3 y 211 bis 5 existen agravantes atendiendo a la calidad del sujeto activo, en el primero de ellos cuando el acto lo cometan servidores públicos o servidores en alguna institución de seguridad pública; en el segundo artículo señala que aumentará la penalidad cuando sea realizado por funcionarios o empleados del sistema financiero.

“Artículo 211 bis 3.- A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. **Si el responsable es o hubiera sido servidor público en una institución de seguridad pública,** se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.”

Atendiendo a lo que el legislador federal redactó en los tipos penales plasmados en los artículos 211 bis 2 a 211 bis 5 aparecen exigencias en el sujeto pasivo como son:

Artículos 211 bis 2 y 211 bis 3.- Aparece una calidad de sujeto pasivo al señalar al Estado como sujeto al que le es lesionado su bien jurídico:

“**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...”.

Artículos 211 bis 4 y 211 bis 5.- Aparece una calidad de sujeto pasivo cuando nombra a las instituciones del sistema financiero como entidades sobre las que recae el daño de la acción típica.

“**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.....”.

4.5.2 EL OBJETO MATERIAL Y EL BIEN JURÍDICO

Como ya quedó establecido anteriormente, en la doctrina penal mexicana se diferencia entre el objeto material y el objeto jurídico, siendo el primero la cosa, o bien la persona sobre la que recae el daño de un delito, mientras que el objeto jurídico es considerado el bien tutelado por la norma penal.

En este orden de ideas y de conformidad a lo establecido por los artículos 211 bis 1 a 211 bis 7 del CPF, podemos establecer que el objeto material en tales tipos penales estaría integrado por los datos portadores de información contenida en un sistema informático e inclusive el propio equipo computacional, ya que cabe recordar que se puede incurrir en este delito cuando se use, altere o se destruyan tales objetos.

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

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

En el caso de los delitos que utilizan como medio para su realización los elementos informáticos el objeto material será el objeto externo donde recaiga la acción, así, en el caso de fraude a alguna Institución del sistema Financiero por medio de una intrusión al su sistema a través de una computadora, los datos alterados o modificados son el objeto material de la acción, ya que representan un objeto corporal como lo es el dinero en efectivo independientemente del método con que el autor manipuló o engañó el sistema.

Por lo que respecta al bien jurídico tutelado por los artículos antes citados podemos señalar que es la confidencialidad y protección de la información que se almacena en los sistemas informáticos, perteneciendo al género de los delitos patrimoniales, debido a que en todos y cada uno de los tipos en comento se aprecia que el legislador hace referencia como elemento esencial de estos tipos penales, que exista “información” contenida en sistemas o equipos de informática, sin embargo, el legislador colocó a los delitos informáticos en el título noveno al saber que estas intrusiones y modificaciones de información en la realidad violentan varios bienes jurídicos y para ya no batallar a la hora de su legislación les colocó un título que sólo demuestra su falta de conocimiento en esta materia que demerita mucho su función legislativa.

4.5.3 CONDUCTA Y RESULTADO

La conducta punible se encuentra descrita por el tipo penal y puede ser de acción u omisión, en los tipos penales en análisis del 211bis 1 al 211 bis 5 del CPF, observamos que todos son de los llamados de acción, lo anterior se desprende de que tipifican conductas como “conocer, modificar, destruir o provocar pérdida” de información de un sistema o equipo informático, siendo todas estas actividades que requieren un accionar físico exterior del cuerpo humano.

“**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.”

Ahora bien, el resultado material en estos tipos penales en estudio se encuentra presente cuando se produce el daño, destrucción, pérdida, modificación o conocimiento sin autorización de la información contenida en sistemas o equipos de informática especificados en cada artículo.

En otros casos, cuando se utilicen los equipos informáticos como medio para cometer otros delitos, el resultado material dependerá del tipo de delito, por decir cuando se modifique una página web ilícitamente, el resultado material será la página modificada siempre y cuando se tipifique la acción de modificar dichas páginas sin autorización o se encuentre contenida subjetivamente dentro de otro tipo penal.

4.5.4 ELEMENTOS NORMATIVOS Y SUBJETIVOS

En los delitos informáticos el elemento normativo es importante ya que al igual que los elementos subjetivos pueden provocar atipicidad de la conducta, como lo pudiera ser la hipótesis en que se sustraiga información de un ordenador informático pero se justifique porque se cuente con el derecho para hacerlo.

Así, de los artículos 211 bis 1, 211 bis 2 y 211 bis 4, se puede apreciar que se exige como elemento normativo para establecer tipicidad el que el acto se realice por algún sujeto “sin autorización”.

“**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...”

En los artículos 211 bis 3 y 211 bis 5 se precisa la necesidad de que la acción sea desplegada por alguien que “estando autorizado” para acceder al sistema informático, pero “indebidamente” modifique, destruya, provoque pérdida o copie información de las Instituciones del Estado o del Sistema Financiero.

“**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...”.

Por otro lado, como ya se estableció, los elementos subjetivos son los que reflejan una especial culpabilidad del sujeto activo para la comisión de un delito, es decir, se refieren al ánimo de una persona demostrando su situación interna.

En los tipos penales el legislador ha colocado esos elementos subjetivos cuando hace mención a términos tales como: maliciosamente, dolosamente, a sabiendas, el que con conocimiento, el que intencionalmente, entre otras.

Ejecutando el análisis de los artículos en comento, no encontramos ningún elemento subjetivo, ni aun cuando el artículo 211 bis 7 prescribe que se aumentarán en una mitad las penas establecidas en todo el capítulo en análisis, cuando la información obtenida se utilice en provecho propio o ajeno, ya que no se hace referencia al ánimo de provecho para que existan tales figuras delictivas, sino que es una circunstancia agravante posterior e independiente el que la información no autorizada, su destrucción o modificación sea para la obtención de un provecho.

CAPITULO V

ANÁLISIS SOBRE EL REORDENAMIENTO DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL FEDERAL MEXICANO

5.1 DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL FEDERAL

Debemos destacar que en el Derecho Positivo Mexicano, el Código Penal Federal es la Ley Federal en la Legislación Mexicana que tipifica con mayor abundamiento a los delitos informáticos, aun así, proponemos que sean reordenados los delitos informáticos en un solo capítulo especial, por lo que a continuación transcribimos el texto actual concerniente al tema en este Código:

“Libro Segundo

Título Noveno

Revelaciones secretos y acceso ilícito a sistemas y equipos de
informática

[...]

Capítulo II

Acceso ilícito a sistemas y equipos de informática

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

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

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiere sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211bis 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.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo

general vigente en el Distrito Federal. Si el responsable es o hubiere sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, 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.”¹²⁴

Así mismo en los Artículos 424-bis, 424-ter y 368 se establece tipificación sobre la piratería informática, que a la letra dice:

“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 para quienes, 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.

Artículo 424-ter.- Se impondrá prisión de seis meses a seis años y de cinco mil a treinta mil días multa, a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial,

¹²⁴ Código Penal Federal, Edit. Porrúa, 2013.

copias de obras, fonogramas, videogramas o libros, a que se refiere la fracción I del artículo anterior.

Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en el artículo 424 Bis de este Código.¹²⁵

5.2 CRÍTICA AL CAPÍTULO II DEL TÍTULO NOVENO Y TÍTULO VIGÉSIMO SEXTO DEL CÓDIGO PENAL FEDERAL MEXICANO

En el Código Penal Federal se establecen condiciones especiales del Tipo, y, sólo se hace referencia a los sistemas y a los equipos ya protegidos por algún mecanismo de seguridad, cuestión que parece ser infundada ya que la violación de la propiedad o de la privacidad es la misma, ya se trate de un sistema protegido ó de uno sin clave alguna; sin embargo, en definitiva lo que se quiere proteger es el bien jurídico, pero tal calidad especial en el objeto material no debiera contemplarse, ya que en la mayoría de los casos los sistemas y equipos que se consideran caseros, no poseen mecanismo de seguridad alguno que los pueda considerar como incluidos dentro del tipo penal.

No se contemplan todos los tipos comunes de ataques informáticos, sólo se castiga el acceso ilícito a sistemas informáticos, pero qué pasa con los actos ya mencionados en otros capítulos como la modificación de una página web, cuyo titular sea cualquier simple mortal, o se introduzca un virus que ocasione una denegación de servicios o inhabilitación parcial del ordenador, no podría actualizarse el delito de daño en propiedad ajena ya que el concepto de cosa es aplicable al soporte y no a su contenido, es decir, una página web no puede asimilarse a lo que significa cosa, ya que no se trata de un material corpóreo ni se puede mostrar materialmente.

¹²⁵ Op. cit.

El simple descuido del legislador ha generado la exclusión del tipo cuando alguien autorizado copia información privada, y esto, en virtud de la importancia de los bienes a proteger, lo cual me parece inaceptable en términos jurídicos. Si en los casos en que el sujeto activo pertenece a las Instituciones Financieras, se debe agravar la pena, ya que la relación laboral y de confianza es la misma, y la no inclusión de este agravante no tiene fundamento jurídico o lógico alguno. Me parece más aceptada la redacción que imponga al fin de lucro como agravante genérica sin incriminar o desincriminar a las conductas que no tengan este objetivo.

Otra cuestión de análisis es que en dicho Código Penal se protege a las instituciones Financieras y al Estado, dejando excluidos a los particulares, sólo trata fugazmente de proteger estos últimos en el artículo 211 bis 1 del Código Penal; sin embargo, en la vida diaria los delitos informáticos son cometidos a personas y empresas particulares.

Como nos dice el licenciado Joel Gómez Treviño presidente de la Academia Mexicana de Derecho Informático, A.C., nuestro código no contempla todos los tipos más comunes de ataques informáticos. Además de que el Capítulo II titulado “Acceso ilícito a sistemas y equipos de informática” está titulado de manera incorrecta, porque su articulado no se refiere únicamente al acceso ilícito; el problema radica en que muchos ataques informáticos se perpetran sin necesidad de acceder directamente a un sistema informático, como sucedería en un ataque mediante virus, donde el diseñador no tiene acceso directo a ninguna computadora, ya que desencadena el daño enviando el virus por correo electrónico o de maneras similares.¹²⁶

Se puede apreciar una escala de penas en la que sus tipos básicos son de seis meses a dos años, cuestión con la cual no estoy de acuerdo, ya que esta escala no permite casi en ningún caso la extradición cuando los sujetos activos se

¹²⁶ <http://www.amdi.org.mx>

encuentren fuera de territorio, lo cual es una cuestión que favorece la impunidad de todas estas actividades.

En los tipos agravados este problema no se presentaría, pero ello implica que la pena atribuida a los reincidentes no sea, a mi criterio, demasiado baja, lo cual podría ser modificado, imponiendo un mínimo de prisión de al menos tres años para poder realizar así una protección extraterritorial de los bienes jurídicos, ya que pueden verse violentados desde espacios geográficos muy lejanos al territorio mexicano en concreto, lo cual acarrearía la necesidad de extradición que la misma norma impediría con una pena tan baja.

Además, por tal motivo, ninguna de las figuras aquí comentadas ha alcanzado la definición de delito grave, a excepción de la hipótesis del artículo 424 bis, que habla sobre la piratería informática de software que defiende los derechos de autor que establece una pena de tres a diez años de prisión; por lo que observamos una seria dificultad en el procesamiento de estos delincuentes, debido a que cuentan con el beneficio de la libertad bajo caución, y lo más probable es que estos sujetos puedan obtenerla y luego desaparecer.

Actualmente, México de acuerdo al informe sobre las amenazas a la seguridad en Internet realizada y publicada por Symantec en Septiembre de 2012, es de los principales países a nivel mundial que sufre de ataques cibernéticos.¹²⁷

Cabe aclarar que nuestro país ha avanzado en esta materia, pero no lo suficiente como para estar listos ante cualquier ataque cibernético en forma rápida y expedita, ¿la razón?, falta de acuerdo y entendimiento en cuanto a este concepto, y mientras no haya un claro panorama de ello, no podrá existir una ley específica sobre los delitos informáticos de acuerdo con los avances tecnológicos que hoy en día tenemos en el mundo y que involucran a la sociedad mexicana, a pesar de que ya existen algunos artículos al respecto en algunas leyes mexicanas anteriormente mencionadas. Todo ello es a consecuencia de un analfabetismo

¹²⁷ <http://www.symantec.com>

informático y para la posible solución a esta problemática, se hacen las siguientes propuestas:

Se deben corregir las fallas anteriores y además contemplar una posible reforma bajo los siguientes argumentos informáticos, jurídicos y sociales:

➤ Los delitos informáticos contenidos en el Código Penal Federal, se deben organizar en un solo capítulo especial que se titule “Delitos Informáticos”.

Con esta propuesta de reordenamiento para los delitos informáticos y creación de un título especial que lleve su nombre en el Código Penal Federal, se pretende que el Estado cumpla con su deber de protección y tutela de bienes jurídicos mediante la utilización del derecho punitivo, para que por medio de la pena que pueda aplicar, se lleve a cabo la retribución, consistente en hacerle un mal al delincuente, principalmente privarle del bien jurídico de la libertad, y a su vez se actualice la prevención especial para que el sujeto se intimide y no reincida; pero además de las anteriores, por medio del ius puniendi, se verifica lo que la doctrina conoce como prevención general, que es un medio de amenaza genérica dirigida hacia todo el grupo social a fin de que se abstenga de cometer el delito.

En este sentido, los delitos informáticos se pueden prevenir, por medio del temor ciudadano al ser encausado en un proceso penal en el que se imponga una sanción fuerte para el individuo transgresor, y éste sepa de antemano que tales acciones son investigadas y perseguidas eficazmente, que se puede llevar a cabo incluso la extradición a otro país y viceversa, para que así se llegue a introyectar en la mente de las personas de preferencia desde la infancia, la imagen de “computadora-cuidado-delitos-informáticos-sanción-cárcel”, para que se vaya moldeando la concepción que tenga la sociedad en su conjunto, siendo necesario que ésta sepa, identifique, censure y condene dichos actos fraudulentos, y por ninguna razón se considere a sus ejecutantes como celebridades de la informática.

➤ Es cierto, que un delito informático puede ser simplemente un delito clásico en un nuevo envoltorio, los legisladores deben saber que la tecnología no es una forma de nueva conducta, sino un medio para ejercitar las ya conocidas, pero este medio no es cualquier medio, sino uno disponible a millones de personas que pueden aprovechar las ventajas que proporciona éste para cometer estos delitos sin problemas como el tiempo o espacio, y gracias a los medios informáticos se puede destruir hasta la mismísima humanidad. No dudo que ante la falta de ley que los vaya restringiendo, surjan nuevos delitos hasta hoy inimaginados.

Los legisladores opinan que no hay que crear una norma separada, especial o autónoma para regular los mencionados delitos porque los instrumentos normativos vigentes pueden amparar por sí solos o con ciertas modificaciones, las conductas realizadas a través de las computadoras o por medios similares.

No compartimos esta visión del problema; frente al panorama de la revolución informática se considera que el legislador debe clasificar las conductas en nuevos tipos penales, y no manejar sólo hipótesis equiparables carentes de resonancia e impacto social. Si bien es cierto que algunos tipos penales descritos en el Código Penal son aplicables a las conductas descritas en la clasificación de los delitos informáticos, las mismas resultan insuficientes frente a las nuevas necesidades de la colectividad, y, además, dado que en Derecho Penal está expresamente prohibida la aplicación analógica de los tipos debido al reconocimiento del principio de legalidad, de no producirse la creación de nuevas figuras delictuosas, numerosas conductas criminales continuarán quedando sin la aplicación de sanciones penales.

Por lo anterior proponemos la creación de tres tipos básicos de delitos informáticos en los que se consideren:

- a) Acceso ilícito a sistemas informáticos.- Para empezar, el simple acceso a un archivo, sistema informático o redes de este tipo sin

autorización, que por lo regular se hace mediante softwares especiales diseñados por los llamados “hackers”.

Con este tipo se debe resguardar el derecho a la privacidad y a la intimidad, ya que el delito más cometido en el territorio mexicano ha sido el Hacking, así, la acción elemental para los hackers consiste en “cortar” (to hack) las barreras establecidas para evitar los ingresos no deseados, por ello se puede inducir que esa es la acción base de toda esta nueva gama de delitos.

b) Robo de información de sistemas informáticos.- En este delito se debe castigar al que conozca o copie información no autorizada de un archivo, sistema o red informática. Para que así se puedan cubrir los posibles ataques de “trashers” (pepenadores de información) y “bucaneros” que pueden vender o sacar algún provecho de tal información. Es de suma importancia tipificar este delito ya que por medio de los sistemas informáticos el robo de información se da sin el desapoderamiento físico del bien, ya que la información contenida en un archivo, sistema o red informática se puede llevar a cabo la copia en segundos y por lo tanto dicha información pasa a estar en poder de dos personas, el propietario legítimo y el ladrón que podría darle muchos usos a tales archivos como los chantajes o extorsión, pago de rescate, entre otros.

Aquí, hacemos énfasis al robo de información como ejemplo, ya que anteriormente nadie podía entrar a nuestra mente o nuestras vidas pero, a medida que la tecnología avanzó, personas de cualquier estrato social como ejecutivos de negocios, empleados, obreros, estudiantes de todos los niveles y un sinnúmero de individuos actualmente acostumbramos traer cargando nuestra computadora o en su defecto “memorias usb” donde quiera que vamos, también ponemos en peligro la seguridad de los datos almacenados en tales dispositivos.

Por lo tanto, al vulnerarse nuestros archivos contenedores de datos personales, formas de vida, preferencias sexuales, pasatiempos, horarios e incluso archivos valiosos de trabajo o escolares, hacen que se deba considerar a

la información personal y privada contenida en computadoras, dispositivos y sistemas informáticos como un bien jurídico de gran valor a efecto de ser considerado por los legisladores.

c) Sabotaje informático.- Se introduzcan o envíen programas o instrucciones informáticas para alterar el normal funcionamiento o estado de archivos, programas, sistemas o redes informáticos, ya que esto se hace principalmente por “crackers” utilizando diversos medios como son los virus, gusanos, caballos de Troya o bombas lógicas.

Cabe mencionar que estos tipos de delitos son los que comúnmente se realizan con un afán de molestia y en sentido de burla o protesta hacia las víctimas, por lo que deben de considerarse dentro de una buena ley que los recoja, organice y castigue.

➤ Siguiendo los lineamientos ya analizados de los elementos del tipo en los delitos informáticos creo pertinente que los tres tipos básicos deben ser agravados como actualmente se contempla en el referido Código, cuando se cometan en contra del Estado o las Instituciones del Sistema Financiero, pero también cuando se viole una relación de confianza, cuando se cometan por más de dos personas, aprovechando alguna invasión, confusión social o desastre, cuando sean cometidos por profesionales en la materia, así como el ya conocidísimo fin de lucro.

Además de las anteriores, podría pensarse, ahora sí, en una agravante genérica de los tipos penales anteriormente establecidos consistente en la elevación de la pena cuando el acceso se produzca en aquellos equipos que cuenten con medidas de seguridad, basados en el hecho de que se requiere del despliegue de una actividad mayor por parte del sujeto activo.

➤ Considero pertinente la creación de tipos especiales como lo pueden ser:

a) **“Fraude informático financiero”**, en el que se persiga la acción de llevar a cabo operaciones o transferencias de dinero o valores ilícitamente, ya sea que se engañe al sistema con claves personales mediante el denominado robo de identidad o bien se ingrese al sistema y se modifiquen los datos, activos o pasivos, aumentándolos o disminuyéndolos de alguna cuenta bancaria o financiera.

b) **“Fraude cibernético”**, que cometerá quien engañe o aproveche el error en que otro se encuentra por medio de anuncios en páginas web o mediante correos electrónicos con el fin de obtener algún beneficio o lucro indebido.

Por ejemplo, los artistas del fraude envían un correo electrónico pidiendo que se envíe dinero para ayudar a una pobre niña cuyos padres murieron en un accidente de automóvil, y que enviando ese mail a 10 personas más recibirá de vuelta la inversión, y un poco más por ayudar a tan noble causa.

Otros fraudes pueden ser, por ejemplo, la presentación de credenciales falsas para conseguir negocios sin proporcionar luego el servicio vendido, como en el caso de las ventas de artículos que no son lo que aparentan en la página web o en las subastas “on line”, ya que el Internet simplemente ha sido la herramienta que facilita y agiliza las operaciones de estos estafadores proporcionándoles un número mucho mayor de víctimas potenciales a las cuales atacar.

➤ Propongo que los delitos contenidos en el Título Vigésimo Sexto del Código Penal Federal, en materia de derechos de autor que tengan relación con la informática, programas y los software “piratas” en sus diferentes variantes, como lo pueden ser el fabricar dispositivos o programas para desactivar sistemas de protección de un programa de computación; o el producir, almacenar, transportar o vender obras protegidas por la Ley Federal de Derechos de Autor, en este caso el llamado “software pirata”, o realizar actos para descifrar señales satelitales portadoras de programas que se encuentran contenidos en los artículos 424bis, 424ter y 426 deben ser reubicados en el nuevo capítulo especial para delitos informáticos, con el fin de unificar estos delitos ya que como lo establecimos con

anterioridad, los delitos informáticos clasificados en cuanto a su fin, tienen también como objeto la información lógica de los equipos informáticos, más aún si estos programas pueden servir para llevar a cabo un gran número de otros delitos informáticos.

➤ Por su parte, otros delitos como la violación de correspondencia y la falsificación de documentos también deben contenerse en este nuevo Capítulo, añadiendo que el documento escrito, indispensable en estos tipos, deberá ser el contenido en sistemas informáticos o electrónicos.

CONCLUSIONES

PRIMERA. Desde la antigüedad hasta nuestros días, el hombre en su necesidad de comunicarse y a medida que se fue incrementando la complejidad de sus problemas, se vio en la necesidad de inventar mejores sistemas y medios de procesamiento que permitieran resolverlos, llegando a desarrollar desde las tablas de contar de piedra, ábacos, tablillas, telares, hasta máquinas más sofisticadas como máquinas registradoras, calculadoras, y alrededor de cinco generaciones de computadoras, entre otras.

A raíz del desarrollo de las computadoras, específicamente después de la cuarta generación surge un nuevo concepto, la “informática”, disciplina llamada a cumplir un papel relevante en la sociedad mundial y su desarrollo, definida como “el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores”. La informática combina los aspectos teóricos y prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano. Los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica.

SEGUNDA. Los avances en la tecnología y la ciencia han favorecido en gran parte el desarrollo de la sociedad, la informática es un instrumento de vital importancia en la vida cotidiana de los seres humanos ya que se utiliza en todos los aspectos de esta. Como ejemplos claros, podemos citar desde una calculadora, teléfonos celulares, tabletas electrónicas, memorias flash, hasta las computadoras de escritorio y personales, que son instrumentos indispensables tanto en el ámbito social, educativo o laboral.

El mundo moderno de la alta tecnología nunca hubiese existido de no ser por el desarrollo de la computadora. Toda la sociedad utiliza estas máquinas, en distintos tipos y tamaños, para el almacenamiento y manipulación de datos. Los equipos informáticos han abierto una nueva era en la industria de fabricación,

gracias a las técnicas de automatización y han permitido mejorar los sistemas modernos de comunicación, son herramientas esenciales prácticamente en todos los campos de investigación y tecnología aplicada, como los diagnósticos médicos, las condiciones meteorológicas, el control de movimientos bancarios del sistema financiero mundial, la automatización de plantas industriales o fábricas, por mencionar algunos.

De acuerdo a la investigación realizada por los diversos medios de consulta, constaté que los elementos informáticos que ahora nos rodean serán esenciales para aspirar a nuevos horizontes. Si bien es cierto los conocimientos básicos que un usuario debe contemplar son sin duda los más requeridos por la misma tecnología, pues en un futuro no muy lejano, se podría considerar como analfabeta a aquella persona que no tiene las bases de la computación, ya que esta es una herramienta más de uso indispensable en todas las áreas, como la escuela, el trabajo o la oficina, entre otras.

Estamos en una sociedad donde las tecnologías informáticas han llegado a ser la figura representativa de nuestra cultura y los servicios de bases de datos y redes mundiales permiten acceder a una gran variedad de fuentes de información, pero esas mismas técnicas avanzadas también posibilitan la invasión sobre lo privado y las fuentes de información restringida, riesgos que la sociedad deberá enfrentar si desea gozar de las ventajas de la tecnología moderna.

El uso de la informática en manos del Estado como de los particulares crea diversos riesgos que pueden sugerir una amenaza de agresión a la intimidad de los gobernados o de los usuarios del servicio. El reto de todo avance tecnológico siempre ha sido que el hombre domine a la tecnología y no ella a él.

TERCERA. La Informática Jurídica estudia el tratamiento automatizado de las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (Informática Jurídica Documental); las fuentes de producción jurídica, a través de la elaboración informática de los factores lógico-formales que concurren en el proceso legislativo y en la decisión

judicial (Informática Jurídica Decisional); y en los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho (Informática Jurídica de Gestión).

La Informática Jurídica, es la ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el derecho, es decir, la ayuda que éste uso presta al desarrollo y aplicación del derecho.

Ahora bien, el llamado “derecho informático” nace de la necesidad de regular las relaciones sociales y jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática, por ejemplo, las normas regulatorias de la protección de datos personales, normas relativas al régimen jurídico del software y particularmente a la problemática de su protección jurídica, sancionadas ya en un conjunto de países, y con proyectos normativos elaborados y normas relativas a la regulación jurídica de los flujos de datos transfronterizos o de los contratos informáticos.

CUARTA. El gran desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia, ya que la manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Los delitos informáticos son aquellas actividades ilícitas que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación, que tiene por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos. También se puede definir al delito informático como la conducta típica, antijurídica, culpable y punible, en que se tiene a las computadoras como instrumento o fin.

Como vemos, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial como las estafas o las apropiaciones indebidas.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, provisionales y de identificación de las personas, y, si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares, se comprenderá que están en juego o podrían llegar a estarlo algunos valores colectivos y los consiguientes bienes jurídicos que se deben proteger.

QUINTA. Al sujeto que realiza las conductas señaladas anteriormente se le conoce como hacker, el cual es una persona muy interesada en el funcionamiento de sistemas operativos, es aquel curioso que simplemente le gusta husmear por todas partes, llegar a conocer el funcionamiento de cualquier sistema informático mejor que quienes lo inventaron. La palabra hacker es un término inglés que caracteriza al delincuente silencioso o tecnológico, con capacidad de crear sus propios softwares para entrar a los sistemas.

Los hackers suelen ser verdaderos expertos en el uso de las computadoras y por lo general rechazan hacer un uso delictivo de sus conocimientos, aunque no tienen reparo en intentar acceder a cualquier máquina conectada a la red, o incluso penetrar a una Intranet privada, siempre con el declarado fin de investigar las defensas de estos sistemas, sus lados débiles y obtener el mérito de haber logrado burlar a sus administradores. Muchos de ellos dan a conocer a sus víctimas los errores encontrados en la seguridad e incluso sugieren cómo

corregirlos, otros llegan a publicar sus hallazgos en revistas o páginas Web de poder hacerlo.

A su vez los llamados Crackers son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general, a causar problemas. Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware, así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

Como su nombre indica se dedican a romper, por supuesto las protecciones y otros elementos de seguridad de los programas comerciales, en su mayoría con el fin confeso de sacar provecho de los mismos del mercado negro. Estos crean códigos para utilizarlos en la copia de archivos. Sus acciones pueden ir desde la destrucción de información ya sea a través de virus u otros medios, hasta el robo de datos y venta de ellos. Ejemplo de su actuar ilegal son los millones de CD's con software pirata que circulan por el mundo entero y de hecho, muchas personas no llegan a sospechar que parte del software que tienen en sus máquinas, incluso con certificados de garantía de procedencia, es craqueado.

Por último se debe mencionar a los phreakers que son especialistas en telefonía, poseen profundos conocimientos de los sistemas de telefonía y amplios conocimientos sobre informática ya que la telefonía celular o fija es la parte primordial de su actividad pero emplean la informática para el procesamiento de datos.

SEXTA. Las conductas perseguibles en la esfera de la computación, varían, ya que se puede tratar de obtención ilícita de información, sabotajes a los sistemas informáticos y páginas web, espionaje, accesos no autorizados a servicios informáticos, robo de servicios, fraudes, manipulación en los datos e informaciones contenidas en los archivos o soportes físicos, destrucción total o parcial de información, copiado y craqueado de programas de cómputo, defraudaciones a la propiedad intelectual, y en general diversas agresiones a los

sistemas o elementos informáticos que ocasionan daños económicos y patrimoniales muy severos en los sistemas de cómputo.

El resultado al cometerse algún delito informático tiende a lesionar diversos bienes jurídicos tutelados como la propiedad, la privacidad, intimidad, el honor, la fe pública e incluso en ocasiones la vida de las personas, como en el caso de secuestro y terrorismo.

Las características más importantes de los ciberdelitos son:

Son conductas criminógenas de cuello blanco, en tanto que sólo determinado número de personas con ciertos conocimientos técnicos pueden llegar a cometerlas. Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.

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. Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.

Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse; presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico, además, en su mayoría son imprudenciales y no necesariamente se cometen con intención y ofrecen facilidades para su comisión a los menores de edad.

SÉPTIMA. Analizando un poco la situación internacional, se aprecia que algunos países contemplan los delitos informáticos dentro de sus códigos penales y algunos otros han creado leyes especiales, ya que cada país contempló dichas normas de acuerdo a sus necesidades propias; podemos observar que algunos países se enfocaron propiamente a proteger el derecho a la privacidad, y a la propiedad intelectual, o como el que disponga de informaciones nominativas y

haga un mal uso de ello; otros tantos a proteger al patrimonio de las personas afectadas como en los fraudes informáticos. Las legislaciones de otros países nos ayudan y nos dan la pauta para que nuestros legisladores contemplen las figuras delictivas de "delitos informáticos" de acuerdo a nuestra propia realidad.

También se puede ver que los delitos informáticos tienden a quedar impunes debido a las diferencias en las legislaciones en el mundo, y como ya lo hemos visto, se vuelve un problema casi imposible de resolver debido al fácil traspaso de fronteras, por lo que se deben crear los tratados y convenciones internacionales pertinentes, y a su vez es imperiosa la necesidad de estandarizar los tipos penales, para que se puedan investigar eficazmente a nivel internacional, y para que además, no se haga ilusoria la potestad de castigar tales actos; ya que, cuando están involucrados distintos países existen trabas de todo tipo, y por lo regular sólo los delitos de mayor relevancia terminarán en sentencia y ejecución.

Para enfrentarse a los problemas causados por todos estos delitos relacionados con la informática e Internet, numerosos países se han unido y firmado la Convención del Consejo Europeo contra el Cibercrimen, que requiere que los miembros consideren delictivas todas las actividades relacionadas con el Ciberterrorismo y otras formas de delitos informáticos, como Estados Unidos, Canadá, Japón y Sudáfrica, México aún no se ha adherido a dicha Convención lo cual es un error que se podría componer. Gracias a esta cooperación, las actividades como la piratería, la intervención en sistemas informáticos, el fraude, la falsificación y otros delitos relacionados se consideran ahora ilegales en todos los países firmantes del acuerdo. Este acuerdo también facilita la cooperación internacional para detectar, investigar y perseguir tales delitos, así como para usar medios electrónicos para reunir pruebas para delitos relacionados con el terrorismo, el crimen organizado y otros delitos que se llevan a cabo a escala global mediante la organización de ordenadores y de redes.

OCTAVA. Los diversos tipos de delitos informáticos que se realizan en la actualidad, dan lugar a una interpretación fuera de los límites de la legalidad, por

lo que muchas veces quedan impunes ante la mirada atónita de las víctimas, y en el caso específico de nuestro Código Penal Federal, no se ha tipificado completamente sobre los delitos informáticos, además de que este ordenamiento adolece de varios defectos, porque se ha ido adicionando, o más bien, se ha ido “parchando”, por lo que actualmente los nuevos métodos y conductas de este tipo han rebasado la naturaleza de los actuales delitos.

La cuestión se centra en la creación de nuevos tipos o bien, la modificación de los mismos, debemos atender a la naturaleza del acto, pues como lo señala el maestro Cárpoli, no se deberían tener problemas al aplicar los tipos básicos a estas conductas informáticas. Por lo anteriormente dicho, es necesario una rápida acción del legislador con el propósito de definir los nuevos tipos penales y agregarlos a los vigentes, sin perjuicio de que al hacer las respectivas modificaciones, puedan agravarse algunos tipos existentes en función del uso de nuevas tecnologías informáticas.

NOVENA. El sujeto activo del delito es aquella persona que lleva a cabo la realización de la conducta calificada como delictiva, es decir, el delincuente. Mientras que el sujeto pasivo es aquella persona en la que recae el daño.

En el tema que nos ocupa, 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 ilícitos, hoy en día cualquier persona con medianos conocimientos de informática puede llegar a ser un delincuente informático ya que la posibilidad de acceder a algún sistema informático se puede realizar desde algún lugar remoto.

En nuestro Código Penal Federal sólo en los artículos 211 bis 3 y 211 bis 5 existen agravantes atendiendo a la calidad del sujeto activo, en el primero de ellos cuando el acto lo cometan servidores públicos o servidores en alguna institución

de seguridad pública; en el segundo artículo señala que aumentará la penalidad cuando sea realizado por funcionarios o empleados del sistema financiero.

DÉCIMA. En la doctrina penal mexicana se diferencia entre el objeto material y el objeto jurídico, siendo el primero la cosa, o bien la persona sobre la que recae el daño de un delito, mientras que el objeto jurídico es considerado el bien tutelado por la norma penal.

En este orden de ideas y de conformidad a lo establecido por los artículos 211 bis 1 a 211 bis 7 del CPF, podemos establecer que el objeto material en tales tipos penales estaría integrado por los datos portadores de información contenida en un sistema informático e inclusive el propio equipo computacional, ya que cabe recordar que se puede incurrir en este delito cuando se use, altere o se destruyan tales objetos.

En el caso de los delitos que utilizan como medio para su realización los elementos informáticos el objeto material será el objeto externo donde recaiga la acción, así, en el caso de fraude a alguna Institución del sistema financiero por medio de una intrusión a su sistema a través de una computadora, los datos alterados o modificados son el objeto material de la acción, ya que representan un objeto corporal como lo es el dinero en efectivo independientemente del método con que el autor manipuló o engañó el sistema.

Por lo que respecta al bien jurídico tutelado por los artículos antes citados podemos señalar que es la confidencialidad y protección de la información que se almacena en los sistemas informáticos, perteneciendo al género de los delitos patrimoniales, debido a que en todos y cada uno de los tipos en comento se aprecia que el legislador hace referencia como elemento esencial de estos tipos penales, que exista “información” contenida en sistemas o equipos de informática, sin embargo, el legislador colocó a los delitos informáticos en el título noveno al saber que estas intrusiones y modificaciones de información en la realidad violentan varios bienes jurídicos y para ya no batallar a la hora de su legislación

les colocó un título que sólo demuestra su falta de conocimiento en esta materia que demerita mucho su función legislativa.

DÉCIMO PRIMERA. La conducta también llamada acto o acción, lato sensu, es la manifestación externa de la voluntad por parte del sujeto activo; en el delito y su tipificación puede manifestarse mediante haceres positivos (acciones) o negativos, es decir, por abstenciones como en el caso de la omisión o la comisión por omisión.

En estricto sensu, la acción es todo hecho humano voluntario, todo movimiento voluntario del organismo humano capaz de modificar el mundo exterior o de poner en peligro dicha modificación.

La conducta punible se encuentra descrita por el tipo penal y puede ser de acción u omisión, en los tipos penales en análisis del 211bis 1 al 211 bis 5 del Código Penal Federral, observamos que todos son de los llamados de acción, lo anterior se desprende de que tipifican conductas como “conocer, modificar, destruir o provocar pérdida” de información de un sistema o equipo informático, siendo todas estas actividades que requieren un accionar físico exterior del cuerpo humano.

DÉCIMO SEGUNDA. El resultado material se puede definir como la consecuencia de la acción, que la ley considera decisiva para la realización del tipo del delito, o lo que es lo mismo, la realización del tipo del delito fijado por la ley, es el efecto voluntario en el mundo exterior, o más precisamente, la modificación del mundo exterior como efecto de la actividad delictuosa

Ahora bien, el resultado material en estos tipos penales en estudio se encuentra presente cuando se produce el daño, destrucción, pérdida, modificación o conocimiento sin autorización de la información contenida en sistemas o equipos de informática especificados en cada artículo.

En otros casos, cuando se utilicen los equipos informáticos como medio para cometer otros delitos, el resultado material dependerá del tipo de delito, por decir cuando se modifique una página web ilícitamente, el resultado material será la página modificada siempre y cuando se tipifique la acción de modificar dichas páginas sin autorización o se encuentre contenida subjetivamente dentro de otro tipo penal.

DÉCIMO TERCERA. Los elementos normativos son presupuestos del injusto típico, forman parte de la descripción contenida en los tipos penales y hacen referencia a la antijuridicidad, se expresan mediante fórmulas tales como “sin derecho”, “sin causa justificada”, “injustificadamente” o “al que indebidamente”. Estos elementos indican que el comportamiento realizado por el delincuente contraviene la norma jurídica. La propia norma lo resalta con expresiones como las indicadas, lo que interpretado a contrario sensu significa que el comportamiento no sería antijurídico. Por ejemplo si alguien toma una cosa mueble ajena “con derecho” “o bien “con consentimiento”, la conducta no es ilícita.

En los delitos informáticos el elemento normativo es importante ya que al igual que los elementos subjetivos pueden provocar atipicidad de la conducta, como lo pudiera ser la hipótesis en que se sustraiga información de un ordenador informático pero se justifique porque se cuente con el derecho para hacerlo.

Así, de los artículos 211 bis 1, 211 bis 2 y 211 bis 4 de nuestro Código Penal Federal, se puede apreciar que se exige como elemento normativo para establecer tipicidad el que el acto se realice por algún sujeto “sin autorización”.

En los artículos 211 bis 3 y 211 bis 5 de la Ley Penal Federal se precisa la necesidad de que la acción sea desplegada por alguien que “estando autorizado” para acceder al sistema informático, pero “indebidamente” modifique, destruya, provoque pérdida o copie información de las Instituciones del Estado o del Sistema Financiero.

DÉCIMO CUARTA. Los elementos subjetivos dentro de un tipo penal son los que reflejan una especial culpabilidad del sujeto activo para la comisión de un delito, es decir, se refieren al ánimo de una persona demostrando su situación interna.

En tales casos el legislador ha colocado esos elementos subjetivos cuando hace mención a términos tales como: maliciosamente, dolosamente, a sabiendas, el que con conocimiento, el que intencionalmente, entre otras.

Tomando en cuenta el análisis de los artículos de la ley sustantiva en comento, no encontramos ningún elemento subjetivo, ni aun cuando el artículo 211 bis 7 prescribe que se aumentarán en una mitad las penas establecidas en todo el capítulo en análisis, cuando la información obtenida se utilice en provecho propio o ajeno, ya que no se hace referencia al ánimo de provecho para que existan tales figuras delictivas, sino que es una circunstancia agravante posterior e independiente el que la información no autorizada, su destrucción o modificación sea para la obtención de un provecho.

DÉCIMO QUINTA. En el Código Penal Federal se establecen condiciones especiales del tipo, y sólo se hace referencia a los sistemas y a los equipos ya protegidos por algún mecanismo de seguridad, cuestión que parece ser infundada ya que la violación de la propiedad o de la privacidad es la misma, ya se trate de un sistema protegido ó de uno sin clave alguna; sin embargo, en definitiva lo que se quiere proteger es el bien jurídico, pero tal calidad especial en el objeto material no debiera contemplarse, ya que en la mayoría de los casos los sistemas y equipos que se consideran caseros, no poseen mecanismo de seguridad alguno que los pueda considerar como incluidos dentro del tipo penal.

No se contemplan todos los tipos comunes de ataques informáticos, sólo se castiga el acceso ilícito a sistemas informáticos, pero qué pasa con los actos ya mencionados en otros capítulos como la modificación de una página web, cuyo titular sea cualquier simple mortal, o se introduzca un virus que ocasione una denegación de servicios o inhabilitación parcial del ordenador, no podría

actualizarse el delito de daño en propiedad ajena ya que el concepto de cosa es aplicable al soporte y no a su contenido, es decir, una página web no puede asimilarse a lo que significa cosa, ya que no se trata de un material corpóreo ni se puede mostrar materialmente.

El simple descuido del legislador ha generado la exclusión del tipo cuando alguien autorizado copia información privada, y esto, en virtud de la importancia de los bienes a proteger, lo cual me parece inaceptable en términos jurídicos. Si en los casos en que el sujeto activo pertenece a las Instituciones Financieras, se debe agravar la pena, ya que la relación laboral y de confianza es la misma, y la no inclusión de este agravante no tiene fundamento jurídico o lógico alguno. Me parece más aceptada la redacción que imponga al fin de lucro como agravante genérica sin incriminar o desincriminar a las conductas que no tengan este objetivo.

Otra cuestión de análisis es que en dicho Código Penal se protege a las instituciones Financieras y al Estado, dejando excluidos a los particulares, sólo trata fugazmente de proteger estos últimos en el artículo 211 bis 1 del Código Penal; sin embargo, en la vida diaria los delitos informáticos son cometidos a personas y empresas particulares.

Se puede apreciar una escala de penas en la que sus tipos básicos son de seis meses a dos años, cuestión con la cual no estoy de acuerdo, ya que esta escala no permite casi en ningún caso la extradición cuando los sujetos activos se encuentren fuera de territorio, lo cual es una cuestión que favorece la impunidad de todas estas actividades.

DÉCIMO SEXTA. Es cierto, que un delito informático puede ser simplemente un delito clásico en un nuevo envoltorio, los legisladores deben saber que la tecnología no es una forma de nueva conducta, sino un medio para ejercitar las ya conocidas, pero este medio no es cualquier medio, sino uno disponible a millones de personas que pueden aprovechar las ventajas que proporciona éste para cometer estos delitos sin problemas como el tiempo o

espacio, y gracias a los medios informáticos se puede destruir hasta la mismísima humanidad. No dudo que ante la falta de ley que los vaya restringiendo, surjan nuevos delitos hasta hoy no imaginados.

Los legisladores opinan que no hay que crear una norma separada, especial o autónoma para regular los mencionados delitos porque los instrumentos normativos vigentes pueden amparar por sí solos o con ciertas modificaciones, las conductas realizadas a través de las computadoras o por medios similares.

No compartimos esta visión del problema; frente al panorama de la revolución informática se considera que el legislador debe clasificar las conductas en nuevos tipos penales, y no manejar sólo hipótesis equiparables carentes de resonancia e impacto social. Si bien es cierto que algunos tipos penales descritos en el Código Penal son aplicables a las conductas descritas en la clasificación de los delitos informáticos, las mismas resultan insuficientes frente a las nuevas necesidades de la colectividad, y, además, dado que en Derecho Penal está expresamente prohibida la aplicación analógica de los tipos debido al reconocimiento del principio de legalidad, de no producirse la creación de nuevas figuras delictuosas, numerosas conductas criminales continuarán quedando sin la aplicación de sanciones penales.

DÉCIMO SÉPTIMA. Propongo como la solución más viable a este vacío en la legislación Federal, la creación de un nuevo capítulo denominado “Delitos Informáticos”, para que ahí se reordenen estos delitos y se establezcan nuevos tipos penales, para que por lo menos, la mayoría de las conductas criminales posibles en el ambiente informático y la red de redes (Internet), puedan ser detectadas, investigadas, perseguidas y castigadas eficazmente.

También propongo que las penas se adecúen a la realidad y sean un poco más severas, con el fin de que se logre la intimación de tales sujetos a sabiendas de que no se gozaría del derecho de libertad bajo caución y también existiera la posibilidad de su extradición.

Pienso que con la creación de este nuevo capítulo, se lograría la difusión necesaria de que las autoridades han tomado cartas en el asunto, y se castigará a quienes cometan tales delitos; además, la sociedad en su conjunto, deberá estar informada sobre las consecuencias de realizar algún acto de esta naturaleza. Ya no se debe tener la errónea concepción de la computadora como un simple juego o como un aparato electrónico más en la casa; al contrario, se debe empezar a considerar tal vez como un arma “electrónica”, por lo que se debe utilizar solo para fines honestos, y de esta forma, se cumpla con la principal finalidad del Derecho Penal que es el “prevenir” los actos delictivos.

DÉCIMO OCTAVA. También se debe impulsar la creación de normas procesales enfocadas a la acreditación de los delitos informáticos, y así lograr fundamentar y motivar la labor del Ministerio Público Federal y los cuerpos especializados, como el que existe actualmente en México denominado Unidad de Policía Cibernética, la cual depende de la Policía Federal Preventiva (PFP), ya que si no existe un delito que perseguir, las averiguaciones que realicen no pasarán de ahí, de simples averiguaciones, porque no se podrá ejercitar la acción penal debido a la falta de tipos penales en los cuales encuadren estas conductas criminales.

Así mismo, propongo como método para reducir la incidencia de los delitos informáticos, fomentar la presión social hacia estos “hackers”; ya que si en la sociedad los cibercriminales son rechazados en lugar de ser admirados, será probable que muchos de ellos dejen de repetir las mismas conductas, sobre todo creo que funcionaría en los jóvenes, ya que la mayoría de estos delincuentes, son adolescentes que muchas veces llevan a cabo tales actos con el objeto de impresionar a sus amigos.

En este sentido, los delitos informáticos se pueden prevenir, por medio del temor ciudadano al ser encausado en un proceso penal en el que se imponga una sanción fuerte para el individuo transgresor, y éste sepa de antemano que tales acciones son investigadas y perseguidas eficazmente, que se puede llevar a cabo

incluso la extradición a otro país y viceversa, para que así se llegue a introyectar en la mente de las personas de preferencia desde la infancia, la imagen de “computadora-cuidado-delitos-informáticos-sanción-cárcel”, para que se vaya moldeando la concepción que tenga la sociedad en su conjunto, siendo necesario que ésta sepa, identifique, censure y condene dichos actos fraudulentos, y por ninguna razón se considere a sus ejecutantes como celebridades de la informática.

FUENTES DE CONSULTA

BIBLIOGRAFÍA

- Altmark, Daniel Ricardo *"Informática y Derecho, Aportes de Doctrina Internacional"*, Vol. I, s/e, Depalma, Buenos Aires, Argentina, 1987.
- Amuchategui, Irma y Villasana Ignacio. *"Diccionario Jurídico, Derecho Penal"*, Vol. I, Oxford., México, 2002.
- Baón Ramírez, Rogelio. *"Visión General de la Informática en el Nuevo Código Penal"*, Cuadernos de Derecho Judicial. Madrid.1996.
- Bejarano Sánchez, Manuel. *"Obligaciones Civiles"* 5ª ed., Edit. Oxford, México, 2002.
- Cámpoli, Gabriel A. *"Delitos Informáticos en la Legislación Mexicana"*. INACIPE, México, 2005.
- Castellanos Tena, Fernando *"Lineamientos elementales de Derecho Penal"*. edit. Porrúa, México, 1989
- Corominas, Joan, *"Breve Diccionario etimológico de la lengua castellana"*, Madrid, 1983.
- Davara Rodríguez Miguel Ángel. *"Manual de Derecho Informático"*, Edit. Aranzadi, 1999.
- Delpiazzo, Carlos, Eirin, Álvaro, Montano, Pero. *"Introducción a la Informática Jurídica y al Derecho Informático"*, Edit. Amalio Fernández, 1984,4º, Montevideo.
- Fernández Calvo, Rafael. *"El Tratamiento del llamado "Delito Informático"*, Edit. Mérida, Extremadura, 1996.
- Fernández Carrasquilla, Juan *"Derecho Penal Fundamental- Teoría General Del Delito y Punibilidad"*, Vol. II. 2ª. ed., Temis, Bogotá-Colombia, 1989.
- Ferreira D., Francisco José *"Teoría General Del Delito"*, s/e, TEMIS, Bogotá-Colombia, 1988.

- Fontain Palestra, Carlos. Traducción de Ledesma A. C. Guillermo. "*Derecho Penal-Introducción y Parte General*", 13ª ed., Abeledo-Perrot, Argentina, 1991.
- Frosini, Vittorio "*Cibernética, Derecho Y Sociedad*", s/e, Tecnos Editores, España, 1982.
- González, Raúl- Salas Campos "*La Teoría Del Bien Jurídico en el Derecho Penal*". Pereznieto Editores, México, 1995.
- Gómez Perals, Miguel. "Delitos Informáticos en el Derecho Español" Edit. Aranzadi, Barcelona, 1994.
- Haliday, Caroline M. "*Secretos de los Sistemas de PC*". Edit. Limusa, México, 1994.
- Hernández Jiménez, Ricardo y Luz María del Pozo "*Informática en Derecho*". Trillas, México, 1992.
- Huerta Miranda, Marcelo y Libano Manssur, Claudio. "*Delitos Informáticos*". Edit. Jurídica Cono Sur. Santiago de Chile, 1998.
- Jijena Leiva, Renato Javier, Chile. "*La protección penal de la intimidad y el delito informático*". Santiago, Ed. Jurídica de Chile, 1992.
- Jiménez de Asúa, Luis "*Lecciones de Derecho Penal*", Pedagógica Iberoamericana, México, 1995.
- Jiménez de Asúa, Luis "*Teoría del delito*" Cursos jurídicos temáticos hispanoamericanos, Iure Editores, México, 2003.
- Jiménez Huerta, Mariano. "*Derecho Penal Mexicano: Introducción al estudio de las figuras típicas*", Porrúa, México, 1977.
- Jiménez Huerta, Mariano "*Derecho Penal Mexicano*", 4ª ed., Porrúa S.A., México, 1983.
- Lima de la Luz, María. "*Delitos electrónicos.*" México, D.F., Edit. Porrúa. 1984.
- Long, Larry y Nancy Long, "*Introducción a las computadoras y el procesamiento de Información*". Cuarta edición, Editorial Prentice may, España, 1995
- M. Correa, Carlos "*Derecho Informático*", s/e, Depalma, Argentina, 1987.

- Malo Camacho, Gustavo. "*Derecho Penal Mexicano*", Porrúa, S.A., México, 1997.
- Meján, Luis Manuel. "*El Derecho a la Intimidad y la Informática*", 2ª ed., Porrúa S.A., México, 1996.
- Mezger, Edmundo "*Tratado de Derecho Penal*" Tomo I. Revista de Derecho Privado, Madrid España, 1955.
- Mora, José Luis y Enzo Molino. "*Introducción A La Informática*", 2ª impresión, Porrúa S.A., México, 1987
- Orellana Wiarco, Octavio A. "*Curso de Derecho Penal*" Parte General. Porrúa S.A., México, 1999,
- Pavón Vasconcelos, Francisco. "*Manual de Derecho Penal Mexicano*" Parte General, 10ª ed., Porrúa, S.A., México, 1991
- Pérez Nuñó, Antonio Enrique. "*Manual de Informática y Derecho*". Barcelona, Edit. Ariel. 1996.
- Reyes Echandi, Alfonso, "*Tipicidad*", 6º Ed, Temis, Bogotá, 1989.
- Riestra Gaytán Emma. Apuntes "*Los delitos Informáticos en el Derecho Positivo Mexicano*" Curso Introducción a los Delitos Informáticos. Instituto Nacional de Ciencias Penales, julio del 2000.
- Ruiz Vadillo, Enrique. "*Falsedad y defraudaciones por abuso informático*". Colección: Cuadernos de Derecho Judicial. Madrid. 1995.
- Romeo Casabona, Carlos María. "*Los llamados delitos informáticos*". Edit. Impactos, Madrid, 1987.
- S. Tanenbaum, Andrew, "*Organización de computadoras. Un enfoque estructurado*". Tercera edición. Editorial Prentice Hall, 1993.
- Tiedemann, Klaus. "*Poder económico y delito*", Barcelona, 1985.
- Téllez, Julio. "*Derecho Informático*", UNAM, México, 1994.
- Barriuso Ruiz, Carlos, "*Interacción del Derecho y la Informática*", Dykinson, Madrid, 1996.

LEGISLACIÓN

“Constitución Política De Los Estados Unidos Mexicanos”, Edit. Porrúa S.A., México, 2013.

“Código Penal Federal”, Edit. Porrúa S.A., México, 2013.

“Ley Federal del Derecho de Autor”, Edit. Porrúa S.A., México, 2013.

“Ley de la Propiedad Industrial”, Edit. Porrúa S.A., México, 2013.

SITIOS WEB

<http://www.amdi.org.mx> 30-ago-2011 21:45

<http://www.conventios.coe.int> 7-sep-2011 18:15

<http://www.delitosinformaticos.com> 25-sep-2011 20:36

<http://es.wikipedia.org> 25-sep-2011 22:00

<http://www.forodelderecho.blogcindario.com> 27-nov-2011 1:15

<http://www.germanwings.com/es> 17-dic-2011 2:25

<http://www.informaticajuridica.com> 8-feb-2012 19:13

<http://www.iurilex.org> 17-oct-2011 12:47

<http://www.julionunezderechoinformatico.blogspot.com> 13-mar-2012 11:35

http://www.jus.unitn.it/cardoza/law_web/home_it.html 15-nov-2011 2:35

<http://www.law.unican.es/incade/lex/cpint.htm> 25-sep-2011 9:47

<http://legal.web.aol.com/resources/legislation/ecpa.html> 29-oct-2011 11:39

[http://www.legifrance.gouv.fr/citoyen/code00.ow?heure2=032030494971&code=cp
enall.rcv&no=66](http://www.legifrance.gouv.fr/citoyen/code00.ow?heure2=032030494971&code=cp
enall.rcv&no=66) 17-abr-2012 22:15

<http://www.legislacionmundial.com> 17-dic-2011 2:45

<http://www.loc.gov/law/help/guide/nations/austria.php#legislative> 22-dic-2011
10:58

<http://www.loc.gov/law/help/guide/nations/england.php> 29-oct-2011 12:00

<http://www.loc.gov/law/help/guide/nations/netherlands.php> 31-ene-2012 22:45

<http://www.oas.org> 27-sep-2011 18:50

<http://www.rae.es> 27-sep-2011 19:36

<http://www.redi.org> 31-sep-2011 22:50

[http://www.todoelderecho.com/SeccionInternacional/Codigos/Chile/codigo%20pen
al-chile.htm](http://www.todoelderecho.com/SeccionInternacional/Codigos/Chile/codigo%20pen
al-chile.htm) 26-ene-2012 19:50

<http://www.uncjin.org> 5-abr-2012 22:15

<http://www.unesco.org> 15-mar-2012 2:00

<http://wings.buffalo.edu/law/bclcl/germind.htm> 28-feb-2012 17:20