UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGÓN

"EL DERECHO PENAL Y LOS DELITOS INFORMÁTICOS"

T E S I S

QUE PARA OBTENER EL TÍTULO DE

MAESTRO EN DERECHO
(CIENCIAS PENALES)

P R E S E N T A :

LIC. ALBERTO RAFAEL HORACIO
BUENDIA MADRIGAL

ASESOR:
MAESTRO: FRANCISCO JESÚS FERRER VEGA

SAN JUAN DE ARAGÓN 2001

EL DERECHO PENAL Y LOS DELITOS INFORMÁTICOS.

INDICE GENERAL.

INTRODUCCION.

El crecimiento de las tecnologías ha venido a revolucionar la Información. Sin embargo, Hoy en día, la tecnología toca cada vez mas aspecto de nuestra vida, importando poco la ubicación en el mundo. Sin perder de vista que las actividades diarias de todos se ven afectadas en su forma, contenido y tiempo por una computadora, siendo evidente que recibimos a todas horas los beneficios de estos avances tecnológicos. Ya que cada vez más personas, empresas, industrias, negocios, hospitales y gobiernos se vuelven dependientes de esta. No sólo son usadas intensamente para desempeñar las funciones industriales y económicas de la sociedad, sino también para realizar muchas funciones cotidianas. Las computadoras son utilizadas para guardar datos confidenciales de naturaleza política, social, económica o personal, ayudando con esto al mejoramiento de los países. Y con esto al progreso de las comunicaciones, las áreas científicas y la industria que han logrado rápidamente sus avances, ayudados tecnológicamente por una computadora, que día a día a hecho que nuestra forma de vivir haya cambiado vertiginosamente.

Pero también las tecnologías traen aparejado un lado negativo, que ha abierto la puerta al comportamiento antisocial y criminal. Ya que los sistemas de computación ofrecen nuevas y sofisticadas oportunidades para quebrantar la ley y crear la posibilidad de cometer delitos por vías poco comunes. Trayendo consecuencias económicas por este tipo de delitos, la sociedad depende de los sistemas computarizados para la mayoría de sus actividades. La rápida extensión transnacional de redes computacionales a gran escala y la disponibilidad de acceder a muchos sistemas a través de líneas telefónicas incrementa la vulnerabilidad de estos sistemas y la oportunidad del mal uso o de la actividad criminal.

Desafortunadamente en nuestro país, aún no se ha podido lograr una cultura informática, que ayude a la prevención de dichos delitos, por lo que se requiere plantar nuevas políticas, procedimientos y medidas de seguridad que ayuden a resolver este tipo de problemas adecuando este tipo de conductas a nuestros ordenamientos penales.

Por lo tanto la presente investigación pretende aportar algunos de los muchos elementos que se pueden obtener de la interrelación que se tiene entre la Informática, las Comunicaciones y el Derecho. Que servirán para formarnos un criterio de los retos que debemos enfrentar y la consciencia a la que debemos llegar, al aportar nuevas ideas que ayuden a nuestra sociedad, siempre con la firme convicción de que nuestros representantes y autoridades, estarán obligados a proporcionar los medios jurídicos para enfrentar los cambios de una era moderna, que requiriere una revaloración de sus leyes, con la finalidad de cumplir todas las necesidades de una realidad social, sin dejar a un lado la imperiosa necesidad de regular todas aquellas conductas, que son conocidas, hoy como Delitos Informáticos. Por lo que no podemos perder la lucha contra la impunidad, tomando las medidas necesarias que darán solución a los problemas de una sociedad, dando con esto las bases a un sistema jurídico seguro.

Cabe mencionar que para dar una visión más amplia de esta investigación, la misma la dividimos en tres partes fundamentales: La Informática y las Telecomunicaciones, El Derecho Penal y los Delitos Informáticos, así como las Consideraciones sobre el Sujeto Activo en los Delitos Informáticos. Sin perder de vista que la bibliografía que enriqueció a esta fue obtenida de obras nacionales como extranjeras, que si bien no se citan todas ellas, fueron de mucha utilidad para la formación de nuestro criterio, que se expresa en cada parte de este trabajo.

CAPITULO I

LA INFORMÁTICA Y LAS TELECOMUNICACIONES.

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.

En lo que respecta a los campos de aplicación, las computadoras las encontramos por todas partes: en los aeropuertos al reservar un vuelo, en una tienda de autoservicio al registrar alguna compra; en las grandes empresas, en el gobierno, en las comunicaciones a distancia, en los laboratorios procesando los resultados de un análisis, en un taller de diseño ayudando a la expresión gráfica; y en una larga lista que podemos encontrar.

Todo esto se visualizo muchos años atrás por diversos especialistas en la materia, quienes sabían que los avances de la tecnología día a día eran mejores, pero también sabían de las consecuencias que podría traer en el futuro.

Se considera que en los próximos años se darán cambios drásticos en la estructura, funcionamiento y aplicación de las computadoras. Como ya se visualizaba en los años 80´s.

De esta manera los servicios de transmisión de datos se verán ampliados, se desarrollará aún más la microelectrónica y la microprogramación, se dará mayor cabida a las computadoras tanto en oficinas, consultorios médicos, fábricas, hogares, y se alcanzará un auge de actividades tales como el correo electrónico, las compras electrónicas, el banco electrónico y aun los sistemas de aprendizaje vía computadora"[1]

[1] Business WeeK. The Microchip Revolution: Preciding New Society. 10 Nov. 1980. pág. 86.

Sin embargo, cabe destacar que hay quienes contemplan de una manera optimista el uso futuro de las computadoras, y por el contrario, hay quienes consideran que dichos instrumentos y tecnología en general llegarán a ser perjudiciales para la humanidad.[2]

Una sociedad consciente de los beneficios y peligros que implica la informatización es la que en última instancia podrá hacer válida la prospección más adecuada: la optimista.[3]

Por otro lado tenemos a las Telecomunicaciones, como aquel campo de la tecnología que tiene que ver con las comunicaciones a distancia, ya que la información con la que cuenta debe tener ciertas características que son necesarias para su transmisión, utilizando diversos medios de comunicación, orientado al medio ambiente de cada uno de los centros de trabajo, comprendiendo con esto las ventajas y alcances de las comunicaciones.

Las computadoras y las telecomunicaciones se han vuelto hoy en día, una herramienta común para la sociedad. Siendo fundamental la protección de información y los sistemas computacionales en donde ésta se trasmita, ya que la red mundial de internet ha venido a transformar todas las actividades humanas al brindar una extraordinaria forma de acceso a toda información. Por lo tanto para poder entender algún termino relacionado con las nuevas tecnologías es importante destacar los conceptos y conocimientos generales de la informática y sus áreas afines.

1. INFORMÁTICA.

La informática es una ciencia encargada del tratamiento y estudio de la información, a través del uso y aplicación adecuado de una computadora.[4]

---

[2] Cfr.Toffer. Alvin. El Shock del Futuro.

[3] Cfr.Sander. Donald. Informática. Presente y Futuro. McGraw- Hill. México, 1985.

[4] Manual de Informática y las Telecomunicaciones. elaborado por la Dirección General de Tecnología y Sistemas Informáticos de la P.G. J. D.F. (Curso Básico de Computación "La informática como herramienta para el personal sustantivo de la PFJDF) 1998. Pág.4

La informática es el conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones.[5]

Podemos ver que la informática es el estudio que delimita 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.[6]

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.[7]

Por lo tanto la informática se encuentra dividida de acuerdo al objeto de estudio y al área en que se desarrolle.

1.1. RAMAS DE LA INFORMATICA.

Las ramas de la informática son innumerables y según el campo de estudio se extienden mas y más, por lo que señalamos las de mayor actualidad. [8]

a) Cibernética.

Rama de la informática que busca integrar las teorías y estudios de la comunicación y control en máquinas y organismos vivos. Un ejemplo de aplicación es el diseño de robots industriales, simuladores espaciales, entre otros.

---

[5] Téllez Valdés Julio. Derecho Informático. Segunda Edición, McGraw-Hill México 1996, Pág. 5

[6] Mora, José Luis y Molino, Enzo. Introducción a la informática. México, 1974, pág. 12. Según cita de Téllez Valdés Julio, Derecho Informático. Pág. 5.

[7] "Informática." Enciclopedia Microsoft® Encarta® 2000. © 1993-1999 Microsoft Corporation.

[8] Cfr. Manual de Informatica y las Telecomunicaciones. Págs. 4 y 5.

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.

c) Realidad Virtual.

Área de la informática que trata el estudio de herramientas que combinadas con un equipo de computo permiten al ser humano vivir experiencias a través de Imágenes y sensaciones virtuales que sin llegar a ser reales lo parecieran. Por ejemplo se puede vivir la experiencia de encontrarse 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 vídeo, 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.

Más aun, adquirir diferentes artículos y bienes de consumo por medio de una computadora, es hoy en día una realidad. El usuario tan sólo debe ordenar a partir de

una lista desplegada en la pantalla. Asimismo, existen algunas revistas y periódicos elaborados e impresos en medios electrónicos personales.[9]

f) Domotica.

Informática aplicada a las 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 detección de presencia, etc.

1.1.1. APLICACIONES Y BENEFICIOS DE LA INFORMÁTICA.

La aplicación de la informática y los beneficios que esta proporciona se da en diferentes campos del conocimiento. Que a continuación se mencionan algunos de ellos.

Los científicos pueden usar las computadoras para llevara cabo investigaciones en áreas de gran complejidad que de otra manera no podrían considerar.

Los ingenieros de diseño y los arquitectos utilizan ahora las computadoras para simplificar el trabajo, diseñando y ampliando sus alternativas que pueden utilizar, tomando como herramienta el Cad-Diseño Asistido por Computadora.

En la medicina las computadoras han revolucionado la aplicación de esta en diversos campos, a través de complejos sistemas que permiten analizar muestras y poner al descubierto imágenes del cuerpo humano que antes no eran posibles y así determinar a tiempo un diagnóstico; mantener en los sistemas de computo, los registros y expedientes de los pacientes, así como los antecedentes para futuros tratamientos.

---

[9] Michel Beauséjour, "L'informatique, un monde en évolution", en Micro-Gazette, mayo-junio de 1996, pág. 6-12. Según cita de Pierre Gratton. Protección Informática. Edit. Trillas. México 1998. Pág 25.

Los ingenieros de estructuras emplean modelos computarizados para pronosticar los efectos de la tensión en diversas configuraciones estructurales.

Los abogados, se valen de las bases de datos para localizar información relativa a diversos homicidios, delincuentes, modos de operación y archivos de casos anteriores para tomarlos como referencia, entre muchos otros datos.

Los vendedores de bienes y servicios pueden recibir más información puntual relacionada con sus clientes e inventarios de productos; pueden ofrecer un manejo más eficiente de sus pedidos para mejorar su servicio y, por consiguiente, incrementar sus ingresos. Y todo esto con el apoyo de un sistema de computo.

Servicios de Información Compartidos a través del uso de una red de información global, la cual permite acceder, consultar y extraer información de múltiples áreas del conocimiento desde diversas partes del mundo, usando como medio una computadora y una simple estructura de comunicaciones.

Los deberes de los empleados de diversas oficinas han cambiado su repetitiva rutina, por labores más variadas y atractivas, mediante el uso de las computadoras.

1.1.2. HISTORIA DE LA COMPUTADORA.

Según cita la historia, la primera máquina de calcular mecánica, fue inventada en 1642 por el matemático francés Blaise Pascal. Siendo aquel dispositivo que 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. En 1670 el filósofo y matemático alemán Gottfried Wilhelm Leibniz perfeccionó esta máquina e inventó una que también podía multiplicar.

El inventor francés Joseph Marie Jacquard, al diseñar un telar automático, utilizó delgadas placas de madera perforadas para controlar el tejido utilizado en los diseños complejos. Durante la década de 1880 el estadístico estadounidense Herman Hollerith concibió la idea de utilizar tarjetas perforadas, similares a las placas de Jacquard, para procesar datos. Hollerith consiguió compilar la información estadística destinada al censo de población de 1890 de Estados Unidos mediante la utilización de un sistema que hacía pasar tarjetas perforadas sobre contactos eléctricos.

a) La Máquina Analítica.

También en el siglo XIX el matemático e inventor británico Charles Babbage elaboró los principios de la computadora digital moderna. Inventó una serie de máquinas, como la máquina diferencial, diseñada para solucionar problemas matemáticos complejos. 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. La tecnología de aquella época no era capaz de trasladar a la práctica sus acertados conceptos; pero una de sus invenciones, fue la máquina analítica, ya que tenía muchas de las características de un ordenador moderno. Incluía una corriente o flujo de entrada en forma de paquete de tarjetas perforadas, una memoria para guardar los datos, un procesador para las operaciones matemáticas y una impresora para hacer permanente el registro.

b) Primeros Ordenadores.

Los ordenadores analógicos comenzaron a construirse a principios del siglo XX. Los primeros modelos realizaban los cálculos mediante ejes y engranajes giratorios. Con estas máquinas se evaluaban las aproximaciones numéricas de ecuaciones demasiado difíciles, para poder ser resueltas mediante otros métodos. Durante las dos guerras mundiales se utilizaron sistemas informáticos analógicos, primero mecánicos y más

tarde eléctricos, para predecir la trayectoria de los torpedos en los submarinos y para el manejo a distancia de las bombas en la aviación.

c) Ordenadores Electrónicos.

Durante la II Guerra Mundial (1939-1945), un equipo de científicos y matemáticos que trabajaban en Bletchley Park, al norte de Londres, crearon lo que se consideró el primer ordenador digital totalmente electrónico: El *Colossus*, hacia diciembre de 1943 el *Colossus*, que incorporaba 1.500 válvulas o tubos de vacío, era ya operativo. Fue utilizado por el equipo dirigido por Alan Turing para descodificar los mensajes de radio cifrados de los alemanes. En 1939 y con independencia de este proyecto, John Atanasoff y Clifford Berry ya habían construido un prototipo de máquina electrónica en el Iowa State College (EEUU). Este prototipo y las investigaciones posteriores se realizaron en el anonimato, y más tarde quedaron eclipsadas por el desarrollo del Calculador e integrador numérico electrónico (en inglés ENIAC, *Electronic Numerical Integrator and Computer*) en 1946. El ENIAC, que según se demostró se basaba en gran medida en el ordenador Atanasoff-Berry (en inglés ABC, *Atanasoff-Berry Computer*), obtuvo una patente que caducó, varias décadas más tarde, en 1973.

El ENIAC contenía 18.000 válvulas de vacío y tenía una velocidad de varios cientos de multiplicaciones por minuto, pero su programa estaba conectado al procesador y debía ser modificado manualmente. Se construyó un sucesor del ENIAC con un almacenamiento de programa que estaba basado en los conceptos del matemático húngaro-estadounidense John Von Neumann. Las instrucciones se almacenaban dentro de una llamada memoria, lo que liberaba al ordenador de las limitaciones de velocidad del lector de cinta de papel durante la ejecución y permitía resolver problemas sin necesidad de volver a conectarse al ordenador.

A finales de la década de 1950 el uso del *transistor* en los ordenadores marcó el advenimiento de elementos lógicos más pequeños, rápidos y versátiles de lo que permitían las máquinas con válvulas. Como los transistores utilizan mucha menos energía y tienen una vida útil más prolongada; a su desarrollo se debió el nacimiento de máquinas más perfeccionadas, que fueron llamadas ordenadores o computadoras de segunda generación. Los componentes se hicieron más pequeños, así como los espacios entre ellos, por lo que la fabricación del sistema resultaba más barata.

d) Circuitos integrados.

A finales de la década de 1960 apareció el circuito integrado (CI), que posibilitó la fabricación de varios transistores en un único sustrato de silicio en el que los cables de interconexión iban soldados. El circuito integrado permitió una posterior reducción del precio, el tamaño y los porcentajes de error. A mediados de la década de 1970, el microprocesador se convirtió en una realidad, con la introducción del circuito de integración a gran escala (LSI, acrónimo de Large Scale Integrated) y, más tarde, con el circuito de integración a mayor escala (VLSI, acrónimo de Very Large Scale Integrated), con varios miles de transistores interconectados soldados sobre un único sustrato de silicio.

1.1.3. LAS COMPUTADORAS.

Una computadora es una máquina orientada al procesamiento de datos ó información. Se define como un conjunto de elementos que al interactuar entre sí, que relacionan entradas con salidas útiles para el usuario, conforme a un procedimiento predefinido por él. [10]

PC (informática), acrónimo de *personal computer*. Se utiliza para designar los ordenadores o computadoras personales.

[10] Crf. Manual de Informatica y las Telecomunicaciones. Pág. 7

La palabra computadora es un término general, que se aplica a todo el espectro de dispositivos computacionales[11]

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

Computadora.
- Monitor.
- Unidad Central de Proceso (CPU).
- Teclado.

El monitor. Es un dispositivo de salida que permite ver los resultados de las operaciones que se realizan en la computadora.

La Unidad Central de Proceso. Es el cerebro de la computadora.

El teclado. Es un dispositivo de entrada que permite introducir datos e instrucciones al equipo para efectuar alguna acción.

Ordenador o **Computadora**, dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre datos numéricos, o bien compilando y correlacionando otros tipos de información. [12]

[11] Gookin Dan y Rathbone Andy, PCs para Inexpertos, Edit. Limusa, S.A. de C.V. México, D. F. 1998, pág 33
[12] Referencias Didacticas de Informática, realizado por la Subdirección de Control Interno y Desarrollo del Instituto de Formación Profesional de la Procuraduría General de Justicia del Distrito Federal.1999 pág.2

El mundo de la alta tecnología nunca hubiera 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 fabricación gracias a las técnicas de automatización, y han permitido mejorar los sistemas modernos de comunicación.

1.1.4. TIPOS DE ORDENADORES O COMPUTADORAS.

En la actualidad se utilizan dos tipos principales de ordenadores: analógicos y digitales. Sin embargo, el término ordenador o computadora suele utilizarse para referirse exclusivamente al tipo digital. Los ordenadores analógicos aprovechan la similitud matemática entre las interrelaciones físicas de determinados problemas y emplean circuitos electrónicos o hidráulicos para simular el problema físico. Los ordenadores digitales resuelven los problemas realizando cálculos y tratando cada número dígito por dígito[13].

Las instalaciones que contienen elementos de ordenadores digitales y analógicos se denominan ordenadores híbridos. Por lo general se utilizan para problemas en los que hay que calcular grandes cantidades de ecuaciones complejas, conocidas como integrales de tiempo. En un ordenador digital también pueden introducirse datos en forma analógica mediante un convertidor analógico digital, y viceversa (convertidor digital a analógico).

[13] Idem.pág.3

a) Ordenadores analógicos.

El ordenador analógico es un dispositivo electrónico o hidráulico diseñado para manipular la entrada de datos por ejemplo, niveles de tensión o presiones hidráulicas, 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.

b) Ordenadores digitales.

Todo lo que hace un ordenador digital se basa 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. La velocidad del ordenador se mide 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 discretas 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.

1.1.5. CLASIFICACION DE LAS COMPUTADORAS.

Las computadoras se dividen por su tamaño y capacidad en tres clases: [14]

a) Macrocomputadoras.

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.

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 multiusuarias.

c) Microcomputadoras.

Las usa una persona a la vez, son monousuarias, por ello se llaman también computadoras personales o PCs (Personal Computer). Su capacidad es menor que las anteriores, cubren las necesidades de un departamento pequeño, un despacho o una oficina.

[14] Ob. Cit. Manual de Informatica y las Telecomunicaciones. Pág. 8.

1.2. HARDWARE.

Es el conjunto mecánico, eléctrico y electrónico que forma la computadora, es decir, todo lo que se puede ver y tocar.

Constituido por las partes mecánicas, 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.[15]

El hardware es la unidad del sistema, el monitor y los periféricos como el módem, el ratón o la impresora.[16]

En realidad, un ordenador 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 todos los elementos del sistema y conecta a éste con el mundo exterior.

1.2.1. UNIDAD CENTRAL DE PROCESO (CPU).

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 memoria adicionales. El resultado son unos ordenadores más pequeños y la

[15] Ob Cit. Téllez Valdés Julio, Derecho Informático, pág 11.
[16] Halliday Caroline M. Secretos de los Sistemas de PC, Edit Limusa, S.A. de C.V., México 1994, pág. 42.

reducción del sistema de circuitos de soporte. Los microprocesadores se utilizan en la mayoría de los ordenadores personales de la actualidad.

La mayoría de los chips de CPU y de los microprocesadores están compuestos de:

a) La Unidad de Control.

Es la que interpreta las instrucciones, dirige y controla las unidades de entrada y de salida, de almacenamiento y las operaciones aritméticas y lógicas. Controla la memoria externa también.

b) La Unidad Aritmética y Lógica.

Esta efectúa las operaciones aritméticas: suma, resta, multiplicación y división. Compara lógicamente, por ejemplo: entre dos números cuál es el mayor.

c) Las Unidades de Entrada y de Salida.

También llamadas periféricos, son las que nos permiten introducir o extraer información de la máquina. Por ejemplo:

1) Dispositivos de entrada.

Estos dispositivos permiten al usuario del ordenador introducir datos, comandos y programas en el CPU. El dispositivo de entrada más común es un teclado similar al de las máquinas de escribir. La información introducida con el mismo, es transformada por el ordenador en modelos reconocibles. Otros dispositivos de entrada son los lápices ópticos, que transmiten información gráfica desde tabletas electrónicas hasta el

ordenador; *joysticks*[17] y el ratón o *mouse*, que convierte el movimiento físico en movimiento dentro de una pantalla de ordenador; los escáneres luminosos, que leen palabras o símbolos de una página impresa y los traducen a configuraciones electrónicas que el ordenador puede manipular y almacenar; y los módulos de reconocimiento de voz, que convierten la palabra hablada en señales digitales comprensibles para el ordenador. También es posible utilizar los dispositivos de almacenamiento para introducir datos en la unidad de proceso.

2) Dispositivos de almacenamiento.

Los sistemas informáticos pueden almacenar los datos tanto interna (en la memoria) como externamente (en los dispositivos de almacenamiento). Internamente, las instrucciones o datos pueden almacenarse por un tiempo en los chips de silicio de la RAM (memoria de acceso aleatorio) montados directamente en la placa de circuitos principal de la computadora, o bien en chips montados en tarjetas periféricas conectadas a la placa de circuitos principal del ordenador. Estos chips de RAM constan de conmutadores sensibles a los cambios de la corriente eléctrica.

Los chips de RAM estática conservan sus bits de datos mientras la corriente siga fluyendo a través del circuito, mientras que los chips de RAM dinámica (DRAM, acrónimo de Dynamic Random Access Memory) necesitan la aplicación de tensiones altas o bajas a intervalos regulares aproximadamente cada dos milisegundos para no perder su información.

Otro tipo de memoria interna son los chips de silicio en los que ya están instalados todos los conmutadores. Las configuraciones en este tipo de chips de ROM (memoria de sólo lectura) forman los comandos, los datos o los programas que el ordenador necesita para funcionar correctamente. Los chips de RAM son como pedazos de papel

[17] "Pequeña palanca que se mueve apoyada de una base. El mover tal palanca hace que el cursor se desplace sobre la pantalla" . Dan Gookin, Wally Wang y Chris Van Buren. Diccionario Ilustrado de Computación para Inexpertos. Edit. Limuna, S.A. de C. V. 1995. Ppág.282.

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 al CPU a través de circuitos.

Los dispositivos de almacenamiento externos, que pueden residir físicamente dentro de la unidad de proceso principal del ordenador, están fuera de la placa de circuitos principal. Estos dispositivos almacenan los datos en forma de cargas sobre un medio magnéticamente sensible, por ejemplo una cinta de sonido o lo que es más común, sobre un disco revestido de una fina capa de partículas metálicas. Los dispositivos de almacenamiento externo más frecuentes son los disquetes y los discos duros, aunque la mayoría de los grandes sistemas informáticos utiliza bancos de unidades de almacenamiento en cinta magnética. Los discos flexibles pueden contener, según sea el sistema, desde varios centenares de miles de bytes hasta bastante más de un millón de bytes de datos. Los discos duros no pueden extraerse de los receptáculos de la unidad de disco, que contienen los dispositivos electrónicos para leer y escribir datos sobre la superficie magnética de los discos y pueden almacenar desde varios millones de bytes hasta algunos centenares de millones. La tecnología de CD-ROM, que emplea las mismas técnicas láser utilizadas para crear los discos compactos (CD) de audio, permiten capacidades de almacenamiento del orden de varios cientos de megabytes (millones de bytes) de datos.

3) 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 Vídeo Display Unit), que consiste en un monitor que presenta los caracteres y gráficos en una pantalla similar a la del televisor. 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 Crystal Displays) o electroluminiscentes. Otros

dispositivos de salida más comunes son las impresoras y los módem. Un módem enlaza dos ordenadores transformando las señales digitales en analógicas para que los datos puedan transmitirse a través de las telecomunicaciones.

UNIDADES DE ENTRADA.

- Teclado.
- Mouse.
- Unidades lectoras de discos y cintas.
- Scanner.

UNIDADES DE SALIDA.

- Monitor.
- Impresora.
- Unidades de cinta y discos.

1.2.2. MEMORIA PRINCIPAL.

Es donde se almacena la información con la que se va a trabajar. Hay dos clases de memoria:

a) RAM (Random Access Memory).

Memoria de acceso aleatorio: Contiene la información de lectura y escritura que se procesa en el instante, por lo que cambia constantemente su contenido.

b) ROM (Read Oniy Memory).

Memoria de sólo lectura: Son circuitos integrados con programas especialmente grabados que debe seguir la computadora cada vez que se enciende. Este tipo de memoria no es modificable.

1.2.3. MEMORIA SECUNDARIA.

Son los dispositivos de almacenamiento, donde se guarda la información, tales como los discos duros o flexibles, las cintas o los discos ópticos (CD), entre otros, permanentemente.

1.2.4. UNIDADES DE DISCO.

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 ó floppies (5 1/4, 3 1/2).

a) Discos Flexibles.

Un disco flexible (disquete ó floppy) es un disco magnético de plástico flexible. Los discos flexibles están protegidos con una cubierta. El anverso del disco es liso y el reverso presenta unos remaches.

b) Discos Duros.

Los discos duros están fijos en el interior de su computadora y pueden almacenar una gran cantidad de información, accediendo a la información contenida en la memoria mucho más rápido que los discos flexibles. Estos se diferencian por la marca y tamaño, proporcionando típicamente una capacidad de almacenamiento de 80, 100 o 120 Megabytes.

c) Discos Opticos (Cd-Rom).

La tecnología del Disco Compacto o CD fue desarrollada inicialmente desde 1976, como resultado de un esfuerzo conjunto de países como Holanda y Japón. La aplicación potencial de la tecnología CD como un medio para almacenar grandes cantidades de datos a bajo costo, dio como resultado que en 1983 se especificara un estándar para la fabricación del Disco Compacto-Memoria Sólo de Lectura (del inglés, Compact Disk - Read Oniy Memory). Los datos grabados en un CD-ROM se leen mediante una Unidad de Discos Compactos que se conecta y forma parte de un sistema de cómputo. El CD-ROM es esencialmente una tecnología para la publicación de documentos, diseñado para aquellas aplicaciones que requieren muchas copias de una base de datos grande u otra información masiva.

1.2.5. CAPACIDAD DE ALMACENAMIENTO.

El elemento básico ó unidad básica de información que usan las computadoras es el bit. Esta unidad es una abreviatura de Binary Digit (dígito binario) y tiene la posibilidad de adquirir los valores "1" y "0".

Los **bit's** se agrupan en conjuntos de ocho, formando bytes. Un byte es igual a un carácter, es decir que una letra representa en la computadora 8 bits, con ellos podemos simbolizar caracteres como las letras del alfabeto (28), los dígitos del sistema decimal (10) y aún nos sobran para los signos de puntuación, acentos y muchos otros símbolos. La capacidad de almacenaje se calcula en **bytes** y sus múltiples., como se presenta en la siguiente tabla:

8 Bits	1 Byte	1 Carácter
1024 Bytes	1 Kilobyte	113 de página
1024 Kilobytes	1 Megabyte	350 páginas
1024 Megabytes	1 Gigabyte	350,000 páginas ò 1,000 libros

1.3. SOFTWARE.

Son una serie de instrucciones que la computadora debe seguir para realizar un proceso o tarea, a la cual se le llama programa; 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; es muy variado debido a sus constantes innovaciones y lo hemos clasificado en: Sistemas Operativos, Lenguajes y Compiladores, Sistemas de Información y Programas de Aplicación.

El Software, constituye la estructura lógica que permite a la computadora la ejecución del trabajo que se ha realizado. [18]

a) Sistemas Operativos.

Son los más importantes ya que sin ellos es imposible trabajar; enlazan al usuario con el procesador de la computadora. Estos sistemas son un conjunto de instrucciones que coordinan y dirigen la operación de la computadora, la cual lo primero que hace al encenderse es leer el Sistema Operativo y transferir una parte a la memoria de la máquina, esta carga inicial o "Boot" toma el control y administra las actividades del ordenador.

Cada computadora requiere de un sistema operativo particular acorde con su arquitectura, los más usuales son:

MS-DOS	(monousuario)
WINDOWS	(monousuario)
OS/2	(multiusuario)
UNIX	(multiusuario)
NETWARE	(red)

[18] Ob Cit. Téllez Valdés Julio. Derecho Informático, pág.11.

Los sistemas operativos internos fueron desarrollados sobre todo para coordinar y trasladar estos flujos de datos que procedían de fuentes distintas, como las unidades de disco o los coprocesadores (chips de procesamiento que ejecutan operaciones simultáneamente con la unidad central, aunque son diferentes).

Un sistema operativo es un programa de control principal, almacenado de forma permanente en la memoria, que interpreta los comandos del usuario que solicita diversos tipos de servicios, como visualización, impresión o copia de un archivo de datos; presenta una lista de todos los archivos existentes en un directorio o ejecuta un determinado programa.

b) Programación.

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 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.

c) 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.

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.

Los lenguajes más comunes son:

- **Basic** (Beginner's All-purpose Symbolic Instrution Code)
  Código de instrucción simbólico 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.

- **Visual Fox, Visual C, Power Builder.**
  Lenguajes orientado a usos comerciales y oficiales en diversas áreas, administrativas, contables, financieras, entre otras.

- **Oracle, Informix.**
  Lenguajes robustos diseñados para el desarrollo de aplicaciones múltiples, pudiendo incorporar tecnología de multimedia, imágenes, entre otros.

- **Pascal.**
  Primer lenguaje estructurado y utilizado en las universidades para enseñar las bases de programación.

1.4. TELECOMUNICACIONES.

a) Concepto.

El término "telecomunicaciones" se considera generalmente que abarca todas las formas de comunicación punto a punto por medios eléctricos o de radio y también todos los métodos de radiolocalización y radio navegación. Las Telecomunicaciones son una rama de la Electrónica.[19]

b) Antecedentes.

La facultad que posee la raza humana para comunicarse, o sea, para suministrar información, ha sido la principal causa de su desarrollo. Su necesidad sé a convertido en buscar los medios de comunicación que tengan la capacidad para comunicarse a través de las distancias, todo esto lo brindan los servicios de telecomunicación de hoy en día.

El prefijo "tele" de la palabra telecomunicaciones proviene del griego, significa "a gran distancia" y enfatiza la importancia dada a las comunicaciones entre puntos distantes entre sí.

La comunicación de datos se refiere a los medios y métodos de comunicación que se emplean para transferir datos entre localidades de procesamiento. Es el adhesivo que permite la conexión interactiva directa entre las personas que trabajan con las estaciones y los sistemas centrales de procesamiento.

La tecnología de las telecomunicaciones es sólo una pequeña parte de una disciplina más extensa que puede ir desde el estudio de la lingüística hasta el transporte de las comunicaciones.

[19] Ob. Cit. Manual de Informática y las Telecomunicaciones. Pág. 25.

1.4.1. TELEMATICA.

La telemática es la disciplina que une a la informática con las telecomunicaciones, esta disciplina se identifica plenamente en la informática por su lado y con las telecomunicaciones por el otro.[20]

1.4.2. OTROS MEDIOS DE COMUNICACIÓN.

En los 75 años que siguieron al invento del teléfono se estableció una red compleja de sistemas de telecomunicación para conectar entre sí los distintos puntos del planeta, pasando de las comunicaciones analógicas a las comunicaciones digitales. Aumentando las velocidades y distancias en la transmisión de mensajes y tipo de datos. Así surgen distintos medios y áreas en la transmisión de información aparte del telégrafo y del teléfono que por su especialización son áreas que se han desarrollado significativamente a través de los años como[21]:

- La Radio.
- El Facsímil.
- La Televisión.
- Comunicaciones por satélite.
- Comunicaciones por microondas.
- Radar.
- Radiolocalización.
- Redes de Comunicación de Datos.
- Internet.

Actualmente uno de los medios de comunicación que ha causando impacto en el intercambio de información a nivel mundial es el Internet.

---

[20] 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. 7.
[21] Cfr. Manual de Informática y las Telecomunicaciones. Pág. 26.

a) Internet.

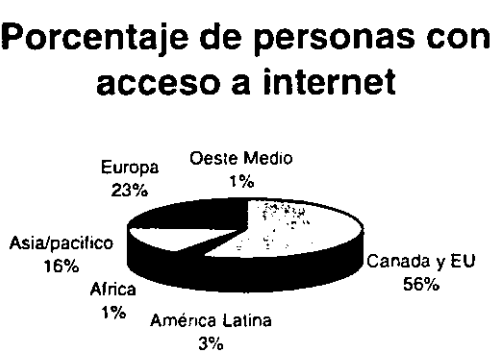
Podría definirse como una red global de redes de computadoras cuya finalidad es permitir él intercambio libre de información entre todos sus usuarios. Para darnos una idea de lo grande que es la red, una persona conectada a Internet tiene acceso a más de 25000 redes de computadoras en todo el mundo y cuenta con más de 70 millones de usuarios de la red potencialmente dispuestos a compartir con él experiencias, conocimientos e información. A Internet están conectados personas de todo tipo y clase.[22]

El Internet basa su utilidad básicamente en cuatro servicios: 1) correo electrónico, 2) servicio de información, 3) acceso remoto y 4) transferencia de archivos. Con el correo electrónico, cada usuario puede ponerse en contacto con cualquier otro a lo largo de todo el mundo e intercambiar información con él, mensajes, archivos, experiencias, etc. Con el servicio de información se tiene acceso a una cantidad inmensa de información de todo tipo y de todas las áreas de la ciencia a su alcance sin tener que salir de su casa u oficina, Medicina, Biología, Computación, Ciencias, Noticias, Empresas, Servicios y mucho más. Mediante el acceso remoto podemos conectarnos potencialmente como terminal de cualquier computadora o red situada en cualquier parte del mundo. Por último, mediante el servicio de transferencia de archivos, cualquier usuario puede recuperar archivos desde cualquier lugar.

Internet es sobre todo una herramienta para la comunicación. El uso que se le pueda dar a este depende mucho de las necesidades e inventivas de los usuarios. Si hay algo que caracteriza a Internet es su capacidad de evolución y de adaptación a las nuevas necesidades que puedan aparecer. Hoy en día, los usos y aplicaciones fundamentales de Internet son múltiples.

[22] Idem. Pág. 27.

En la actualidad, internet es la red de computación más grande del orbe porque agrupa numerosas redes locales.[23]



1.4.3. REDES.

Al haber necesidad de tener comunicación de datos que involucra a más de dos puntos de comunicación, nace lo que se conoce como "Redes de Comunicación de Datos". Las Redes de Comunicación de datos tienen su origen desde la invención del telégrafo, y posteriormente evolucionaron a la red de télex.

Con el advenimiento de las computadoras y con la necesidad de procesar información desde diversos lugares nace lo que ahora conocemos como redes de computadora, esto es la infraestructura de comunicaciones que permite la realización de las mismas, las cuales se han ido desarrollando conforme avanza la tecnología tanto en el campo de las computadoras como en el campo de las telecomunicaciones.

Alguna de las razones que han conducido al desarrollo de las redes de comunicación de datos son:

1. Satisfacer la demanda, cada vez mayor, de los servicios de cómputo.
2. Organizar recursos geográficamente dispersos.

---

[23] Francois, Picard, "Internet, premier de l'autoroute de l'information", en Autout Micro, octubre de 1994, pág 40. Según señala Pierre Gratton, Protección Informática pág. 28.

Las tendencias actuales indican una definitiva orientación hacia la conectividad de datos. No sólo en el envío de información de una computadora a otra sino, sobre todo, en la distribución del procedimiento a lo largo de grandes redes en toda la empresa.

a) Redes Informáticas.

Análogamente como ocurrió con otras etapas de la civilización, en la era informática y de telecomunicaciones, también se han implementado redes que siguen los mismos objetivos generales de mantener jerarquías compartiendo sus recursos y haciendo más fuertes a las agrupaciones que las integren.

También es importante señalar que las redes se agrupan según el objetivo específico que persigan, en tres tipos:

1. Redes de investigación y cooperación como la Red Académica del Politécnico y las redes del Tecnológico y UNAM y BITNET en Estados Unidos.

2. Redes de empresas privadas, especialmente de multinacionales como IBM, DEC, XEROX .

3. Redes comerciales para uso del público en general, y vía pago de suscripción como las accesibles a través del SECOBI del CONACYT o INTERNET, red global que en los últimos tiempos se ha convertido en un medio muy importante de acceso a información de todo tipo.

b) Concepto.

Una red es el conjunto de computadoras y dispositivos periféricos que se unen física y lógicamente para compartir sus recursos y mantener una comunicación directa para el envío y recepción de información sea voz, datos, imágenes, etc.[24]

c) Clasificación de las Redes.

Las redes de empresas privadas se pueden clasificar por la cobertura que tienen en dos:

Redes LAN (Local Area Network) Redes de Área Local, lo cual significa que su cobertura es en un solo lugar físico como un edificio, conectado a sus diferentes adscripciones.

Redes WAN (Wide Area Network) Redes de Área Amplia, en donde sus estaciones se conectan entre edificios, ciudades, estados y países.

d) Ventajas del Uso de Redes.

- Compartir información.
  - Bases de datos.
  - Información administrativa.
  - Accesos a Sistemas de información desde cualquier oficina.

- Evita el traslado de información en discos flexibles.

- Compartir Periféricos.
  - Impresoras.
  - Unidades CD-ROM.
  - Unidades de Discos Flexibles.
  - Discos Duros.

[24] Ob. Cit. Manual de Informática y las Telecomunicaciones. Pág. 30.

- Comunicación entre usuarios a través de Correo Electrónico para el envío y recepción de información.

1.4.4. LA RED COMO AVANCE TECNOLÓGICO Y EL IMPACTO QUE TRAE A LA SOCIEDAD POR SU USO.

La Red, por computación es el avance tecnológico más significativo de este siglo en todo el mundo no obstante que se han dado varios adelantos científicos y tecnológicos como por ejemplo: la llegada a otro planeta, el avance científico para la lucha contra el cáncer, el sida, etc.

Por consiguiente esta herramienta (La Red) auxiliara más a todas estas investigaciones, ya que el intercambio de notas entre científicos, ayudara para que trabajen en conjunto; esto beneficia a que naciones como México o "países del tercer mundo pudieran un día significar un freno a la fuga de cerebros"[25] ya que al preveerlos de una infraestructura computacional capaz de auxiliarlos y propiciar el intercambio de información se eficientizan los procesos de investigación.

La Red, como se pude ver, es un inminente mecanismo para realizar transacciones comerciales; cabe señalar que, como medio de comunicación, esta siendo utilizado por grandes Consorcios, Empresas, Negocios, etc. Para dar a conocer sus productos sin descuidar los medios más comunes tales como: la radio, televisión y prensa. Sin embargo en la Red estos anuncios publicitarios, llegan al consumidor por medio de estímulos interactivos que permitan al navegante involucrarse con el mismo, mientras es percibido por el usuario.

Por otro lado, nos encontramos con un medio de comunicación que no ha sido censurado por la transmisión de información como ha ocurrido con los medios tradicionales de comunicación, ya mencionados. No obstante se tiene que puntualizar que la Red, no es un medio tan veraz como se esperaba, ya que muchas de las noticias aún no son

[25] Flores Olea, Víctor. Internet y la Revolución Cibernética. Edit. Océano de México, 1997. Pág., 33.

confirmadas o el que emite la noticia oculta su identidad para especular o salvaguardar su integridad.

a) Es un Medio para Comunicarse con Todo el Mundo.

Las redes y en especial Internet ofrecen, el servicio de poder comunicarse con otra computadora o con el usuario en cualquier parte del mundo, sin tener con ello que pagar largas distancias. A lo mismo que el usuario no se preocupa por el tiempo en que realiza la comunicación en Internet pues se da la opción de entrar a un grupo de conversación, para ello en la misma Red existen diferentes alternativas como el CHAT. Esta no es la única opción para comunicarse en las redes, pero si es una de las más utilizadas. En ellas no solo se busca círculos de charla, sino que encontramos que las personas realizan intercambio de información o de sentimientos con otras personas.

También encontramos que hay otras posibilidades u opciones de comunicarnos, una de las más utilizadas en el mundo es aquella llamada CORREO ELECTRÓNICO (email), esto se refiere a dejar mensajes como el correo clásico en otra computadora, pero aquí el receptor si tiene el vínculo para regresar el mensaje al emisor, incluso es de gran utilidad para todos ya que se presume que es una comunicación confidencial.

Cabe señalar, que la RED va a crecer mucho más en años siguientes, pues como lo veremos "en la estadística proporcionada por City Bank, estima que dentro de tres años habrá 100 millones de personas en Estados Unidos utilizando Internet, y que ésta servirá para un comercio anual de 100 millones de dólares".[26]

Así como también hay una contraparte que niega que la Red crecerá, pues ha comenzado a romperse por la sobrecarga de datos (correo electrónico, transferencia de archivos y la transmisión de vídeo y audio) y por el intenso tráfico que soporta (N millones de acceso al día). Para muchos usuarios, la consulta de información se ha vuelto más lenta e imprevisible. Otro problema es el frecuente corte de suministro eléctrico en

[26] Reforma. Hay tecnología, falta confianza. Kanell. E. Michael. Interfase. Lunes 28 de abril, 1997. Pág.59 A.

diversas partes de la RED. Asimismo, hay constantes "caídas" de sistema en diversas firmas que otorgan el acceso a la RED.

Analizando a fondo este tema, nos encontramos con la paradoja "Es un hecho que algunos de los indicadores que mejor definen el desarrollo de una sociedad son el número de teléfonos por habitantes y de redes de carreteras; esto tiene que ver con la capacidad de los individuos para comunicarse y obtener mayor información."[27] Podrá ser, que en un futuro, consideremos como ciudad desarrollada a aquélla que tenga el mayor número de nacionales dentro de la RED.

Cabe mencionar, que el *Usenet* es otro servicio que en términos de comunicación nos ofrece grandes ventajas. Al igual, que el Correo Electrónico, podemos enviar mensajes a otras personas, con la diferencia de que aquí, los mensajes son públicos y los pueden leer y responder todas las personas que formen parte de un "grupo de interés".

Hay un cúmulo importante de información que viaja en la RED, en la que podemos encontrar visitas guiadas a museos, enciclopedias, viajes turísticos, información generada en las universidades en el momento mismo de los hechos etc. y aquí destaca el aspecto económico, puesto que al sentarnos frente a la computadora podemos tener acceso a esta variedad de opciones y no tener que trasladarnos a esos sitios distantes ni adquirir enciclopedias costosas o planear unas mejores vacaciones teniendo en nuestra pantalla aquellos sitios que nos llamaron la atención de conocer y no lo contemplábamos en los folletos.

Otra herramienta es la TelNet, la cual permite conectarse a otra computadora de cualquier parte del mundo para obtener información. Al rededor del planeta existen, por ejemplo, computadoras que permiten a los usuarios consultar el reporte del clima, conocer los movimientos del mercado, etc. e incluso se puede decir que ofrecen varios servicios simultáneos.

---

[27] El universal. Internet hoy, mañana y a futuro. Guerra, Víctor. Universo de la Computación. Lunes 3 marzo, 1997. Pág.5.

"Su expansión, como se sabe bien, ha sido exponencial en los últimos años hasta el punto en que se cubre hoy una red mundial de computadoras entrelazadas que probablemente sobrepasa ya los cincuenta millones de aparatos en más de ciento cincuenta países. Para el año 2000 se calcula que existirán en el mundo alrededor de trescientos millones de usuarios de Internet".[28]

b) Como Instrumento para Adquirir Bienes.

En la RED se realizan miles de intercambios comerciales entre empresa y público en general, es aquí también donde se llevan acabo un sin número de delitos diarios, y hasta el día de hoy fácilmente se siguen cometiendo, Sin embargo este tema lo profundizaremos en él capitulo siguiente.

En la RED el usuario selecciona algo en un catálogo en la pagina web luego llena una orden con su número de tarjeta de crédito, y se realiza la operación.

El comercio electrónico es la realización de transacciones sobre redes computacionales, entre ellas la de Internet. Incluye la compra y venta de bienes sobre ésta publicidad y mercadotecnia electrónica, y transferencias electrónicas de fondos. Buscando generar guías y recomendaciones para el uso adecuado del comercio electrónico con la tecnología adecuada y así generar oportunidades de negocios para las empresas pequeñas y medianas más allá de las fronteras de sus propios países. Por ejemplo, se creó el Comité de Trabajo de Comercio Electrónico, auspiciado por el Grupo de los 7, que integra a Estados Unidos, Canadá, Japón, Alemania, Francia, Inglaterra e Italia.

Para ampliar la representatividad del Comité, recientemente se invito a Infosel y al Banco Interamericano de Desarrollo para que representaran a Latinoamérica".[29]

[28] Ob. Cit. Reforma. Pág. 25.

[29] Reforma. Genera Oportunidades Comercio Electrónico. Chavez, Miguel Angel. Interfese. Lunes 28 de abril de 1997. Pág. 6.

"Hoy, el comercio en Internet en México representa únicamente 0.04% del mundo pero para el 2001 se estima que será 0.3%. ver gráfica." [30]

USUARIOS DE INTERNET EN MÉXICO 1998.

	Mega	Corporativos	Grande	Mediana	Pequeña	Micro	Total
Comercio	2,396	303	268	205	477	356	4,005
Finanzas	4,709	4,657	7,974	3,938	3,096	159	24,533
Manufactura	5,571	3,011	5,279	2,219	21	5	16,106
Procesos	33,890	17,133	5,524	3,312	121	13	59,992
Servicios	6,651	11,574	7,746	5,650	11,096	2,752	45,469
Servicios P.	88,859	36,290	76,878	2,079	3,651	51	207,808
Total	142,077	72,967	103,669	17,403	18,462	3,335	357,912

NÚMERO DE EMPLEADOS EN LA ORGANIZACIÓN

Micro: < 15 Pequeña: 16-100 Mediana: 101-250 Grande: 251-1000 Corporativo: 1001-5000 Mega: > 5000

Si bien el comercio electrónico está creciendo rápidamente, se mantiene como un experimento relativamente pequeño, de quizás mil millones de dólares al año (minúsculo en comparación con los 6 billones de dólares de la economía estadounidense)".[31]

---

[30] El Universal. Internet/Intranet: ¿realidad o espejismo?. Pérez Fajardo. Judith. Universo de la Computación. Lunes 27 de octubre de 1997. Pág. 9

[31] Ob. Cit. El universal Pág. 9.

Mientras tanto, la mayoría de los negocios que han establecido presencia en la World Wide Web lo han hecho en gran parte para no verse fuera de moda, aunque no esperan obtener grandes recompensas aún. No obstante, hay empresarios que no pierden el entusiasmo para defender la tecnología.

Quienes están a favor del comercio electrónico confían en que dentro de poco las redes computacionales del mundo serán aprovechadas para distintos fines comerciales, tales como colocar pedidos, hacer pagos por bienes y servicios, realizar operaciones bancarias, y permitir la coordinación de negocios entre clientes y proveedores.

De hecho, gran parte de eso ya se realiza hoy en día, pero solamente unos cuantos consumidores compran pantalones o refacciones por la RED. Y la mayor parte de la actividad se reparte entre unas pocas empresas (bancos, Correduría, firmas de alta tecnología).

Como se ha visto, el acelerado desarrollo de las tecnologías y la comunicación y de la información impone otra visión en las relaciones entre las personas y naciones se conceptualiza la unificación económica y se desarrollan nuevas formas de comercializar es decir, se forma el libre mercado que forma el concepto de los mercados electrónicos:[32]

- Los mercados electrónicos llevan a cabo las tres funciones de los mercados tradicionales, apoyándose en la tecnología de redes y sistemas, reduciendo con ello los costos de transacción, incrementando su efectividad y creando nuevos roles intermediarios.

- Un mercado electrónico es un mecanismo económico de coordinación del flujo de bienes y servicios, mediante las fuerzas de oferta y demanda, y de las transacciones de mercado entre compradores y vendedores vías sistemas electrónicos.

[32] Ob. Cit. Riestra Gaytán Emma. Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 8

En el mundo más de 171 millones de personas cuentan con acceso a Internet y realizan transacciones por cerca de 43 mil millones de dólares.

En 1997 había en nuestro país cerca de 3.5 millones de computadoras y se espera que en el 2001 la cifra supere los 5.2 millones, mientras que los usuarios de internet se estiman que estarán por arriba de los 2.2 millones en este año; es decir un crecimiento de 65%, una de las tasas de crecimiento más alto en el ámbito internacional.[33]

c) El Medio de Información más Grande en Todo el Mundo.

La RED como ya lo hemos observado es un instrumento tecnológico con el cual podemos transmitir información, aunque no hay que sorprendernos pues esa fue la idea por la cual se creo. Sin embargo en sus orígenes la RED solamente se encontraba como una herramienta científica y militar, para el día de hoy es una "supercarretera de la información", con la variedad de que es 100% civil, y en ella se puede expresar quien guste. Debemos contemplar una legislación de la RED para que en ella no existan xenofobicos, racistas, gente que dañe la reputación de otra, y esconda la mano, lo cual lo haría inmune a sufrir un castigo o ha resarcir los daños causados, una de las ventajas más apreciables que encontramos es, que la RED no esta centralizada y esto es de gran beneficio, ya que si se rompiera una sección de la telaraña, la porción que quedara estaría libre y podría volver a renovarse. En éste punto queremos enfatizar que gracias a que la RED no se encuentra centralizada no se puede legislar por completo; ya que lo que sea bueno para una nación para otra no lo será, pero un país si puede regular a la RED por cuanto hace a los usuarios que se encuentren en ese territorio, de esto hablaremos más adelante.

Otro detalle que no debemos olvidar, por ejemplo es el uso de la RED que ha demostrado su eficiencia a través de los periódicos que se integraron a la misma, lo que hace suponer

[33] Idem. Pág. 8

que estas instituciones informativas, si responderán de la veracidad de sus publicaciones; algunos Gobiernos también emiten sus comunicados públicos (las declaraciones de sus voceros oficiales) en la RED; en México tuvimos el privilegio por primera vez en nuestra historia, de poder conocer los resultados electorales de julio (1997) en el momento mismo en que estos eran capturados por IFE[34], cosa que habla muy bien del tan sonado cambio democrático de nuestro país.

Existen muchos hechos que pueden demostrar la ventaja de la RED, tal es el caso que ocurrió en "En diciembre de 1996, el Times de Nueva York que dio a conocer que la RED de redes había dado al traste con los planes del presidente serbio Slobodan Milosevié - enemigo de la libertad- de suprimir la prensa independiente. Los periodistas y disidentes serbios formaron páginas electrónicas en las que narraron su historia a sus compatriotas y al resto del mundo".[35]

Lo anterior nos da un parámetro de la magnitud de la RED, y nos deja entrever que no existen medios suficientes para poder controlarla, sin embargo, podemos tomar medidas preventivas que reglamenten el debido uso.

Otro ejemplo visible en la RED como el medio de información más masivo que en un futuro será es el que encontramos "Hoy en día, cientos de personas que platican y discuten en línea con bots (Robots de Software que habitan la RED); otros tantos aceptan psicoanalizarse por sistemas expertos, o bien acuden a confesares con un sacerdote electrónico en el WWW".[36]

Es por eso y muchos otros ejemplos más que podemos citar, que la RED es hoy por hoy el medio de comunicación más trascendente de nuestros tiempos, y no nos queda duda

[34] IFE: Instituto Federal Electoral.
[35] Selecciones. Se equivoco George Owell. Kinsley, Michael. Edit Reader's Digest. D.F. octubre de 1997. Págs. 219-224.
[36] La Jornada. La Jornada Virtual. Yehya, Naief. Domingo 27 de abril de 1997. Cultural Pág. 3.

que "la supercarretera de la información" se convertirá en el instrumento más utilizado para la comunicación.

De tal forma que ese es un factor que no debemos descuidar, ya que podría perjudicar a la seguridad de las personas, su honor, su patrimonio, etc., es el momento para comenzar a preocuparnos por todos los delitos que se pudieren realizar en este sistema de comunicación.

1.4.5. NOCION DE VIRUS.

Los virus de las computadoras son programas elaborados por personas, estos programas contienen instrucciones para que la computadora las ejecuten.

Un virus de computadora es un programa que se copia a sí mismo en una computadora e infecta a otros programas, interrumpe el funcionamiento del sistema o se infiltra en una red para afectar el rendimiento de las computadoras afectadas.[37]

Se les dio el nombre de virus por la gran similitud entre el funcionamiento de estos y los virus biológicos.

Como se sabe los virus biológicos infectan las células del organismo humano y modifican su información genética al irse reproduciendo dentro de las células afectadas, también pueden estar latentes en el organismo durante bastante tiempo sin que éste presente ningún síntoma de infección. Los programas de virus tienen algunas características especiales: son muy pequeños, casi nunca incluyen el nombre del autor, se reproducen así mismos y toman el control o modifican otros programas.

[37] Ob. Cit. Pierre Gratton. Protección Informática. Pág.254.

Antes de presentarse el problema de los virus en las dependencias del gobierno, empresas y centros de investigación había un gran escepticismo sobre el tema, por lo que no se ha dado una definición exacta de ellos.

"Todo aquél código que al ser ejecutado altera la estructura del software del sistema y destruye programas o datos sin autorización ni conocimiento del operador". [38]

La definición mencionada anteriormente se considera como una de las más claramente expresadas para todo tipo de lectores pues el concepto de virus es tan compleja, como la diversidad y variedad de clasificaciones y efectos que estos provocan.

a) Antecedentes.

No existe hasta el momento ninguna información fidedigna que permita reconstruir la historia de los virus y sus efectos. Sin embargo, se tiene noticia que desde la década de los 50's Jonh Von Neumann, descubrió algunos programas "que se reproducen a sí mismos" estableciendo el primer antecedente de los virus.

No es sino hasta 1983, cuando el Dr. Fred Cohen realizó un experimento en la Universidad del Sur de California, presentando el primer virus residente en una PC, es por ello que se le conoce como el Padre de los virus informáticos.

En 1986 se difunde desde Pakistán un virus que provoca destrozos en la información de miles de usuarios, atacando a una gran cantidad de computadoras, este hecho fue provocado por dos hermanos residentes en Lahore, Pakistán que cansados de que los usuarios copiaran grandes cantidades de cada original vendido, introdujeron en copias legales de programas famosos y en su propio programa, un virus benigno que otros programadores modificaron hasta convertirlo en uno de los virus más dañinos. Los turistas que llegaban a comprar a su tienda se llevaron a sus países los programas

[38] Rojas Alberto en su artículo "¿Ya vacunó a su PC?" Artículo - Revista PCMPS. Pág. 12.

infectados, contagiando más de 18,000 computadoras, solamente en los Estados Unidos de Norteamérica.

b) Tipos de Virus.

1. Virus Latente.

Es aquel que espera una fecha determinada o algún evento para activarse.

2. Virus Activo.

Este se activa desde el momento de introducirse en una computadora.

3.- Virus Mutante.

Puede activarse a sí mismo y sufrir una transformación para adaptarse a las condiciones del medio donde se propaga.

4. Virus Mortal.

Se trata de un virus destructivo que borra los programas o datos contenidos en el disco duro o los disquetes e interrumpe el funcionamiento de la computadora o la red a la que está conectada.[39]

Cuando un Virus logra introducirse en un soporte adecuado para su ejecución, busca la oportunidad de propagarse al disco duro de la computadora o contaminar los disquetes insertados en las unidades del sistema.[40]

Uno de los problemas más graves surgido a raíz de la publicidad de los virus es de carácter psicológico. Hoy en día muchos problemas originados por algún error en la máquina o del operador son atribuidos al ataque de virus. No hay que alarmarse y primero tener paciencia, verificar si no es una falla de Hardware o Software, antes de afirmar ¡mi computadora tiene virus!

---

[39] Ob. Cit. Pierre Gratton. Protección Informática. pág.256.

[40] P. Astor y E. Kain. "Les virus informatiques: connaissances, prévention et protection", en Soft & Micro, septiembre de 1991. Según señala Pierre Gratton. Protección Informática pag. 257.

CAPITULO II.

EL DERECHO PENAL Y LOS DELITOS INFORMÁTICOS.

Siempre sé a hablado de los múltiples beneficios que trae consigo los medios de comunicación y el uso de la informática, en favor de la sociedad, pero también sabemos que el desarrollo de la tecnología informática trae consigo aspectos negativos, que dejan abierta la posibilidad de cometer conductas antisociales y delictivas, las cuales se manifiestan de muchas formas, ya que hoy, los sistemas computacionales dan pauta a nuevas oportunidades para infringir la ley.

Podemos damos cuenta que los llamados delitos informáticos, no son cometidos por las computadoras, sino por las personas que se valen de ello para cometerlos, por eso la gran importancia de regular dichas conductas en ley penal.

Nuestro país, en la actualidad no cuenta con un adecuado control sobre los delitos informáticos, todo esto, como un reflejo de la falta de legislación en dicho tema, siendo evidente la suma de víctimas que día a día se ven afectadas por estas conductas.

Por lo que será necesario analizar diversas concepciones, respecto al derecho informático, la informática jurídica y los delitos informáticos, tomando en consideración los estudios realizados por algunos de los países Europeos, Estados Unidos de Norteamérica y América Latina, los cuales han aportado avances considerables a sus leyes penales.

2. DERECHO INFORMÁTICO.

En la actualidad muchos de nosotros hemos escuchado temas relacionados con el Derecho Informático o la Informática Jurídica, que sin reflexionarlos pensaríamos que se trata de la aplicación de las computadoras al estudio y practica del derecho, teniendo conceptos muy vagos de los mismos, siendo que encierran concepciones totalmente distintas en su aplicación, por lo que será necesario introducirnos a fondo sobre estos dos temas que son de mucho interés para nuestra investigación.

"Estamos en una sociedad donde las tecnologías de la información ha 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".[41]

La importancia de la información es tal que nuestra carta Magna en su reforma de 1977 reconoce el Derecho a la Información, por adiciones a los artículos 6 "...el derecho a la información será garantizado por el Estado."[42] 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...."[43] de tal suerte, resultado, que estructuralmente hablando se consagra como garantía individual, y también como garantía formalmente política y materialmente social.[44]

---

[41] Rodríguez Hernández Victor, Director de la Revista Electrónica de Derecho Mexicano. La Informática Jurídica y su Papel en el Derecho Méxicano.1999 Derecho Org.(México) R.E.D.I. (Revista Electrónica de Derecho informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www. yahoo.com.) pág. 1.

[42] Cuadernos de Derecho. Compilación y Actualización Legislativa. Constitución Política de los Estados Unidos Mexicanos, Vol. 67, enero de 2000, Director Lic. Jorge Orozco Flores, Públicación de ABZ Editores S.A. de C.V., pág.4.

[43] Idem. Pág. 13

[44] Ob Cit. Rodriguez Hernández Victor, La informática Jurídica y su Papel en el Derecho Mexicano, pág. 1

El mismo Derecho, ha reconocido y tratado de distintas maneras esa información, de la cual ha hablado tanto; a veces como en la cita anterior creando normas y leyes que la regulen o garanticen, también estudiando y analizando dicha información para crear, trasmitir y aplicar los Derechos y Obligaciones que rigen nuestra vida en sociedad.[45]

El Derecho Informático, como una nueva rama del conocimiento jurídico, es una disciplina en continuo desarrollo, teniendo en su haber (al menos hasta esta fecha) incipientes antecedentes a nivel histórico; sin embargo, podemos decir que las alusiones más específicas sobre esta interpelación, las tenemos a partir del año de 1949 con la obra de Norbert Wiener,[46] en cuyo capítulo IV, consagrando al derecho y las comunicaciones, nos expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico.[47]

Por lo que será de suma importancia hablar de todos los antecedentes históricos y aspectos generales que representa la informática jurídica y la diferencia con el derecho informático.

2.1. ANTECEDENTES Y ASPECTOS GENERALES DE LA INFORMÁTICA JURÍDICA.

El punto de partida, de lo que en si mismo encierra la concepción de la informática jurídica, lo vemos plasmado 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.

Siendo importante destacar 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 en su aplicación y objetivos.

---

[45] Idem. Pág 1.
[46] Sobre el particualar consultar la obra de los maestros Fix- Zamudio, Trueba Urbina y otros. Según señala Téllez Valdés Julio en su obra Derecho Informático. Pág. 21.
[47] Idem. Pág 21.

Aunque difícil de conceptualizar por el variado numero de peculiaridades y muy a pesar de los opuestos puntos de vista que pudieran provocar, podemos decir que el Derecho Informático es una rama de las ciencias jurídicas que contempla a la información como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática).[48]

En función a lo anterior, es notorio que la clasificación de dicho Derecho Informático obedecerá a dos vertientes fundamentales. La informática jurídica y el derecho de la información.[49]

La Informática Jurídica y el Derecho Informático tras denotados esfuerzos por consolidarse como ramas autónomas del Derecho, constituyen dos de las mas 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 de avanzada del Derecho.[50]

Siguiendo a GIANCARLO TADDEI ELMI quien refería que "la informática jurídica nace hacia fines de los años cuarenta bajo la onda del entusiasmo cibernético, y cabalga sobre la fortuna del neopositivismo lógico, ambientación cultural extremadamente favorable y homogénea a la formalización del derecho.[51]

Por otra parte en el año de 1949 el juez norteamericano LEE LOEVINGER público un artículo de 38 hojas en la revista Minnesota Law Review intitulado "The Next Step Forward" en donde menciona que "el próximo pasa adelante en el largo camino del

[48] Ob. Cit Téllez Valdés Julio. Derecho Informático. Pág. 22.
[49] Idem. Pág 22.
[50] Lara Márquez Jaime. Abogado. Profesor de Informática Jurídica de la pontificia Universidad Católica del Perú (Perú). Derecho y Técnologia. "Una visión prospectiva del Derecho". 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www.yahoo.com) Pág. 1.
[51] Bauzá Reilly Marcelo. Abogado Asesor en temas de Derecho & Informática. Doctor en Derecho y Ciencias Sociales. Profesor de Informática Jurídica de la Universidad de la República. Director de CINADE (Centro de Investigación de Informática Aplicada al Derecho. Facultad de Derecho de la UR). DEA en Informática Jurídica y Derecho de la Informática en la Universidad de Montpellier. Vicepresidente de FIADI (Federación Iberoamericana de Derecho e Informática). (Uruguay). "Informática Jurídica en la Facultad de Derecho. Roles y Perpectivas". 1999. Derecho Og. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www. Yahoo.com) Pág. 4.

progreso del hombre, debe ser el de la transición de la Teoría General del Derecho hacia la Jurimetría, que es la investigación científica acerca de los problemas jurídicos..." [52]

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. Corría el año de 1949 cuando es manager al frente de la Oficina encargada de dichos controles acuña el término "Jurimetría", a propósito de poder llegar a "medir"- si ello fuera posible- la conducta de los jueces dentro de un sistema jurídico como el anglosajón, en el cual el descubrimiento del precedente judicial pertinente –dentro de una masa creciente de los mismos- ha sido siempre una concreta necesidad para el funcionamiento del sistema jurídico." [53]

Para el año de 1963 el estudioso HANS BAADE, al prolongar una obra colectiva sobre "jurimetría" definió a ésta como el análisis científico de los problemas jurídicos, señala tres áreas de estudios y aplicaciones: Primera, la memorización y recuperación de datos contenidos en soporte informático, segunda, el análisis conductista de las decisiones judiciales mediante revelamientos estadísticos y cálculos probabilísticos; y tercera, la aplicación de la lógica simbólica a los fallos y normas jurídicas en general.[54]

Como se puede apreciar, esta primera fase de lo que al devenir del tiempo vendría a configurar la Informática Jurídica, tiene lugar dentro del sistema jurídico "common law" (dentro del sistema jurídico anglo-norteamericano, el conjunto de reglas y normas tradicionales que constituyen el núcleo común a los Derechos de ese sistema, particularmente según han sido reconocidos por la jurisprudencia).[55] Un ambiente cultural y unas necesidades de ejercicio y práctica de derecho, llevaron a descubrir ciertas utilidades del computador para objetivos fundamentalmente de tipo documental y

---

[52] Cabe mencionar que los articulados de Loevinger tuvieron tal trascendencia que a principios de los sesenta surgió una revista con el nombre de Jurimetrics Jornal, que en un primer momento fue conocida con el nombre de MULL (Modern Uses of Logic Law). Según señala Téllez Valdés Julio. Derecho Informático. Pág.22.

[53] Ob Cit. Bauzá Reilly Marcelo. Informatica Jurídica en la Facultad de Derecho. Roles y Perpectivas. Pág.4

[54] Idem. Pág. 5

[55] Cabanellas de las Cuevas Guillermo y Hoague Eleanor C. Diccionario Jurídico, Inglés- Español. Edit. Heliasta S.R.L. Buenos Aires, Argentina 1996. Pág. 121.

previsional, en cuento a la conducta seguida por los jueces antes similares hipótesis fácticas.[56]

Tenemos que gran parte de las preocupaciones de la informática jurídica han partido, del reconocimiento de los problemas derivados de la "explosión documental"[57] y de las correlativas dificultades que ello genera en el manejo de las fuentes, inclusive para los propios especialistas en áreas bien determinadas.

Para el año de 1968 el reconocido profesor italiano MARIO LOSANO, propuso el término Iuscibernética con el propósito de reemplazar al generalmente utilizado hasta entonces jurimetría, pero reformulando sus alcances en cuanto comprendía una aproximación cibernética del 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 optimo tratamiento informático.[58]

Por otra parte en 1962, el francés PHILIPPE DREYFUS inventó un termino nuevo Informatique, unificado de esta manera los dos términos de "información y "automática".[59]

A partir de esta etapa se ha logrado la difusión y aceptación en el ámbito académico jurídico el término informática jurídica, para designar la aplicación de la informática al derecho por contraposición al de derecho informático.

---

[56] Ob Cit. Bauzá Reilly Marcelo. Informatica Jurídica en la Facultad de Derecho. Roles y Perpectivas pág.5

[57] López Muñiz Goñi. Miguel. Informática Jurídica documental. Madrid. Diaz de Santos.S.A. 1984. Pág. 11 Según señala Lara Márquez Jaime. Derecho y Técnologia. Una visión prospectiva del Derecho. Pág. 2

[58] Losano Mario. Curso de Informática Jurídica. Madrid, Tecnos, 1987, pág. 45 y siguientes. Según cita Lara Márquez Jaime. Pág. 2 .

2.1.2. CONCEPTOS Y GENERALIDADES DE LA INFORMÁTICA JURÍDICA.

La informática Jurídica debe entenderse como el conjunto de estudios e instrumentos derivados de la aplicación de la informática al Derecho, o mas precisamente a los procesos de creación, aplicación y conocimiento del Derecho.[60]

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 este uso presta al desarrollo y aplicación del derecho. En otras palabras, es ver el aspecto instrumental dado a raíz de la informática del derecho.[61]

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 los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho (informática jurídica de gestión).[62]

Así pues la informática jurídica tiene por objeto la aplicación de la tecnología de la información al derecho.[63]

---

[59] Frosini Vittorio, Informática y Derecho. Bogotá, Edt. Temis. S.A., 1988 pág. 43 Según cita Lara Márquez Jaime. Pág. 2

[60] Concepto sustenado por el Dr. Hector Fix Fierro, Según lo cita Rodríguez Hernández Victor ."La Informática Jurídica y su Papel en el Derecho Méxicano" REDI (Revista Electronica de Derecho Informatico). pág 2.

[61] Peñaranda Hector. Doctor en Derecho Magister en Gerencia Tributaria, Profesor y Jefe de Cátedra de la materia: Seminario de Informática Jurídica de la Universidad Rafael Belloso Cacín, Maracaibo. Venezuela. "La informática jurídica y el Derecho informático como ciencias. El derecho informático como rama autónoma del Derecho". 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www.yahoo.com). Pág. 2.

[62] Perez Luño, Antonio Enrique. Manual de Informática y derecho. Barcelona, Edt. Ariel, 1996, pág 22. Según señala Lara Márquez Jaime. Pág. 2

[63] Idem. Pag.22.

De igual .forma consideramos importante señalar las diversas posturas de los especialistas en la materia quienes han analizado debidamente la naturaleza y objeto de la informática jurídica.

a) Informática Jurídica como suma de tres áreas: jurimetría, informática jurídica y derecho de la informática.

Fue de los primeros planteamientos hechos a la materia, y de los más propios del ámbito anglosajón que del pensamiento europeo continental. Entre sus precursores más representativos fue el canadiense MACKAAY, quien desde 1971 se pronuncia sobre el tema a través de varios escritos. Por ***jurimetría***, entiende a la aplicación de técnicas estadísticas y matemáticas que permiten verificar la regulación de ciertas hipótesis interesantes en el acontecer jurídico, resolver algunos problemas concretos e –incluso- elaborar a partir de dichos datos una cierta teoría del derecho. ***La Informática Jurídica*** para el autor consiste en el tratamiento lógico y automático de la información- en este caso jurídica- en tato soporte del conocimiento y la comunicación humana. Y el ***Derecho de la Informática*** lo entiende como el conjunto de problemas jurídicos producidos por la informática.

b) La Informática Jurídica como relación simétrica entre elaboración electrónica y derecho, basada en la necesidad social de información.

Es la tesis de STEINMULLER (1970), para quien la Informática Jurídica tiene un doble objeto: por un lado las aplicaciones de la computadora al derecho (informática jurídica propiamente dicha), y por otro lado los problemas jurídicos derivados del impacto de estas tecnologías en la sociedad y su consecuente reglamentación jurídica (derecho informático).

c) La informática Jurídica como teoría estructural del Derecho.

MARIO LOSANO y HEBERT FIEDLER, representantes de esta concepción. El propio TADDEI ELMI define y adhiere a esta posición al establecer 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".[64]

El estructuralismo, como se sabe ha tenido mucha fuerza a través de numerosas disciplinas, en ciertas épocas modernas. Uno de sus dominios ha sido la Lingüística, donde nociones tales como: sistemas, signos, significante y significado; han tenido desarrollos mayores que también ha aprovechado el derecho.

Bajo éstos presupuestos, MARIO LOSANO (1969) desarrollo una de las primeras aproximaciones representativas y bien conocidas de la Informática Jurídica que se llena de componentes derivados de la filosofía analítica del lenguaje, el estructuralismo y la lógica formal.

d) La informática y el Derecho se relacionan instrumental y sistemáticamente.

Según el francés CHOURAQUI (1974), 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 –aun mas- todo lo ligado a lo jurídico (social, económico, político.- informativo, gestionario – administrativo, etc).[65]

[64] Ob Cit. Bauzá Reilly Marcelo, Informática jurídica en una facultad de Derecho. Roles y Perspectivas. Pág.7
[65] Idem. Pág.8

Para este autor francés toma como puntos de referencia la actividad de los tres poderes del Estado (Parlamentario, Administración y Justicia), y la Universidad, esta en cuenta a la enseñanza y la investigación. Mismo que le asigna una gran importancia a la Informática Judicial, y confirma el rol notable de la Informática al servicio de la Universidad y la investigación científica.

Para el español PEREZ LUÑO en su reciente Manual de Informática y Derecho para retomar esta clara distinción entre el Derecho Informático e Informática Jurídica. La primera sostiene, es "una materia inequívocamente jurídica, conformada por el sector normativo de los sistemas jurídicos contemporáneos integrados por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de información y la comunicación, es decir, la informática y la telemática"[66] Eso por un lado. Y en cuento a la Informática Jurídica nos expresa que " tiene por objeto la aplicación de la tecnología de la información al Derecho". Como "disciplinas bifronte", ya que entre ellas se entrecruzan la metodología tecnológica con el objeto jurídico, lo cual condiciona las posibilidades o modalidades de su aplicación. Y termina haciendo la clásica distinción de las tres informáticas jurídicas: documental, decisional y de gestión.[67]

e) La informática Jurídica como soporte de la decisión jurídica adoptada bajo el principio de legalidad.

Es claro apreciar que el principio de legalidad, es de gran importancia para el derecho, ya que es el verdadero fundamento para un estado de derecho. Y bien, para el autor noruego BING, no está tan alejado el mantenimiento de este principio con el basamiento y justificación de la informática jurídica. El enunciado principio se apoya en elementos tales como la predecibilidad del sistema jurídico y sus decisiones, la objetividad de estas últimas, el principio de igualdad en cuento a sus destinatarios, y el factor tiempo relacionado con la calidad de la decisión judicial.

[66] Idem. Pág. 8
[67] Idem. Pág. 9

f) La 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. Este autor es contrario a atribuir competencia exclusiva a los cultores del derecho industrial, comercial, penal, constitucional, etc. Para el estudio de problemas tales como la naturaleza del computador y del programa de computación, sus respectivos funcionamientos, sus límites y posibilidades en cuento presupuestos para resolver problemas jurídicos.[68]

Por lo que el autor se aboca a distinguir la informática de la informática jurídica. Y expresa que la primera, es una especie de una disciplina más basta, cual resulta la electrónica. Mientras que la Informática Jurídica no pertenece ni a una ni a otra en totalidad, no que tiene un carácter interdisciplinario y transversal.

Por lo que podremos señalar en términos generales que la Informática Jurídica será "La técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimiento 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".[69]

De igual forma encontramos otras denominaciones con los que se conoce la Informática Jurídica.

- Computer and law (países anglosajones).
- Rechtsinformatique (en Alemania).
- Jurismática (México).
- Rechtcibernetik (países de Europa Oriental).

[68] Ob Cit. Bauzá Reilly Marcelo, Informatica jurídica en una facultad de Derecho. Roles y Perspectivas. Pág. 9.
[69] Ob. Cit. Téllez Valdés Julio, Derecho Informático. Pág. 26.

2.1.3. CLASIFICACIÓN DE LA INFORMÁTICA JURÍDICA.

En sus primeros años, la informática jurídica se presentó en los términos de una informática documentaría de carácter jurídico, es decir, la 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, contratos, promociones, mandatos judiciales, etcétera. Así nació a fines de los años setenta 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 documentaría.[70]

A lo anterior podemos clasificar a informática jurídica de la siguiente manera:

a) Informática Jurídica Documentaría.

El reciente desarrollo de los sistemas de documentación automatizada corresponde a una realidad sensible en relación a los campos del conocimiento, el creciente volumen documentario se ha dado de tal forma, 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. Siendo que los texto de la ley han dejado de ser generales, por ser mas detallados y de mayor cantidad, provocando con esto una labor de legislación más pronunciada en los últimos veinte años.

[70] Idem. Pág. 28.

Siendo que en los sistemas de la informática jurídica documentaría se trata de crear un banco de datos jurídicos, relativo a cualquiera de las fuentes del derecho, con excepción de la costumbre a efecto de consultarlo con base en criterios propios acordes a esa información y su relevancia jurídica.

La finalidad de la informatización en un sistema documentario cosiste en encontrar lo más rápido y pertinentemente posible la información que ha sido almacenada. El conjunto de esas informaciones constituye el banco de datos o corpus (la expresión "base de datos" es por momentos reservada a la designación e subconjuntos del corpus total).[71]

Por lo que la informática jurídica documental, esta constituida por bases de datos de información jurídica. Se centra en el análisis del documento jurídico y esta constituido por la aplicación de las técnicas documentales en el desarrollo de las técnicas informáticas.[72]

En términos generales, los modelos de estructuración de información mas comúnmente adoptados para el análisis documental de la información jurídica son:

1) Indización o Inmediación: Consiste en la elaboración de una lista rígida de descriptores a través de la calificación de la información contenida en el documento fuente, mediante el descriptor o descriptores que se consideran apropiados, se individualiza la información por medio de la designación de una o varias palabras o locuciones clave (descriptores) tomadas de una lista previamente elaborada de acuerdo al tipo de información de que se trate, este tipo de análisis es aplicado al control hemerográfico o bibliográfico.

[71] Ob. Cit. Téllez Valdés Julio, Derecho Informático, Pág.30
[72] Ob Cit. Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 12.

2) Full-Text: Este consiste en el almacenamiento del texto completo en la máquina computadora, con el fin de recuperar la información contenida en él por cualquiera de las materias a que haga referencia, algunos autores señalan que la aplicación de este método resulta inconveniente para la recuperación de la información.

3) Abstract: Es el documento cuya información, obtenida de un documento-fuente, es organizada en forma lógica a través del empleo de restrictores de distancia con el fin de lograr su recuperación así como su presentación sintética.[73]

b) Informática Jurídica de Control y Gestión.

Dentro de los aspectos mas importantes y de gran desarrollo, ha sido la informática jurídica de control y gestión, que abarca los ámbitos jurídico- administrativos, judicial, registral y despacho de abogados, fundamentalmente.

Esta rama de la informática jurídica 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.[74]

Esta área tiene como objeto 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.

[73] El sistema UNAM-JURE un banco de datos legislativos, Dirección General de Publicaciones, Universidad Nacional Autónoma de México, México, 1985 Págs. 33-42.
[74] Ob Cit. Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 13.

En la administración pública y habida cuenta que en la actualidad se presenta un crecimiento extraordinario en el volumen y complejidad de actividades en las dependencias gubernamentales debido, entre otras cosas, al pronunciado desarrollo demográfico, económico y tecnológico. Ello ha obligado a que dicho sector, en sus diferentes niveles (federal, estatal y municipal), esté capacitado para recibir, tramitar, analizar y difundir todo tipo de información jurídica para su correcto funcionamiento.[75]

Ya que mediante la adecuada aplicación de la informática jurídica de control y gestión se puede lograr un mejoramiento sustancial a la estructura jurídico- administrativo y de los sistemas de operación, medida indispensable para que las entidades del sector público, a través de los poderes Ejecutivo, Legislativo y Judicial alcancen sus objetivos sociales, apoyados de una tecnología moderna.

LÓPEZ- MUÑIZ, hace una división de ésta rama en:

1.- Informática Registral: Se ocupa de todos los tipos de registros, sean públicos o privados. Se trata de facilitar a los diferentes usuarios, datos fehacientes en todos los registros oficiales, con rapidez y facilidad de acceso, por ejemplo: los regístrales, civiles, penales etcétera., además permite, la facilidad de elaboración de estadísticas.

2.- Informática Operacional: Es la que trata de facilitar la actuación de las oficinas relacionadas con el Derecho, tanto en el ámbito público, como en el ámbito privado en los que va a permitir que la máquina lleve toda la actuación repetitiva, el control de asuntos, como en el ámbito privado, bufetes, notarias, etcétera (realización de machotes).[76]

[75] Ob Cit. Téllez Valdés Julio, Derecho Informático Pág. 41.
[76] López- Muñiz Goñi, Miguel., Informática Jurídica documental, Edit. Díaz de Santos, S.A. Madrid, España, 1984, pág.10. Según cita de Riestra Gaytán Emma, Pág. 14.

c) Informática Jurídica Metadocumentaria.

Este es otro tipo de aplicación de la informática jurídica, que va mas haya de la esencia de los fines documentarios, ya que sus ámbitos de injerencia son: la ayuda en la decisión, ayuda en la educación, ayuda en la investigación, ayuda en la previsión y finalmente ayuda en la redacción.

Señalaremos que en la actividad de los diversos juristas, la búsqueda del conocimiento jurídico está orientada a resolver cuestiones con consecuencias en la vida política. La informática jurídica ha comenzado a ocuparse en el campo de las decisiones.

La cantidad de variables que se requiere para tomar las más mínimas decisión hace pensar sobre el carácter limitado que tiene la "decisión automática".

Nadie pretende saber exactamente las razones que están detrás de una decisión, sino sólo materializar y sistematizar aquellas "buenas razones" que transforman un juicio jurídico en un juicio objetivo: por un lado, la kantiana "universalización" y por otro lado la fundamentación en una norma vigente.[77]

La teoría de la decisión (ya desarrollada en otros campos de las ciencias sociales, como la económica y la ciencia política) es prácticamente desconocida en la teoría del derecho.[78] Las ventajas que reportaría en el campo jurídico en caso de una adecuada aplicación sería la estructuración del conocimiento y la existencia de una teoría general.

[77] Ob. Cit. Téllez Valdés Julio. Derecho Informático. Pág. 45.
[78] R. Guibourg, An Automated Decision- Marking System y de C. Ciampi, Artificila Inteligence and Legal Information Systems, North Holland, Amsterdam, 1982. Según señala Téllez Valdés Julio. Derecho Informático. Pág. 46.

Como lo señalamos en él capitulo anterior la rama de la informática que se ocupa de estos temas es la Inteligencia Artificial, ya que a través de los sistemas expertos que son una herramienta que a partir de cierta información prevista por un asesor, permite resolver problemas en un dominio específico, mediante la simulación de los razonamientos que los expertos del sistema harían utilizando los conocimientos adquiridos.

"Decidir es elegir entre dos o más medidas (o acciones) optativas con base en información con objeto de alcanzar resultados y objetivos previamente establecidos" "Herbert Simón (pionero especialista en la rama del conocimiento de inteligencia artificial, eph) menciona la existencia de dos tipos de decisiones: las programables y las no programables, las primeras, de carácter rutinario y repetitivo, y las segundas, como aquellas que invocan a la intuición y al sentido común."[79]

2.2. ANTECEDENTES Y ASPECTOS GENERALES DEL DERECHO INFORMÁTICO.

No obstante de lo anterior, podemos señalar 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.

Derecho informático o derecho de la informática es una materia inequívocamente jurídica, conformada por el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y comunicación, es decir de la informática y la telemática.[80]

---

[79] Pelaéz Hernández Eduardo, Memorias del Foro de Consulta sobre Derecho e Informática, Ponencia "Algunas consideraciones sobre la reglamentación del Derecho a la Información mencionado en el artículo 6° Constitucional", Monterrey, Nuevo León, Septiembre de 1996. Aviso Legal 1999. Cámara de Diputados del H. Congreso de la Unión (www. Yahoo.com) Pág. 5.

[80] Ob. Cit. Perez Luño Antonio Enrique. Manuel de informática y derecho. Pág. 18 Según señala el autor Lara Márquez Jaime. Derecho y Tecnología. Una visión prospectiva del Derecho. Pág. 3

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.[81]

El Derecho de la informática, es el conjunto de normas reguladoras del objeto informático o de problemas directamente relacionadas con la misma.[82]

Así planteada las cosas, el Derecho Informático no es sino un área mas del derecho, que puede ser abordado desde las tradicionales perspectivas del análisis jurídico, como el análisis exegénetico o el dogmático, en cuanto estos son suficientes para efectuar el análisis de la normatividad que regula los productos tecnológicos, frente a lo cual, todo fenómeno tecnológico y particularmente el fenómeno informático, no es sino un objeto de interés mediato, en tanto representa un elemento de posible interferencia intersubjetiva.[83]

Así pues, desde los primeros esfuerzos hasta los más recientes, todos los trabajos dedicados al área del Derecho Informático, han estado orientados a propiciar la regulación jurídica de los productos informáticos, así constantemente se ha reclamado la regulación jurídica de todos aquellos contratos que tienen por objeto bienes y servicios informáticos a los que se ha denominado "contratos informáticos"[84] a fin de que dejen de ser contratos atípicos y se configuren en contratos típicos, perspectiva que se ha visto reforzada por el estudio de los contratos en cuanto la voluntad contractual se configura haciendo uso de medios informáticos;[85]así mismo, se ha reclamado la configuración de

---

[81] Ob Cit. Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano. Pág. 16.

[82] Suñé Llinás, Emilio. Introducción a la Informática Jurídica y al Derecho de la Informática. Revista de la Facultad de Derecho de la Universidad Complutense. Informática y Derecho Monográfico 12. Madrid. España. septiembre de 1986. Pág. 77. Según cita de Riestra Gaytán Emma. Pág. 12.

[83] Ob. Cit. Lara Márquez Jaime. Pág. 3

[84] De Lamberterie Isabelle. Contratos informáticos. En: Altamark Dabiel. Informaticay derecho. Aportes de doctrina Internacional. Buenos Aires. Deplama. 1993. Tomo4. Pág.1-32 Según señala el autor Lara Márquez Jaime. Pág. 3.

[85] Castillo Freyre Mario. Las Doctrinas tradicionaels frente a la contratación computahzada. Lama Fondo Editorial de la Pontificia Universidad Católica del Perú 1996. 4 tomos. Según señala el autor Lara Márquez Jaime. Derecho y Tecnología. Una visión prospectiva del Derecho. Pág. 3.

un nuevo tipo de responsabilidad civil denominada "responsabilidad informática"[86] que resuelva los problemas derivados del denominado "daño informático"; lo mismo se puede decir respecto de las exigencias por penalizar conductas antisociales cometidas usando recursos informáticos.[87]

Esa preocupación por proporcionar la regulación jurídica de cuanto instrumento nuevo aparezca, es explicable desde que el Derecho Informático tiene por objeto, el análisis de la normatividad jurídica que regula los bienes informáticos desde una perspectiva tradicional y eminentemente jurídica; toda vez que, esta perspectiva sin una normatividad positiva y específica tiene poco o nada de decir al respecto, y lo peor aún, cada vez que ha reclamado regulación, lo ha hecho pidiendo limitación, prohibición, sanción, antes que mecanismos jurídicos que lo desarrollen, lo viabilicen, lo promocionen o lo hagan posible, lo cual por lo demás es altamente sintomático de su incongruencia con el actual desarrollo tecnológico.[88]

Que contradictorio es el saber que muchos de los precursores informáticos nunca se imaginaron los alcances que llegaría a tener las computadoras en una sociedad llena de tecnología, o aun más en el área jurídica, como reguladora de la informática.

Como podemos ver a finales de los años setenta 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.

---

[86] Fernández Cruz Gastón. La responsabilidad civil del gestor de bases de datos en la informática jurídica. En: Ius Et Veritas N° 15, Lima Facultad de Derecho de la Pontifica Universidad Católica del Perú, pág. 259-283. Según cita el autor Lara Márquez Jaime. Pág. 3.

[87] Bramont Arias Torres Luis Alberto. El delito Informático en el Código Penal Peruano. Lima Fondo Editorial de la Pontificia Universidad Católica del Perú, 1996. Según cita el autor Lara Márquez Jaime. Pág. 3.

[88] Idem pág. 4.

Por lo que podemos ver que el Derecho de la Informática es un instrumento regulador en la sociedad. Que lo podemos conceptualizar como el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática.[89]

Si profundizamos mas sobre este concepto podremos decir que es un conjunto de ***leyes*** en cuanto que, si bien escasos, existen varios ordenamientos jurídicos nacionales e internacionales que hacen alusión específica al fenómeno informático. ***Norma*** en virtud de aquellas que integran la llamada política informática, Principios en función de aquellos postulados emitidos por jueces, magistrados, tratadistas y estudiosos del tema. Siendo ***hechos***, como resultado de un fenómeno aparejado a la informática, es decir, no imputables a los hombres. Y por ultimo, ***actos***, como resultado de un fenómeno directamente vinculado a la informática y provocado por el hombre.

El Derecho Informático en tanto conjunto de normas que regulan el fenómeno informático, como el análisis de las mismas y el razonamiento involucrado en dicho proceso, se mantiene incólume no obstante la novedad de la tecnología, pues regula el fenómeno informático, de la misma manera como siempre ha regulado los bienes patrimoniales, los derechos fundamentales, las sanciones civiles, administrativas y penales, etc.; es decir, gracias a esta perspectiva teórica, el derecho no sufre ninguna transformación fundamental por el embate de las nuevas tecnologías y por el contrario ve asegurada su asepsia y su pureza.[90]

Tenemos por otro lado que a la legislación informática como el conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso (fundamentalmente inadecuado) de la informática, como la reglamentación de puntos específicos.[91]

---

[89] Ob. Cit. Téllez Valdés Julio. Derecho Informático. Pág. 58.
[90] Ob. Cit. Lara Márquez Jaime. Derecho y Tecnología . Una visión prospectiva del Derecho. Pág. 5.
[91] Ob. Cit. Téllez Valdes Julio. Derecho Informático. Pág. 59.

Esta reglamentación contempla los siguientes aspectos:

a) Regulación de los bienes informacionales. Ya que la información como producto informático requiere de un tratamiento jurídico en función de su innegable carácter económico.

b) Protección de datos personales. Es decir, el atentado a los derechos fundamentales de las personas provocado por el manejo inapropiado de informaciones nominativas.

c) Flujo de datos transfronterizos. Con el favorecimiento o restricción en la circulación de datos a través de las fronteras nacionales.

d) Protección de Programas. Como resolución a los problemas provocados por la llamada "piratería" o robo de programas de computo.

e) Delitos Informáticos. Como la comisión de verdaderos actos ilícitos en los que se tengan a las computadoras como instrumento o fin.

f) Contratos informáticos. En función de esta categoría contractual sui generis con evidentes repercusiones fundamentales económicas.

g) Ergonomía informática. Como aquellos problemas laborales suscitados por la informatización de actividades.

h) Valor probatorio de los soportes modernos de información, provocado por la dificultad en la aceptación y apreciación de elementos de prueba derivados de estos soportes entre los órganos jurisdiccionales.

De todo lo anterior podemos señalar la gran importancia que han traído consigo las materias de informática jurídica y derecho informático a nivel internacional relacionados con el derecho en nuestro país, materias que hoy en día se hace necesarias incluirlas en un plan de estudio universitario y de especialización, con la finalidad de tener la formación y conocimientos necesarios, y afrontar con esto los cambios tecnológicos que requiere la sociedad, así como contar con los medios jurídicos que regulen todo acto o hecho relacionado con la informática o medios de información electrónica.

Respecto a la importancia que viste en la actualidad el que esta materia- la informática jurídica y el derecho informático- se incluya en el ámbito universitario, específicamente en las Facultades de Derecho, tanto a nivel nacional como internacional.[92]

En razón a ello, el " Comité de Ministros del Consejo de Europa", recomendó a los Estados la enseñanza, la investigación y formación en materia de "informática y derecho", y que por su "creciente importancia", debe desarrollarse su enseñanza en el nivel universitario.[93]

Dentro de la evolución que ha tenido en los últimos años la materia, podemos establecer claramente tendencias a nivel internacional, que se tienen en los distintos países del mundo, respecto del desarrollo de la informática y el derecho de esta manera podemos enumerar las siguientes tendencias, las cuales cuentan – cada una de ellas --, con sus características particulares, así tenemos: inicial o básica, progresiva o creciente, avanzada o próspera y culminante o innovadora.[94]

---

[92] Correa Carlos M. Y Otros. Derecho Informático. Edic. Depalma, Buenos Aires, Argentina. 1987, Pág. VIII. Según cita el autor Cantú Aguillén Ricardo. Miembro del Comité Académico del Instituto de la Judicatura del Estado de Nuevo León. Miembro adscrito del Instituto de Investigaciones Jurídicas de la facultad de Derecho y Ciencias Sociales de la U.A.N.L. (México) en su artículo "Tendencias actuales de la Informática y el Derecho a Nivel Internacinal". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www.yahoo.com). Pág. 1.

[93] Ob Cit. Cantú Aguillén Ricardo. Tendencias actuales de la Informática y el Derecho a Nivel Internacinal. Derecho Org. Pág. 1.

[94] Idem. Pág. 2.

a) Tendencia Inicial o Básica. 1) Poco avance y desarrollo de la informática jurídica y del derecho informático, debido a la escasa importancia dada a la materia por los profesores de derecho de las Universidades y también por los funcionarios del Gobiemo. 2) Se empieza a promover que se incluya la materia de informática jurídica en los planes de estudio de las facultades de derecho, desarrollo inicial de la doctrina nacional (se estudia al derecho informático, dentro de la informática jurídica).

b) Tendencia Creciente o Progresiva: 1) Distinción clara entre informática jurídica y derecho informático, como ramas totalmente independientes una de la otra, pero relacionadas entre sí; se empieza a desarrollar en firme, la doctrina nacional al respecto. 2) Consideración del derecho informático como rama autónoma del derecho; incluyéndose en los planes de estudio de las principales facultades de derecho del país, de manera separada a la materia de informática jurídica; en Europa se recomienda aglutinar a ambas materias bajo la concepción "informática y derecho", en virtud de considerar más completa esta definición.

c) Tendencia Avanzada o Próspera: 1) Destaca la necesidad e importancia de desarrollar la labor legislativa respecto al derecho informático, normas específicas que regulen su aplicación; auge importante respecto a al doctrina y jurisprudencia al respecto (Ej. Delitos informáticos no tipificados en los códigos penales, etc.). 2) Desarrollo y consolidación importante de la legislación, doctrina y jurisprudencia nacional del derecho informático; controversia de casos prácticos nacionales e internacionales en la Corte Suprema del país.

d) Tendencia Culminante o Innovadora: 1) Avances importantes en respecto de la informática jurídica metadocumental, auge de centros de investigación para la utilización de sistemas de inteligencia artificial aplicados al derecho, desarrollo de tesis doctórales relativas a la inteligencia artificial y el derecho. 2) Desarrollo de proyectos prácticos y específicos de utilización de la inteligencia artificial aplicados al derecho.

2.2.1. REGULACIÓN JURÍDICA DE LA INFORMACIÓN.

Se ha enfatizado mucho en la idea de la "Sociedad de la información" como el actual estado de nuestra civilización contemporánea. Los rápidos y constantes cambios tecnológicos nos han llevado a "un nuevo tiempo, un nuevo espacio y un nuevo hombre".[95]

Hoy en día la humanidad, se encuentra inmersa en un cambio de paradigma, las formas tradicionales de obtener información, publicar bienes, realizar transacciones, han sido resquebrajadas y superadas por el uso de medios tecnológicos que antes no existían. En consecuencia el uso de tecnologías de la información no es tan traumante para el común de las personas, como lo es para el mundo del derecho.[96]

El Derecho tiene que tener las respuestas adecuadas para facilitar la transición del medio físico al mundo virtual, de lo contrario la convivencia social en Internet sería una suerte de anarquía que puede llevar a su propio aniquilamiento. El reto del Derecho es, pues, flexibilizar sus instituciones e incorporar aquellas normas surgidas dentro del internet para que todos los actos jurídicos que se den dentro del mundo virtual tengan idénticas consecuencias en el mundo físico, y que además, cualquier relación jurídica que se desplace entre ambos espacios tenga los mismos efectos legales.[97]

---

[95] En la reciente conferencia de Michel Sarres de la Sorbonne, dictada en la Facultad de Derecho de la Universidad de la República Montevideo- Uruguay. (Públicado en Libro de Ponencias, XI Congreso Latinoamericano y III Iberoamericano de Derecho Penal y Criminología, Fundación de Cultura Universitaria, septiembre de 1999. Fígoli Pacheco Andrés J. El Acceso No Autorizado a Sistemas Informáticos. (internet InfoJur.ccj. ufsc.br) Pág. 1

[96] Calderón Rodriguez Cristian L. Abogado. Miembro del Cibertribunal Peruano.Especialista en Comercio Exterior. Miembro del Instituto Peruano de Comerio Electrónico. Conciliador del Centro de Conciliación de la Pontificia Universidad Católica del Perú. "El Impacto de la Era Digital en el Derecho". Perú 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www.yahoo.com). Págs. 1 y 2.

[97] Idem. Pág. 2.

A raíz de la gran trascendencia que ha adquirido en este siglo la información, cabe resaltar que autores como R. HARTLEY destacaban la utilidad de la información a tal grado de mencionar que la información puede modificarse en función de su utilidad (medida Hartley) y que por lo tanto "la cantidad de información será proporcionada al número de alternativas que se dispongan en un momento dado.[98]

Se señala que el "poder de la información" es una de la exigencia del mundo actual, sediento siempre de noticias. La información es hoy una necesidad vital. El hombre moderno, y particularmente el hombre culto, siente la imperiosa necesidad de conocer los acontecimientos de toda índole que se producen en el mundo en que vive. La información se configura hoy como una de las bases de la sociedad reconocida y regulada en todo el mundo civilizado.[99]

Por ello podemos decir que la comunicación es la base de la educación, la ciencia, el arte y la cultura. Sin ella no puede haber tampoco cooperación ni entre individuos no entre grupos no entre naciones.[100]

Por lo que podemos señalar que la palabra información, viene del latín in-formare, poner en forma, en general, el contenido de un conjunto de DATOS presentados en formato útil para apoyar el logro de resultados y objetivos previamente establecidos constituye información. La información tiene como elemento al DATO, el DATO es la referencia a un HECHO. "La información ha sido considerada como un elemento susceptible de ser transmitido (COMUNICADO, eph) mediante una combinación de SÍMBOLOS". [101]

---

[98] Dicho postulado conocido como la teoría de la medida de la información fue mencionada por Hartley en su obra Transmisión de información escrita en 1928. Según cita Téllez Valdés Julio. Derecho Informático. Pág. 63.

[99] Romero Coloma Aurelía María. Derecho a la Información y Libertad de Expresión, Especial consideración al proceso penal. Edit. Bosh, Casa Editorial, S.A. 1984. Barcelo España. Págs. 27 y 28.

[100] Novoa Monreal Eduardo. Derecho a la Vida Provada y Libertad de Información, un conflico de Derecho. Edt. XXI Siglo Veintiuno Editores, S.A. México, Espeña, Argentina, colombia. 1981. Pág. 138.

[101] Téllez Valdéz Julio. Derecho Informático, UNAM. 1991. Págs 42, 43, 45 y 49.

La información se concibe como un VALOR AGREGADO que el USUARIO (o RECEPTOR) de la misma pudiera lograr a partir del CONTENIDO en una situación "Cualitativamente, la información es la medida de disminución de incertidumbre (desconocimiento) del sujeto respecto a los objetos.." relevantes en un entorno de acuerdo a su actividad y objetos. Las CARACTERÍSTICAS que le dan VALOR a la información son: a) clara e inteligible, respecto a forma, b) relevante, respecto a contenido, c) completa, respecto a contenido, d) oportuna, respecto a contenido, y elaboración, e) confiable, respecto a contenido y elaboración.[102]

Por lo que "Todo individuo tiene derecho a comunicarse. La comunicación es una necesidad humana básica, fundamento de toda organización social. El derecho a la comunicación pertenece a los individuos y a las comunidades, en las relaciones entre los primeros, entre los segundos y entre aquéllos y éstas. Este derecho ha sido reconocido internacionalmente desde hace mucho tiempo y es necesario que su ejercicio evolucione y se amplíe constantemente. Habida cuenta de los cambios sociales y de todos los adelantos de la tecnología, deberán ponerse a disposición de toda la humanidad unos recursos humanos, económicos y tecnológicos apropiados para satisfacer la necesidad de una participación activa en la comunicación y para aplicarse a ese derecho. [103]

"La Información posee una connotación vinculada a una de nuestras más grandes libertades: la opinión y expresión de informaciones e IDEAS por cualquier medio..." [104]
En estos términos, la informática y la información están vinculados de manera estrecha por esta "omnipresencia" de las computadoras en el proceso propio de nuestra vida cotidiana, con implicaciones aún más trascendentes de las estrictamente técnicas.[105]

---

[102] Ob. Cit. Pelaéz Hernández Eduardo, Memorias del Foro de Consulta sobre Derecho e Informática, Pág. 5

[103] Exposición de un grupo pluricultural de trabajo del Instituto Internacional de Radiotelevisión, durante su conferencia de 1975.. Citada en el informe de UNESCO, 19 c/93, de 16 de agosto de 1976, núm. 21. Según cita el autor Novoa Monreal Eduardo. Derecho a la Vida Provada y Libertad de Información. Pág. 139.

[104] Ob. Cit. Pelaéz Hernández Eduardo, Memorias del Foro de Consulta sobre Derecho e Informática, Pág. 5.

[105] Chamoux, Jean- Pierre, "L information sans frontiére", Information et Societé. Núm 8 Doc. Francaise, Paris, 1980. Según cita Téllez Valdés Julio. Derecho Informático. Pág. 64.

Por lo que el derecho a la información comprende un conjunto de tres facultades vinculadas entre sí, como lo son: difundir, investigar y recibir información; todas ellas agrupadas en dos vertientes fundamentales como lo son el deber de informar y el derecho a ser informado.[106]

a) El deber de informar.

Esta comprende las facultades de difundir e investigar, vendría a ser la fórmula moderna de la libertad de expresión, porque dicha libertad no es suficiente para referir la complejidad del proceso informativo, ni sus mecanismos de protección son suficientes para asegurar en las sociedades modernas la existencia de una comunicación libre y democrática.[107]

b) El derecho a ser informado.

Este se refiere básicamente al derecho de los individuos y grupos sociales a estar informados de los sucesos públicos y, en general, de todas las informaciones que pudieran afectar su existencia; todo ello para lograr que el individuo oriente su acción y participe en la vida política de su comunidad.[108]

Cabe considerar que precisamente el sentido del derecho a ser informado implica, desde el punto de vista del receptor, un abandono de esa actitud pasiva al tener la posibilidad jurídica de exigirla al sujeto obligado la cumplimentación del mencionado derecho.[109]

---

[106] Idem. Pág. 66.
[107] López Ayllón Sergio, Derecho a la información, México, Edt. Porrúa 1984. Pág.160.
[108] Ob. Cit. Téllez Valdés Julio. Derecho informático. Pág. 67.
[109] Ob. Cit. López Ayllón Sergio. Derecho a la Información Pág. 161.

Por lo que podemos ver que la información: Es un bien que no se agota con el consumo si no que se enriquece con el uso, y ello permite que su expansión se esté produciendo con la creación de más información provocada en gran medida por el desarrollo de las Tecnologías de la Comunicación y la información.[110]

La información, entendida como un conjunto de datos que esta respaldada en un soporte sistemático-informático y que tiene la característica de estar liberalizada en un flujo de comunicación.[111]

No es ajeno el fenómeno de las nuevas tecnologías de las información y de la comunicación en la llamada sociedad de la información misma que define FERNÁNDEZ como el tipo de sociedad que está surgiendo de la profunda transformación a la que dan lugar las nuevas tecnologías. La sociedad de la información se basa en el uso generalizado de información de bajo costo, el almacenaje de datos y las tecnologías de la transmisión. La generalización del uso de la información y del uso de datos se suma a cambios organizativos comerciales, sociales que cambiaran profundamente la vida tanto en le mundo del trabajo como en la sociedad en general.[112]

Finalizaremos en decir que el tiempo nos ha alcanzado con tantos avances y novedades tecnológicas, que para el día de hoy, nos obliga a tener que actualizar nuestros conocimientos y aportar elementos objetivos que sirvan a nuestros ordenamientos jurídicos, como medios necesarios para la regulación jurídica del bien-información, como un producto informático de una cultura consciente.

---

[110] Davara Rodriguez Miguel Angel. Manual de Derecho Informático, Edit. Aranzadi, 1999. Según Cita Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positovo Mexicano, Pág. 1.

[111] Ob. Cit. Riestra Gaytán Emma. Pág. 1.

[112] Fernández Esteban, Ma. Luisa, Nuevas Tecnologías, Internet y Derechos Fundamentales, Edit. Mc GraW Hill, Monografía Ciencias Jurídicas, Madrid, España, 1998, p'g. XXI. Según Cita de Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positovo Mexicano, Pág. 2.

2.2.2. PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES.

Como hemos visto 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 a 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 en manos particulares, crea diversos riesgos que pueden suponer una amenaza de agresión a la intimidad de los gobernados o de los usuarios del servicio. El riesgo 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 al revés.[113]

No es hasta la década de los setenta cuando comienzan a surgir numerosos archivos con informaciones de tipo personal, con un conjunto mínimo de datos como filiación, fecha y lugar de nacimiento, domicilio, estado civil, etcétera, hasta otro tipo de datos con caracteres aún más distintivos como raza, religión, inclinaciones políticas, ingresos, cuentas bancarias, historia clínica, etcétera. Dicho dato al ser recopilado en diferentes centros de acopio, como lo son los registros censales, civiles, parroquiales, médicos, académicos, deportivos, culturales, administrativos, fiscales, bancarios, laborales etcétera, ya no por medios exclusivamente manuales, sino con el apoyo de medios automatizados, provocan una gran concentración, sistematización y disponibilidad instantánea de ese tipo de información para diferentes fines.[114]

---

[113] Méjan C. Luis Manuel. El Derecho a la Intimidad y la Informática, Segunda Edición, Edit. Porrúa México, 1996. Pág.XIV.

[114] Ob. Cit. Téllez Valdés Julio, Derecho Informático. Pág.69.

Siendo considerable y de gran inquietud que este tipo de datos pueden ser vulnerables, ya que la destinación que puedan ser objeto, pudiendo ser variada, como la información que es empleada para fines publicitarios, comerciales, fiscales, policíacos etcétera, convirtiéndose en un instrumento de opresión y mercantilismo.

Pero también provoca que las personas corran un gran riesgo sobre dicho datos, ya que los mismos pueden ser utilizados para otras finalidades, alterando con esto los derecho fundamentales de los individuos en la sociedad, provocando discriminaciones, manipulaciones, persecuciones, presiones, asedios, etcétera. Quedando al margen de un adecuado control jurídico de dicha información.

Ya desde 1968, en el seno de la Asamblea de los Derechos Humanos auspiciada por la ONU, se mostraba una honda preocupación por la manera en que la ciencia y la tecnología podrían alterar los derechos de los individuos, empezando a detonar la necesaria emanación de un régimen jurídico que pudiera afrontar de manera cabal este género de situaciones.[115]

La expresión protección de datos personales es entendida como la protección jurídica de las personas en lo que concierne al tratamiento automatizado de su datos personales, o expresando en su forma más extensa, el amparo debido de 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. [116]

Ahora bien, la información de carácter personal o información nominativa, está definida en 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,[117] como toda información concerniente a la persona física identificada o identificable.

[115] Idem. Pág. 70.
[116] Davara Rodríguez Miguel Angel., Op Cit. Pág. 18.
[117] Firmado en Estramburo el 28 de enero de 1981.

También existen tres documentos claves en los que debe basarse cualquier regulación relativa a la protección de los datos de carácter personal a saber:

a) El convenio del Consejo de Europa del 28 de enero de 1981 para la protección de las personas con relación a los datos de carácter personal; ratificado por España el 27 de enero de 1984.

b) El acuerdo de Schegen de 14 de junio de 1985 relativo a la supresión gradual de los controles entre las fronteras comunes.

c) La propuesta de Directiva del Consejo de la Comunidad Económica Europea del 24 de septiembre de 1990 relativa a la protección de las personas en lo referente al tratamiento de datos personales (modificada el 15 de octubre de 1992).[118]

MUÑOZ nos explica que las legislaciones que han consagrado la protección sobre el uso y gestión de la información personal, destacan las siguientes características:

1.- El derecho a la autodeterminación informativa: 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 trasmitirlos por los medios informáticos, también denominado "libertad informática". Este derecho toma diversas vertientes de aplicación práctica:

a) Derecho de la información. En el sentido de tener el individuo la posibilidad de conocer la existencia de algún bando de datos o fichero de información personal;

[118] Del Peso Navarro, Emilio y Ramos González, Miguel Angel., Confidencialidad y Seguridad de la Información: la LORTAD y sus implicaciones Socioeconómicas., Edt. Díaz de Santos, S.A., Madrid ., España, 1994. Pág. 69. Según cita de Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 18.

b) 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, almacenamiento de información personal;

c) Derecho de actualización. Gracias al cual, el individuo puede exigir la corrección de ciertos datos;

d) Derecho de confidencialidad. Derecho que concede al sujeto la exigencia a que la información que proporciona permanezca ajena al conocimiento de terceros;

e) Derecho de exclusión. Por la naturaleza de la información puede el individuo cancelar, borrar o solicitar la destrucción de información denominada como sensible.[119]

Completando el anterior análisis, 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 su datos de carácter personal que ofrezca un perfil suyo obtenido de esta forma, y también, por último, del derecho del 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.[120]

Continuando con MUÑOZ que nos indica que dentro de la protección de datos encontramos la ***información sensible***. Para este tipo de información, dice la disposición europea "es la información de carácter personal, relevante al origen racial, opiniones públicas, las convicciones religiosas, así como los datos de carácter personal relativas a la salud o a la vida sexual, no pueden ser tratados automáticamente a menos que el

[119] Muñoz de Alba, Marcia., Manejo de la Información Vs. Vida Privada., en Núcleo de Estudios Interdisciplinarios en Salud y Derechos Humanos, reunión 16-I-95, Instituto de Investigaciones Jurídicas, Universidad Autónoma de México, México, 1995, Págs 5 y ss.

[120] Davara Rodríguez, Miguel Angel., La Protección de datos en Europa., Op Cit. Pág. 25. Según cita de Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 19.

Derecho interno prevea las garantías determinadas. En el mismo sentido se encuentra la información de tipo personal concerniente a las infracciones penales.

Por el contenido de la información sensible los riesgos y daños potenciales por su difusión producen un impacto mayor en la intimidad y dignidad de la persona. Tomando entonces tres vías fundamentales:

a) La información relativa a las creencias religiosa, política o sindicales;

b) Información relativa al origen racial, de salud y preferencias sexuales;

c) Información relativa a los antecedentes penales o infracciones administrativas.[121]

Así la clasificación de los datos nominativos constituye objeto del reconocimiento del derecho a la autodeterminación informativa.

Nos mencionada JOVER Y CABRERA, que el derecho a la autodeterminación informativa es un derecho de acertada denominación jurisprudencial (procedente del Tribunal Constitucional Alemán) vinculado al right of privacy de Warren y Brandeis, y que en la década de los setenta fue utilizado en el ámbito jurídico angloamericano, pero en una acepción diferente a la original: derecho que todo individuo tiene a decir qué información de su vida personal puede ser difundida o decirse si puede o no difundirse. Constituye esta aceptación una modalidad de la noción de "facultad de disposición" sobre los principios datos y concuerda con la que el Tribunal Constitucional Alemán formularía con la expresión de "autodeterminación sobre la información" como emanación del derecho a la persona.[122]

Por lo que dicha problemática ha sido de gran trascendencia a nivel internacional, al regular las variadas figuras de índole jurídico.

---

[121] Muñoz de Alba, Marcia., Op y Pág. Cit. Según señala Riestra Gaytán Emma, Pág. 20.
[122] Jover Pedro, Jose y Cabrera Vilaplana, Silvia, Op. Cit. Pág. 75 Según Cita de Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 12.

Así tenemos que las figuras tales como los derechos humanos, derechos personales, derecho 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 aun las garantías individuales y sociales como pudiera ser el caso en 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.[123]

La intimidad es el conjunto de circunstancias, cosas, expresiones, sentimiento 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 por la develación sea lícita.[124]

Por lo que señalaremos que el Derecho a la Intimidad o Privacía, 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 de terceros o para el bienestar común.[125]

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, y muy especialmente, el Estado, a fin de que se realice el 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 derecho y obligaciones.[126]

---

[123] Ob. Cit. Téllez Valdes Julio, Derecho Informático. Pág. 70.
[124] Méjan C. Luis Manuel. El Derecho a la Intimidad y la Informática,. Pág. 87.
[125] Idem. Pág. 105.
[126] Idem. Pág. 106.

2.2.3. FLUJO DE DATOS TRANSFRONTERIZOS.

Este es otro de los problemas que se ven reflejados en la actualidad en relación a la tecnología y comunicación que se maneja a nivel internacional y que es de suma preocupación en relación a la gran trascendencia que trae consigo.

Según el Consejo de Económico de la Organización de las Naciones Unidas (ONU), el Flujo de Datos Transfronterizos es " la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y repercusión.[127]

Este problema ha sido considerado desde el punto de vista de la limitación o favorecimiento de la circulación de datos a través de las fronteras nacionales, dependiendo de los aspectos positivos o negativos que esto pueda traer aparejado con los diversos países. Problema que 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.

Es evidente que en nuestros días. Los avances tecnológicos han proyectado sociedades aisladas, poniéndolas en contacto con la modernidad. 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. Los resultados son una nueva realidad comercial es la emergencia de mercados globales para consumidores de productos estandarizados en una escala previamente inimaginable. RAVI KALAKOTA.[128]

[127] Ob. Cit. Téllez Valdes Julio. Derecho Informático. Pág.77.

[128] Perez Marayo Guillermo Augusto. Abogado y Notario. Universidad Complutense de Madrid. Asesor Parlamentario, especialista en Investigación de Información en el Internet, "Instrumentos de Pago Internacional. Tecnología Informática y Comercio Electronico". (Costa Rica) Derecho, Tecnología y Cambio. 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), (www.yahoo.com). Pág. 1.

Hasta hace un tiempo, el cambio era lento y pausado, pero con la introducción de las más complejas herramientas generadas por la humanidad a saber, la computadora (la nueva imprenta multimedia) y la red (las nuevas rutas comerciales), el cambio se revolucionó. A partir de la Segunda Guerra Mundial, el modelo industrial se comienza a resquebrajar ante nuestros ojos, poniendo en crisis los conceptos institucionales, organizacionales y las relaciones de poder, heredados desde tiempos inmemoriales. Actualmente los gobiernos son tachados de ineficientes; es común el sentir de que el sistema no responde a la realidad de nuestros tiempos.[129]

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, comunicamos y, en general, nuestra forma de vida. Vivimos en una era que no ha tenido un nombre específico "la Post-Guerra", la era atómica, la era cibernética e informática pero llámese como se llame, no cabe duda de que estamos en la Era Post- Industrial, en donde la nueva ciencia, la tecnología informática, genera constantemente herramientas digitales paradigmáticas de aceptación universal, que transforman la comunidad humana.[130]

En las economías post-industriales en donde el manejo de la información representa hoy en día entre el 40 y 50 % del valor agregado, es natural que los intercambios internacionales de información se destinen a formar un papel importante. Con base a ello se sustenta en buena medida el funcionamiento de la economía mundial en donde la especialización e interdependencia de los Estados se acentúa más. Sin embargo el desplazamiento rápido y las preocupaciones de los derechos del hombre hacia la soberanía nacional, así como las incidencias económicas y sociales de intercambios inmateriales entre las naciones, trae consigo implicaciones positivas como negativas, y que al respecto nos señala JULIO TÉLLEZ VALDES.

[129] Idem. Pág. 2.
[130] Idem. Pág. 3.

Es considerable ver que el Flujo de Datos Transfronterizos aporta beneficios a las colectividades nacionales como:

- **Favorecimiento de la paz y la democracia**. No podríamos dejar de recordar los vínculos estrechos existentes entre libertad de circulación de información, derechos del hombre y valores fundamentales de la humanidad. Libre comunicación de mensajes y de opiniones es esencial para la democracia y la paz mundial.

- **Favorecimiento en el progreso técnico y crecimiento**. La cooperación entre los científicos que constituyen una comunidad a escala mundial y la competencia de industriales y empresarios han hecho gala de su aptitud difundiendo los conocimientos y técnicas.

- **Finalmente, no podemos olvidar que la interdependencia económica de las naciones es hoy en día una realidad irreversible**. A raíz de la internacionalización de compañías y la especialización de actividades nacionales, toda restricción súbita y deliberada a la continuidad del flujo de datos, tal como existen hasta ahora, podría asimilarse a una especie de acta de guerra económica a la par de un bloqueo o embargo. Es imposible concebir hoy en día a algún país que goce de una independencia total en el plano económico.[131]

Del otro lado de la microelectrónica y el progreso de las telecomunicaciones, trae consigo una serie de riesgos, de los que se podrían distinguir, los siguientes:

- **La vulnerabilidad social**, esta la podemos considerar como una eventualidad .como descompostura en la red telemática con una irrupción de los flujos, con entorpecimiento en los tratamientos o la alteración de archivos y programas con motivo de una falla técnica, eventos naturales o intervención humana.

[131] Ob. Cit. Téllez Valdes Julio. Pág. 78 y ss.

- **Amenaza a la identidad cultural**, provocada por la apertura mundial, ya que resulta la transformación de las culturas nacionales respecto aquello que ofrecen las culturas importadas, dándose con esto los fenómenos de transculturación a través de las llamadas industrias de la cultura.

- **Dependencia tecnológica exagerada**. La evolución de firmas multinacionales ha producido una especialización de producciones y mundialización de mercados, teniendo a la informática y las telecomunicaciones como sus máximas manifestaciones, satisfaciendo una serie de necesidades de los Estados en desarrollo.

- **Incidencias económicas notorias**. El desarrollo y pérdida de nuevas tecnologías de la información traen consigo una gran cantidad de inversiones económicas, con notorias desproporciones entre los beneficiarios y los que creen ser uno de ellos.[132]

2.2.4. PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE COMPUTACIÓN (SOFTWARE).

Como ya se ha venido manifestado, la comercialización de las computadoras se inició propiamente en la década de los setenta. Siendo que en un principio el 70% del capital destinado al desarrollo de la industria informática se empleaba en el área de componentes físicos (hardware) en tanto que el 30% se canalizaba al área de soporte lógico (software).

Por lo que en nuestros días, la creación de programas se torna más compleja y mas costosa, ya que los programas de cómputo son los que soportan el adecuado comportamiento y carácter efectivo de las computadoras, invirtiéndose las cifras ya que la industria de la programación absorbe en la actualidad el 70% de los costos.

[132] Idem. Pág. 78.

Al hablar de la protección jurídica de los programas de computadora, consideramos que están inmiscuidos dos tipos elementales: la protección del software y la protección de las bases de datos. Esto es por que finalmente los dos elementos constituyen la protección jurídica de los derechos de autor que consagra la propiedad intelectual. Aunque un programa de computadora sea totalmente diferente a una base de datos pensamos que sus coincidencias y sus efectos jurídicos constituyen es este tipo de protección jurídica intelectual.[133]

Lo anterior es porque, la complejidad de esta protección atañe jurídicamente a áreas del derecho que para su protección hay dos líneas doctrinales. Así, algunos doctrinarios, 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 tantos doctrinarios, se inclinan por el derecho de patentes cosa que no ha tenido gran apoyo en el panorama legislativo.

En términos generales se puede considerar a programa de computadora como toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una tarea u obtener un resultado determinado cualquiera que fuera su forma de expresión y fijación.[134]

Los programas de cómputo se pueden considerar 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.[135]

Podemos distinguir dos tipos de programas:

[133] Paez Maña Jorge, La Protección de las Bases de Datos. España. 1996. Según señala Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 25.
[134] Idem, Pág. 25.
[135] Ob. Cit. Téllez Valdes Julio, Derecho Informático. Pág. 86.

Los programas fuente (conocidos como sistemas operativos o de explotación) están ligados al funcionamiento mismo de la maquina, guardando una relación con las memorias centrales y auxiliares de la computadora.

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.[136]

Este programa permite un adecuado enlace entre la máquina y los trabajos del usuario.

Los Programas Objeto, son aquellos que se realizan para satisfacer las necesidades más variadas de los usuarios, y que permiten el tratamiento de datos definidos concretamente, siendo disociables de la maquina.

El Código objeto, 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.[137]

Es evidente que los programas están relacionados de manera estrecha con los llamados lenguajes de programación, los cuales, sea del nivel de que se traten, fungen como medio de enlace entre el lenguaje natural y el lenguaje de la máquina.

Los programas de cómputo como una de las máximas manifestaciones del producto-información ha provocado un apuntalamiento de la industria de programación, lo cual ha traído consigo que los problemas en torno al software rebasen la esfera puramente técnica, para alcanzar niveles económicos y, por ende, jurídicos.[138]

---

[136] Ceros Perez Ramiro, La Protección de datos personales y programas de computadora, en Ambito Jurídico de las Tecnologías de la información., Plan Estatal de formación. Consejo General del Poder Judicial. Escuela Judicial de Formación Continua. Madrid, España, 20-22 de mayo de 1996. Se Según cita de Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 28.

[137] Idem. Pág. 28.

[138] Ob. Cit. Téllez Valdes Julio. Derecho Informático. Pág. 86.

Siendo que en la actualidad esto representa perdidas económicas, referente a la protección de programas, así como un sin numero de acciones ilícitas que trae repercusiones tanto a empresas como a los particulares cuando se ven afectado por algún delito relacionado a este tema, y el cual se hablara mas adelante.

2.2.5. CONTRATOS INFORMÁTICOS.

Los contratos informáticos surgen ligados a la inminente comercialización de las computadoras. Esto originó una rápida comercialización como consecuencia la proliferación de contratos en materia informática, en el ámbito de los negocios. Favoreciendo la práctica comercial, en la concurrencia del libre mercado.

Con la tecnología informática, se modifica las tradicionales jerarquías organizacionales y las múltiples capas de administradores; las empresas se convierten en virtuales y sus actos de comercio se ejecutan por medio de la red de Internet. Por su parte, el comercio tradicional se transforma en comercio electrónico. Algunos de los componentes de la nueva forma mercantil son:[139]

- Las relaciones empresa a empresa digitalmente conocidas como EXTRANET. Se dice que en la actualidad, que la "producción" no empieza ni termina en la fábrica. El concepto de la línea de ensamblaje, en donde la información fluía verticalmente, se ha transformado. En el nuevo modelo de producción económica, la información fluye horizontalmente, ampliando el proceso de la línea de producción y el proceso de fabricación se llega a extender desde las materias primas hasta el servicio "post-venta" o de apoyo. Se habla de administración transaccional de suplidores que operan en cadena (supply chain management), donde los flujos de procesos/información empresarial se estandarizan para discurrir automáticamente en la red.

[139] Ob. Cit. Perez Marayo Guillermo Augusto. Derecho, Tecnología y Cambio. Pág 3.

- Las relaciones empresa/cliente. En la economía digital surgen innovadores formas de hacer comercio con los clientes y las relaciones tradicionales de comercio "sobre el mostrador" se ven alteradas en el sentido de que los clientes pueden ser atendidos en-línea y realizar la totalidad de la relación comercial vía Internet. Las tradicionales empresas de representación de casas extrajeras, son desintermediadas por la red; tal es el caso cuando las casas matrices ponen a disposición (global) sus productos desde un servidor localizado en cualquier parte del mundo. La intermediación entre productores y consumidores está siendo eliminadas por las redes digitales, la atención en-línea, los help desk , los catálogos, los directorios interactivos y otros sistemas de multimedia.

- Relaciones intraempresa o intranet. A lo interno la empresa también se producen transformaciones; como según se menciono, desaparecen los mandos medios, las nuevas organizaciones desplazan en la medida de lo posible la toma de decisiones desde las esferas más altas hacia la base, hacia la periferia.

Todo esto ha dado como resultado la diversificación contractual, conocida con el anglicismo de unbundling, que consiste en hacer una contratación por separado respecto a los bienes o servicios informáticos, lo que trajo como consecuencia la creación de mercados diversos, surgiendo empresas especializadas en relación a las vertientes informáticas, tanto en la construcción y venta de equipos, como la presentación de bienes o servicios.

Si bien del nacimiento del WWW se sitúa alrededor de 1991, el nacimiento del comercio electrónico se sitúa en 1995 precisamente con la utilización de Internet para los negocios. Desde ese momento, el crecimiento no se ha producido únicamente en el volumen de negocios sino también en la infraestructura de soporte del propio comercio electrónico. Para dar un dato indicativo, la corporación IDC (International Data Corporation) aportó el

Siendo considerable y de gran inquietud que este tipo de datos pueden ser vulnerables, ya que la destinación que puedan ser objeto, pudiendo ser variada, como la información que es empleada para fines publicitarios, comerciales, fiscales, policíacos etcétera, convirtiéndose en un instrumento de opresión y mercantilismo.

Pero también provoca que las personas corran un gran riesgo sobre dicho datos, ya que los mismos pueden ser utilizados para otras finalidades, alterando con esto los derecho fundamentales de los individuos en la sociedad, provocando discriminaciones, manipulaciones, persecuciones, presiones, asedios, etcétera. Quedando al margen de un adecuado control jurídico de dicha información.

Ya desde 1968, en el seno de la Asamblea de los Derechos Humanos auspiciada por la ONU, se mostraba una honda preocupación por la manera en que la ciencia y la tecnología podrían alterar los derechos de los individuos, empezando a detonar la necesaria emanación de un régimen jurídico que pudiera afrontar de manera cabal este género de situaciones.[115]

La expresión protección de datos personales es entendida como la protección jurídica de las personas en lo que concierne al tratamiento automatizado de su datos personales, o expresando en su forma más extensa, el amparo debido de 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. [116]

Ahora bien, la información de carácter personal o información nominativa, está definida en 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,[117] como toda información concerniente a la persona física identificada o identificable.

---

[115] Idem. Pág. 70.
[116] Davara Rodríguez Miguel Angel., Op Cit. Pág. 18.
[117] Firmado en Estramburo el 28 de enero de 1981.

También existen tres documentos claves en los que debe basarse cualquier regulación relativa a la protección de los datos de carácter personal a saber:

a) El convenio del Consejo de Europa del 28 de enero de 1981 para la protección de las personas con relación a los datos de carácter personal; ratificado por España el 27 de enero de 1984.

b) El acuerdo de Schegen de 14 de junio de 1985 relativo a la supresión gradual de los controles entre las fronteras comunes.

c) La propuesta de Directiva del Consejo de la Comunidad Económica Europea del 24 de septiembre de 1990 relativa a la protección de las personas en lo referente al tratamiento de datos personales (modificada el 15 de octubre de 1992).[118]

MUÑOZ nos explica que las legislaciones que han consagrado la protección sobre el uso y gestión de la información personal, destacan las siguientes características:

1.- El derecho a la autodeterminación informativa: 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 trasmitirlos por los medios informáticos, también denominado "libertad informática". Este derecho toma diversas vertientes de aplicación práctica:

a) Derecho de la información. En el sentido de tener el individuo la posibilidad de conocer la existencia de algún bando de datos o fichero de información personal;

[118] Del Peso Navarro, Emilio y Ramos González, Miguel Angel., Confidencialidad y Seguridad de la Información: la LORTAD y sus implicaciones Socioeconómicas., Edt. Díaz de Santos. S.A., Madrid ., España, 1994. Pág. 69. Según cita de Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano. Pág. 18.

b) 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, almacenamiento de información personal;

c) Derecho de actualización. Gracias al cual, el individuo puede exigir la corrección de ciertos datos;

d) Derecho de confidencialidad. Derecho que concede al sujeto la exigencia a que la información que proporciona permanezca ajena al conocimiento de terceros;

e) Derecho de exclusión. Por la naturaleza de la información puede el individuo cancelar, borrar o solicitar la destrucción de información denominada como sensible.[119]

Completando el anterior análisis, 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 su datos de carácter personal que ofrezca un perfil suyo obtenido de esta forma, y también, por último, del derecho del 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.[120]

Continuando con MUÑOZ que nos indica que dentro de la protección de datos encontramos la ***información sensible***. Para este tipo de información, dice la disposición europea "es la información de carácter personal, relevante al origen racial, opiniones públicas, las convicciones religiosas, así como los datos de carácter personal relativas a la salud o a la vida sexual, no pueden ser tratados automáticamente a menos que el

[119] Muñoz de Alba, Marcia., Manejo de la Información Vs. Vida Privada., en Núcleo de Estudios Interdisciplinarios en Salud y Derechos Humanos. reunión 16-1-95. Instituto de Investigaciones Jurídicas. Universidad Autónoma de México. México. 1995. Págs 5 y ss.

[120] Davara Rodríguez. Miguel Angel., La Protección de datos en Europa., Op Cit. Pág. 25. Según cita de Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 19.

Derecho interno prevea las garantías determinadas. En el mismo sentido se encuentra la información de tipo personal concerniente a las infracciones penales.

Por el contenido de la información sensible los riesgos y daños potenciales por su difusión producen un impacto mayor en la intimidad y dignidad de la persona. Tomando entonces tres vías fundamentales:

a) La información relativa a las creencias religiosa, política o sindicales;

b) Información relativa al origen racial, de salud y preferencias sexuales;

c) Información relativa a los antecedentes penales o infracciones administrativas.[121]

Así la clasificación de los datos nominativos constituye objeto del reconocimiento del derecho a la autodeterminación informativa.

Nos mencionada JOVER Y CABRERA, que el derecho a la autodeterminación informativa es un derecho de acertada denominación jurisprudencial (procedente del Tribunal Constitucional Alemán) vinculado al right of privacy de Warren y Brandeis, y que en la década de los setenta fue utilizado en el ámbito jurídico angloamericano, pero en una acepción diferente a la original: derecho que todo individuo tiene a decir qué información de su vida personal puede ser difundida o decirse si puede o no difundirse. Constituye esta aceptación una modalidad de la noción de "facultad de disposición" sobre los principios datos y concuerda con la que el Tribunal Constitucional Alemán formularía con la expresión de "autodeterminación sobre la información" como emanación del derecho a la persona.[122]

Por lo que dicha problemática ha sido de gran trascendencia a nivel internacional, al regular las variadas figuras de índole jurídico.

---

[121] Muñoz de Alba, Marcia.. Op y Pág. Cit. Según señala Riestra Gaytán Emma, Pág. 20.

[122] Jover Pedro, Jose y Cabrera Vilaplana, Silvia. Op. Cit. Pág. 75 Según Cita de Riestra Gaytán Emma. Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 12.

Así tenemos que las figuras tales como los derechos humanos, derechos personales, derecho 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 aun las garantías individuales y sociales como pudiera ser el caso en 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.[123]

La intimidad es el conjunto de circunstancias, cosas, expresiones, sentimiento 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 por la develación sea lícita.[124]

Por lo que señalaremos que el Derecho a la Intimidad o Privacía, 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 de terceros o para el bienestar común.[125]

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, y muy especialmente, el Estado, a fin de que se realice el 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 derecho y obligaciones.[126]

---

[123] Ob. Cit. Téllez Valdes Julio. Derecho Informático. Pág. 70.
[124] Méjan C. Luis Manuel. El Derecho a la Intimidad y la Informática,. Pág. 87.
[125] Idem. Pág. 105.
[126] Idem. Pág. 106.

2.2.3. FLUJO DE DATOS TRANSFRONTERIZOS.

Este es otro de los problemas que se ven reflejados en la actualidad en relación a la tecnología y comunicación que se maneja a nivel internacional y que es de suma preocupación en relación a la gran trascendencia que trae consigo.

Según el Consejo de Económico de la Organización de las Naciones Unidas (ONU), el Flujo de Datos Transfronterizos es " la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y repercusión.[127]

Este problema ha sido considerado desde el punto de vista de la limitación o favorecimiento de la circulación de datos a través de las fronteras nacionales, dependiendo de los aspectos positivos o negativos que esto pueda traer aparejado con los diversos países. Problema que 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.

Es evidente que en nuestros días. Los avances tecnológicos han proyectado sociedades aisladas, poniéndolas en contacto con la modernidad. 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. Los resultados son una nueva realidad comercial es la emergencia de mercados globales para consumidores de productos estandarizados en una escala previamente inimaginable. RAVI KALAKOTA.[128]

[127] Ob. Cit. Téllez Valdés Julio. Derecho Informático. Pág.77.

[128] Perez Marayo Guillermo Augusto. Abogado y Notario, Universidad Complutense de Madrid. Asesor Parlamentario, especialista en Investigación de Información en el Internet. "Instrumentos de Pago Internacional, Tecnología Informática y Comercio Electronico". (Costa Rica) Derecho, Tecnología y Cambio. 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático). (www.yahoo.com). Pág. 1.

Hasta hace un tiempo, el cambio era lento y pausado, pero con la introducción de las más complejas herramientas generadas por la humanidad a saber, la computadora (la nueva imprenta multimedia) y la red (las nuevas rutas comerciales), el cambio se revolucionó. A partir de la Segunda Guerra Mundial, el modelo industrial se comienza a resquebrajar ante nuestros ojos, poniendo en crisis los conceptos institucionales, organizacionales y las relaciones de poder, heredados desde tiempos inmemoriales. Actualmente los gobiernos son tachados de ineficientes; es común el sentir de que el sistema no responde a la realidad de nuestros tiempos.[129]

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, comunicamos y, en general, nuestra forma de vida. Vivimos en una era que no ha tenido un nombre específico "la Post-Guerra", la era atómica, la era cibernética e informática pero llámese como se llame, no cabe duda de que estamos en la Era Post- Industrial, en donde la nueva ciencia, la tecnología informática, genera constantemente herramientas digitales paradigmáticas de aceptación universal, que transforman la comunidad humana.[130]

En las economías post-industriales en donde el manejo de la información representa hoy en día entre el 40 y 50 % del valor agregado, es natural que los intercambios internacionales de información se destinen a formar un papel importante. Con base a ello se sustenta en buena medida el funcionamiento de la economía mundial en donde la especialización e interdependencia de los Estados se acentúa más. Sin embargo el desplazamiento rápido y las preocupaciones de los derechos del hombre hacia la soberanía nacional, así como las incidencias económicas y sociales de intercambios inmateriales entre las naciones, trae consigo implicaciones positivas como negativas, y que al respecto nos señala JULIO TÉLLEZ VALDES.

[129] Idem. Pág. 2.
[130] Idem. Pág. 3.

Es considerable ver que el Flujo de Datos Transfronterizos aporta beneficios a las colectividades nacionales como:

- **Favorecimiento de la paz y la democracia**. No podríamos dejar de recordar los vínculos estrechos existentes entre libertad de circulación de información, derechos del hombre y valores fundamentales de la humanidad. Libre comunicación de mensajes y de opiniones es esencial para la democracia y la paz mundial.

- **Favorecimiento en el progreso técnico y crecimiento**. La cooperación entre los científicos que constituyen una comunidad a escala mundial y la competencia de industriales y empresarios han hecho gala de su aptitud difundiendo los conocimientos y técnicas.

- **Finalmente, no podemos olvidar que la interdependencia económica de las naciones es hoy en día una realidad irreversible**. A raíz de la internacionalización de compañías y la especialización de actividades nacionales, toda restricción súbita y deliberada a la continuidad del flujo de datos, tal como existen hasta ahora, podría asimilarse a una especie de acta de guerra económica a la par de un bloqueo o embargo. Es imposible concebir hoy en día a algún país que goce de una independencia total en el plano económico.[131]

Del otro lado de la microelectrónica y el progreso de las telecomunicaciones, trae consigo una serie de riesgos, de los que se podrían distinguir, los siguientes:

- **La vulnerabilidad social**, esta la podemos considerar como una eventualidad como descompostura en la red telemática con una irrupción de los flujos, con entorpecimiento en los tratamientos o la alteración de archivos y programas con motivo de una falla técnica, eventos naturales o intervención humana.

[131] Ob. Cit. Téllez Valdes Julio. Pág. 78 y ss.

- **Amenaza a la identidad cultural**, provocada por la apertura mundial, ya que resulta la transformación de las culturas nacionales respecto aquello que ofrecen las culturas importadas, dándose con esto los fenómenos de transculturación a través de las llamadas industrias de la cultura.

- **Dependencia tecnológica exagerada**. La evolución de firmas multinacionales ha producido una especialización de producciones y mundialización de mercados, teniendo a la informática y las telecomunicaciones como sus máximas manifestaciones, satisfaciendo una serie de necesidades de los Estados en desarrollo.

- **Incidencias económicas notorias**. El desarrollo y pérdida de nuevas tecnologías de la información traen consigo una gran cantidad de inversiones económicas, con notorias desproporciones entre los beneficiarios y los que creen ser uno de ellos.[132]

2.2.4. PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE COMPUTACIÓN (SOFTWARE).

Como ya se ha venido manifestado, la comercialización de las computadoras se inició propiamente en la década de los setenta. Siendo que en un principio el 70% del capital destinado al desarrollo de la industria informática se empleaba en el área de componentes físicos (hardware) en tanto que el 30% se canalizaba al área de soporte lógico (software).

Por lo que en nuestros días, la creación de programas se torna más compleja y mas costosa, ya que los programas de cómputo son los que soportan el adecuado comportamiento y carácter efectivo de las computadoras, invirtiéndose las cifras ya que la industria de la programación absorbe en la actualidad el 70% de los costos.

[132] Idem. Pág. 78.

Al hablar de la protección jurídica de los programas de computadora, consideramos que están inmiscuidos dos tipos elementales: la protección del software y la protección de las bases de datos. Esto es por que finalmente los dos elementos constituyen la protección jurídica de los derechos de autor que consagra la propiedad intelectual. Aunque un programa de computadora sea totalmente diferente a una base de datos pensamos que sus coincidencias y sus efectos jurídicos constituyen es este tipo de protección jurídica intelectual.[133]

Lo anterior es porque, la complejidad de esta protección atañe jurídicamente a áreas del derecho que para su protección hay dos líneas doctrinales. Así, algunos doctrinarios, 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 tantos doctrinarios, se inclinan por el derecho de patentes cosa que no ha tenido gran apoyo en el panorama legislativo.

En términos generales se puede considerar a programa de computadora como toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una tarea u obtener un resultado determinado cualquiera que fuera su forma de expresión y fijación.[134]

Los programas de cómputo se pueden considerar 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.[135]

Podemos distinguir dos tipos de programas:

---

[133] Paez Maña Jorge. La Protección de las Bases de Datos. España. 1996. Según señala Riestra Gaytán Emma. Los Delitos Informáticos en el Derecho Positivo Mexicano, Pág. 25.
[134] Idem, Pág. 25.
[135] Ob. Cit. Téllez Valdes Julio. Derecho Informático. Pág. 86.

Los programas fuente (conocidos como sistemas operativos o de explotación) están ligados al funcionamiento mismo de la maquina, guardando una relación con las memorias centrales y auxiliares de la computadora.

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.[136]

Este programa permite un adecuado enlace entre la máquina y los trabajos del usuario.

Los Programas Objeto, son aquellos que se realizan para satisfacer las necesidades más variadas de los usuarios, y que permiten el tratamiento de datos definidos concretamente, siendo disociables de la maquina.

El Código objeto, 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.[137]

Es evidente que los programas están relacionados de manera estrecha con los llamados lenguajes de programación, los cuales, sea del nivel de que se traten, fungen como medio de enlace entre el lenguaje natural y el lenguaje de la máquina.

Los programas de cómputo como una de las máximas manifestaciones del producto-información ha provocado un apuntalamiento de la industria de programación, lo cual ha traído consigo que los problemas en torno al software rebasen la esfera puramente técnica, para alcanzar niveles económicos y, por ende, jurídicos.[138]

---

[136] Ceros Perez Ramiro. La Protección de datos personales y programas de computadora, en Ambito Jurídico de las Tecnologías de la información.. Plan Estatal de formación. Consejo General del Poder Judicial. Escuela Judicial de Formación Continua. Madrid, España. 20-22 de mayo de 1996. Se Según cita de Riestra Gaytán Emma. Los Delitos Informáticos en el Derecho Positivo Mexicano. Pág. 28.

[137] Idem. Pág. 28.

[138] Ob. Cit. Téllez Valdes Julio. Derecho Informático. Pág. 86.

Siendo que en la actualidad esto representa perdidas económicas, referente a la protección de programas, así como un sin numero de acciones ilícitas que trae repercusiones tanto a empresas como a los particulares cuando se ven afectado por algún delito relacionado a este tema, y el cual se hablara mas adelante.

2.2.5. CONTRATOS INFORMÁTICOS.

Los contratos informáticos surgen ligados a la inminente comercialización de las computadoras. Esto originó una rápida comercialización como consecuencia la proliferación de contratos en materia informática, en el ámbito de los negocios. Favoreciendo la práctica comercial, en la concurrencia del libre mercado.

Con la tecnología informática, se modifica las tradicionales jerarquías organizacionales y las múltiples capas de administradores; las empresas se convierten en virtuales y sus actos de comercio se ejecutan por medio de la red de Internet. Por su parte, el comercio tradicional se transforma en comercio electrónico. Algunos de los componentes de la nueva forma mercantil son:[139]

- Las relaciones empresa a empresa digitalmente conocidas como EXTRANET. Se dice que en la actualidad, que la "producción" no empieza ni termina en la fábrica. El concepto de la línea de ensamblaje, en donde la información fluía verticalmente, se ha transformado. En el nuevo modelo de producción económica, la información fluye horizontalmente, ampliando el proceso de la línea de producción y el proceso de fabricación se llega a extender desde las materias primas hasta el servicio "post-venta" o de apoyo. Se habla de administración transaccional de suplidores que operan en cadena (supply chain management), donde los flujos de procesos/información empresarial se estandarizan para discurrir automáticamente en la red.

[139] Ob. Cit. Perez Marayo Guillermo Augusto. Derecho, Tecnología y Cambio. Pág 3.

- Las relaciones empresa/cliente. En la economía digital surgen innovadores formas de hacer comercio con los clientes y las relaciones tradicionales de comercio "sobre el mostrador" se ven alteradas en el sentido de que los clientes pueden ser atendidos en-línea y realizar la totalidad de la relación comercial vía Internet. Las tradicionales empresas de representación de casas extrajeras, son desintermediadas por la red; tal es el caso cuando las casas matrices ponen a disposición (global) sus productos desde un servidor localizado en cualquier parte del mundo. La intermediación entre productores y consumidores está siendo eliminadas por las redes digitales, la atención en-línea, los help desk , los catálogos, los directorios interactivos y otros sistemas de multimedia.

- Relaciones intraempresa o intranet. A lo interno la empresa también se producen transformaciones; como según se menciono, desaparecen los mandos medios, las nuevas organizaciones desplazan en la medida de lo posible la toma de decisiones desde las esferas más altas hacia la base, hacia la periferia.

Todo esto ha dado como resultado la diversificación contractual, conocida con el anglicismo de unbundling, que consiste en hacer una contratación por separado respecto a los bienes o servicios informáticos, lo que trajo como consecuencia la creación de mercados diversos, surgiendo empresas especializadas en relación a las vertientes informáticas, tanto en la construcción y venta de equipos, como la presentación de bienes o servicios.

Si bien del nacimiento del WWW se sitúa alrededor de 1991, el nacimiento del comercio electrónico se sitúa en 1995 precisamente con la utilización de Internet para los negocios. Desde ese momento, el crecimiento no se ha producido únicamente en el volumen de negocios sino también en la infraestructura de soporte del propio comercio electrónico. Para dar un dato indicativo, la corporación IDC (International Data Corporation) aportó el

siguiente dato: los ingresos de los proveedores de Internet americano entre el año 1998 y 1999 subieron un 41% y el número de páginas registradas en la red un 137%.[140]

Lo más impresionante de todo es que la facilidad de los consumidores y de los hombres de negocios para acudir a la red de redes hace que el comercio electrónico pueda crecer muy rápidamente.

Sin embargo, Internet juega un rol mucho más importante en las transacciones que se completan al margen de la red. Además de los compradores que escogen sus productos en la red y pagan fuera de ella, Internet es una enorme fuente de información sobre el comportamiento de consumidores que se informan y compran fuera de ella. Cyber Dialogue has estimado que, para 1998, mientras las compras ordenadas y pagadas a través de Internet fueron de 11 mil millones de dólares las compras efectuadas a través de Internet pero pagadas fuera de ella, llegaron a los 15 mil millones de dólares, y no solamente eso, sino que las compras efectuadas fuera de Internet pero influenciadas por ésta superaron los 51.000 millones de dólares.[141]

El comercio electrónico se puede definir, de una forma muy amplia y abarcadora según la Asociación de Usuarios de Internet (España), como cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación. En este sentido, el concepto de comercio electrónico no sólo incluye la compra y venta electrónica de bienes o servicios, que en el concepto común que se tiene, sino que también incorpora el uso de las redes para actividades anteriores o posteriores a la venta, como son:[142]

---

[140] De Paladella Carlos. Abogado por la Universidad deBarcelona (España), Master en Derecho de Empresas por la Universidad Austral (Argentina) y posgrado de especialización sobre Revolución Digital CENIT. (España). "El Derecho en la Era Digital. Aspectos Jurídicos de las nuevas tecnologías de la información y de las comunicaciones (Parte I)". 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, (www.yahoo.com). Pág. 2.

[141] Idem. Pág. 3.

[142] Idem. Pág. 4.

- La Publicidad.
- La Búsqueda de información.
- El aseguramiento de las posibles transacciones.
- El Tratamiento de clientes y proveedores, incluso inversores.
- Trámites ante autoridades de control y fiscalización.
- La negociación de condiciones de compra, suministros, etc.
- La prestación de mantenimientos y servicios posventa.
- La colaboración entre empresas.

Por lo que podemos decir que un contrato informático, es aquel cuyo objeto sea un bien o un servicio informático o ambos o que una de las prestaciones de las partes tenga por objeto ese bien o servicio informático.[143]

Sin olvidar que los contratos son el acuerdo de dos o más voluntades para crear, transferir, modificar o extinguir derechos u obligaciones,[144] ya que en toda relación contractual encontramos a uno o más sujetos, quienes deberán cumplir con sus obligaciones, o en su caso exigir sus derechos ante las autoridades competentes.

Denotando que los contratos informáticos en cuento a este respecto no son la excepción, por lo que las partes que intervienen también son sujetos de derechos y obligaciones, y son catalogados como ***proveedores*** (son aquellos encargados de proporcionar un bien o un servicio) y ***usuarios*** (son aquellos que reciben la prestación de dar o hacer por parte de los proveedores y están constituidos por el sector público y privado en sus diferentes niveles).

Técnicamente, hay una serie de modalidades dependiendo de que se trate de bienes o servicios informáticos, por lo que consideramos importante expresar, aunque sea sólo en una forma enunciativa, algunos de los principales tipos de contratos de acuerdo a esta naturaleza.[145]

---

[143] Ob Cit Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Positivo Mexicano. Pág. 21.
[144] Artículo 1792 del Código Civil para el Distrito Federal. Agenda Civil 98, Edit. ISEF, S.A. Pág 185.
[145] Ob. Cit. Téllez Valdes Julio. Derecho Informático. Pág. 98.

- Contratos de material o de sistemas.
- Compatibilización de equipos y programas.
- Servicios y aprovisionamiento de refacciones.
- Contratos de programa- producto.
- Adquisición de programas.
- Licencia de uso de programas.
- Desarrollo de programas.
- Análisis y tratamiento de datos.
- Contrato de mantenimiento.
- Contrato de Asesoría.
- Contrato de formación o capacitación, etcétera.

Por lo que podemos ver que en la actualidad el comercio electrónico, ha sido de mucha preocupación para nuestro país que en recientes reformas del mes de mayo del presente año, el Código Civil para le Distrito Federal en Materia Común y para toda la República en Materia Federal, se contemplan ya los medios electrónicos como medio expreso de un acuerdo de voluntades.

Artículo 1803. El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:[146]

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

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

[146] Anexo Agenda Civil 2000. Decreto por el que reforma y adiciona diversas disposiciones del Código Civil para el Distrito Federal en Materia Comun y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles. Ediciones Fiscales ISEF. Pág. 75

Siendo otro de los temas relacionados con los contratos informáticos:

a) El Valor probatorio del documento electrónico.

Un documento electrónico es aquel que proviene de la elaboración electrónica, y por ello, documento informático será el que tenga su origen en la informática.[147]

Para tal efecto es necesario delimitar cuales son los elementos de un documento electrónico GIANNATONIO, explica que concebir la escritura como fijación sobre un soporte material de un mensaje destinado a la conservación, afirma que no hay inconveniente para considerar el documento electrónico como documento escrito, ya que:

1.- Contiene un mensaje (texto alfanumérico o diseño gráfico).
2.- El lenguaje convencional (el de los bits).
3.- Sobre soporte (cinta o disco).
4.-Y destinado a durar en el tiempo. [148]

Aún y cuando concibamos la existencia y viabilidad en la prueba jurisdiccional, existen otro elemento que conlleva la problemática de dicha prueba, esto es, que comúnmente consideramos que el acuerdo entre las partes se encuentra formalizado una vez que éstas manifiestan su pleno consentimiento mediante la firma, cosa que en principio en un documento electrónico no aparece, sin embargo, esto como FALCON expresa, la falta de la firma en los documentos informáticos no los inhibe como material probatorio, pero requiere que los Jueces puedan disponer de elementos de control sobre la exactitud de

[147] Carrasco Lopez Valentín. Informática y Derecho. Revista Latinoamericana de Derecho Informático. Vol I. UNED. Centro Regional de Extremadura. Madrid. España. 1998. Según cita de Riestra Gaytán Emma. Los Delitos Informáticos en el Derecho Posito Mexicano, Pág. 21.

[148] Giannatonio, Ettore, El valor jurídico del documento electrónico., Informática y Derecho. Aportes de Doctrina Informática, vol. I DEPALMA. Buenos Aires, Argentina, 1991., Obra Citada Por Carrasco López Valentín, Pág. 156.

la información, confiables que produzcan una razonable certeza sobre la existencia de los hechos que surgen de éstos documentos electrónicos. La autenticidad del documento electrónico no es el único elemento a tener en cuenta. Aún probada la autenticidad del documento electrónico, la atribución del mismo no es tan sencilla. Para ésta habrá que legislar sobre la atribución jurídica en cada uno de los supuestos. Sin embargo, el avance tecnológico es de por sí un particular escollo para poder dar normas con sentido más o menos permanente o por lo menos fijas los puntos de apoyo de una legislación o jurisprudencia interpretativa.[149]

Ya en México, contamos con un la nueva legislación en materia de la valoración del documento electrónico, consagrado en el Código Federal de Procedimientos Civiles en sus recientes reformas realizadas en el mes de mayo del presente año, en su artículo 210-A.

" Se reconoce como prueba la información generada o comunicada que consiste en medios electrónicos, ópticos o de cualquier otra tecnología".[150]

Por lo que podemos ver que el desarrollo de la tecnología ha creado la solución al desarrollar los diversos sistemas de encriptación que presuponen la autentificación del documento de los cuales se deriva la creación de la firma electrónica.

b) Criptografía.

La palabra proviene del griego "Kryptos" que significa esconder y "graphein" que significa escribir. La Criptografía estudia las diferentes maneras de Esconder información en forma escrita, como sonido o imágenes y así pueda ser transmitida por cualquier línea o medio de transmisión insegura, sin temor a ser entendible al ser interceptada por personas no autorizadas. Por otra parte, el Criptoanálisis estudia las técnicas para poder

[149] Falcon Enrique M. ¿Qué es la informática jurídica?, Ed. Abeledo- Perrot., Buenos Aires, Argentina, 1992. Cit. Carrasco López Valentín, Ob. Cit. Pág. 146.
[150] Ob. Cit. Anexo Agenda Civil 2000. Pág. 76.

leer mensajes que hayan sido escondidos, gracias a la Criptografía. Al conjunto de la Criptografía y el Criptoanálisis se le conoce como Criptología.[151]

c) Firma Electrónica.

La firma electrónica consiste en una serie de caracteres puestos al final de un documento. Está elaboración según procedimiento matemático (criptográficos) y realiza un resumen codificado del mensaje, de las informaciones referentes a la fecha y hora del envío del mensaje, a la identidad del remitente y el receptor. Las firmas electrónicas responden a las siguientes características:

- La firma debe permitir la identificación del firmante. La relación firma-firmante, debe ser única y absoluta: a una firma dada no se puede asociar más que un único firmante.

- La firma no puede ser "generada" más que por el emisor del documento. Debe ser suficientemente inimitable e infalsificable. Incluso en materia de firma manuscrita, no puede haber certeza absoluta a este respecto. La misma calidad se puede encontrar en ciertas firmas electrónicas.

- Una firma electrónica es establecida unas veces en función del contenido del documento, otras en función de las informaciones secretas únicas y propias del emisor, otras en función de informaciones comunes, al emisor y al destinatario y que pueden ser públicas (por ejemplo: algoritmo de forma utilizando parámetros eventuales...) o bien una mezcla de los diversos elementos citados.[152]

---

[151] Angel, Jose de Jesus. "Criptografía y Curvas Elípticas". Tesis de Maestría en matemáticas. U. A. M. Iztapalapa. México, 1998. Según Cita Bartolini Esparza Marcelo en su Tesis para obtener el tituto de Licenciado en Derecho. El "Dinero Electrónico " a la luz del Derecho Posito Mexicano. Universidad la Salle, A.C., facultad de Derecho. México, D. F., 1999. Pág. 69.

[152] Ob. Cit. Carrascosa López Valentín. Pág. 143.

Al respecto algunos autores nos señalan que el contenido de la normativa prevista está referido en dos temas centrales: a la definición de la firma electrónica y la delimitación de quienes pueden ser proveedores de servicios de certificación. Así se menciona explícitamente en el artículo 1 que la Directiva tiene como fin facilitar el uso de las firmas electrónicas y procurar su reconocimiento jurídico, estableciendo para ello un sistema jurídico adecuado para regular los servicios de certificación accesibles al público, servicios que son indispensables para asegurar el funcionamiento del mercado interno contando con el mecanismo de las firmas electrónicas. A efectos de evitar confusiones se menciona también que en el mismo artículo que está fuera de la norma lo referido a la validez y conclusión de los contratos y otras formalidades extracontractuales que requieran el uso de formas.[153]

En consecuencia, aunque al igual que en el caso de los documentos comunes puede haber documentos electrónicos sin firma, el documento electrónico- y en especial el documento con giro mercantil- es firmable, en el sentido de que el requisito de la firma autógrafa o equivalente puede ser sustituido, por el lado de la criptografía, por medio de cifras, signos, código de barras, claves u otros atributos alfanuméricos que permitan asegurar la procedencia y veracidad de su autoría y autenticidad de su contenido.[154]

Es evidente que el comercio electrónico, hoy en día viene a formar uno de los aspectos mas importares en la economía de los países, referente al acuerdo de voluntades plasmado en un contrato electrónico y como consecuencia la seguridad de utilizar una firma digital.

---

[153] Galindo Fernando., El proyecto de Directiva Europea sobre firma Electrónica., La Ley Actualidad, Madrid, España. 10 de junio de 1998. Vid. Según cita Riestra Gaytán Emma, Los Delitos Informáticos en el Derecho Posito Mexicano, Pág. 24.

[154] Ribas Javier., Efectos legales de las firmas electrónicas, Diario de Noticias, La Ley Actualidad, año 2 Nú. 84, Madrid, España 5 de julio de 1998. Según cita de Riestra Gaytán Emma, Pág. 24.

En estos momentos varías empresas argentinas están participando en un proyecto de firma digital en el que dicha empresas remitirán a la Comisión Nacional de Valores sus estados contables firmados digitalmente. Dichos estados contables se consideran absolutamente validos toda vez que la Comisión Nacional De Valores dará validez a los documentos enviados con la firma digital de las empresas que previamente habrán obtenido esa firma digital en la autoridad de aplicación.[155]

2.2.6. ERGONOMÍA INFORMÁTICA.

Se refiere etimológicamente, al conjunto de enunciados referidos a la aplicación de la informática en el ámbito laboral. Proviene de ergon, energía, trabajo y nomos, tratado y del vocablo informática ya aludido.

Es el conjunto de implicaciones de orden normativo laboral provocados por el uso de la informática.[156]

Paralelamente a los cambios en las organizaciones, también se producen grandes transformaciones en la composición de las fuerzas laborales, igual como sucedió con el desplazamiento laboral de la agricultura a las fábricas. Hoy día la fuerza laboral se desplaza de trabajos en manufacturas e industria a posiciones de técnicos y profesionales en el sector servicio. La mayoría de la nueva fuerza laboral se consagra el trabajo de conocimiento (trabajo simbólico), en tanto que las industrias de mayor crecimiento son las empresas dedicadas a la información intensiva.[157]

---

[155] De Paladella Salord Carlos. "Derecho en la era digital. Aspectos jurídicos de las nuevas tecnologías dela información y de las comunidades (Parte II)". Web. http// comunidad. Derecho. Org. /carlospaladella/ Director de Derecho Org. Argentina (España) Pág. 25.

[156] Ob. Cit. Téllez Valdes Julio. Derecho Informático. Pág. 109.

[157] Perez Marayo Guillermo Augusto. Derecho, Tecnología y Cambio. Pág. 5.

Las empresas apoderan a sus empleados con nuevas herramientas para manipular la información, recuperarla y disponerla de manera tal que permita a la organización una reacción más rápida ante la crisis y la oportunidad. Con el apoderamiento desaparece la necesidad de los mandos medios. La información agrega valor a la empresa y esta introduce conocimiento a sus productos (muchos de estos son símbolos o herramientas para trabajar con símbolos). En la economía digital, la naturaleza del trabajo se transforma; contrario al trabajo individualista de hoy día, se trabaja en grupo por medio de redes (Internetworking) y se trabaja compartiendo la información, por lo que se habla de la era de la inteligencia compartida en la red.[158]

Surgen nuevas fórmulas de trabajo, como el trabajo en casa, los trabajos de horarios flexibles y el compartido. Algunas empresas, por necesidad, deben contratar trabajadores por solo una ocasión y para labores especificas de conocimiento, que por lo esporádico del trabajo no amerita a tiempo completo; esta nueva forma de trabajo se conoce como outsourcing.[159]

Es indiscutible como lo hemos visto que el creciente uso de los medios informáticos ha sido de gran trascendencia para la humanidad, convirtiéndose en un factor económico, social y político en beneficio de la comunidad mundial, así como un medio imprescindible de trabajo, bienestar y de supervivencia. Sin embargo también a dado pauta a que estos medios sean utilizados en forma ilícita, llevándonos a enfrentar nuevas formas de cometer delitos por medio de una computadora o utilizando esta para dichos fines.

Desafortunadamente, con el crecimiento de los usuarios también aumentan los delincuentes. Este mundo virtual es campo fértil para los delitos perpetrados a distancia, no fáciles de prevenir, no de probar ni de perseguir. Lo cierto es que las pérdidas que producen son millonarias, superando ampliamente los delitos comunes.[160]

---

[158] Idem. Pág. 5.
[159] Idem. Pág. 5.
[160] Ob. Cit. Figoli Pacheco Andrés J. El acceso No Autorizado a Sistemas Informáticos. Pág. 1.

Por lo que tocaremos todo lo referente de los delitos informáticos, como punto medular de este trabajo de investigación.

2.3. DELITOS INFORMÁTICOS.

En los albores del nuevo milenio, podríamos decir que el siglo XXI ya ha comenzado con la llamada "revolución digital", la cual ha tomado forma mediante un complejo y laberíntico entramado de cables, satélites, redes, computadoras, televisores e impulsos eléctricos que constituyen la infraestructura del cyberespacio. Esta revolución, que encuentra en el Internet su máxima expresión, es posible gracias al fenómeno de la convergencia, es decir, al uso combinado de las computadoras y redes de comunicación.

Los efectos de transformación, se están sintiendo en la economía, la política, la educación y el entretenimiento. La forma en que nos interrelacionamos con los demás está siendo realizada por nuevas prácticas (compras on-line, chats. e-mail, educación a distancia, foros de discusión, etc.) y nadie puede ser capaz de predecir exactamente cuán profundos serán los cambios.

Lo que sí parece ser notorio es que el cambio debe ocurrir simultáneamente en todos los ámbitos a fin de lograr un proceso de transición armonioso. Basta con ver hacia atrás, en especial los efectos negativos que tuvo el salto de la era agrícola a la industrial, para comprender el porqué nos preocupa tanto. En esta era digital o de la informática, las instituciones, las normas, las leyes, las costumbres, y las formas de pensar, pareciera que ya resultan inadecuadas e inapropiadas, por lo que necesitamos urgentemente revisar y actualizar dichos rubros en aras de un fin común.

Además, nos queda muy claro todos los beneficios que conlleva la revolución digital, sin olvidar que también se abre un nueva forma para realizar conductas ilícitas.

Cualquiera de nosotros puede ser víctima de un delito, tanto en el mundo "real", como en el "virtual". Sin embargo, parecería que las conductas ilícitas realizadas en éste último gozan de cierta impunidad. Por la falta adecuada de leyes que regulen estas conductas.

2.3.1. DIVERSAS DEFINICIONES SOBRE EL DELITO INFORMÁTICO.

El ***delito informático*** implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho. [161]

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

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que JULIO TÉLLEZ VALDES señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún". [162]

---

[161] Peña Helen, Palazuelos Silvia, Alarcón Rosalía. Delitos Informáticos. División de Estudios de Posgrado, Facultad de Derecho. UNAM 21 de mayo de 1997. Servidor de la Universisad Autonoma de Sinaloa. México 1997. (Web. http// www. Yahoo.com) Pág. 1.

[162] Ob. Cit. Téllez Valdes Julio. Derecho Informático. Pág. 103.

Para CARLOS SARZANA, en su obra Criminalista e tecnologia, 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". [163]

LIDIA CALLEGARI define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas". [164]

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". [165]

MARÍA DE LA LUZ LIMA dice que el "delito electrónico " "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[166]

---

[163] Salazar Carlos. "Criminalità e Tecnología", Computer Crimes, Rasagna Penitenzíaria e criminología Nos. 1-2. Anno 1, Gennaio- Giugno, 1979, Roma, Italia, Pág. 59. Según cita de Téllez Valdes Julio. Pág. 104.

[164] Callegari, Lidia. "Delitos Informáticos" y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio- agosto-septiembre de 1985. Pág. 115. Según cita de Peña Helen, Palazuelos Silvia, Alarcón Rosalía. Delitos Informáticos. Pág. 2.

[165] Fernandez Calvo, Rafael. "El tratamiento del llamado "delito informático" en el proyecto de la Ley Orgánica del Código Penal: reflrexión y propuesta de la CLI (Comisión de libertades e informática y Derecho) Pag. 1150. Según cita de Peña Helen, Palazuelos Silvia, Alarcón Rosalía. Pág. 2.

[166] Lima de la Luz, María. Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Edt. Porrúa. No. 1-6 AñoL. Enero- Junio 1984 Pág. 100.

Nuevamente JULIO TÉLLEZ VALDES conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a " las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin". [167]

La Universidad de México ha realizado un estudio y define a los delitos informáticos como: todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático. [168]

JIJENA LEIVA lo define como Toda acción 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.[169]

La Organización para la Cooperación Económica y el Desarrollo (OECD) da una definición que es considerada como "abarcante" y lo define como: "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos".[170]

DIRK HANSON, establece que el delito informático es una forma de irrumpir y penetrar en los que las herramientas del ladrón, son en esencia un conocimiento de la estructura lógica o los puntos lógicos débiles inherentes a un sistema particular de la programación y proceso. Mas allá de un conocimiento profundo de programación, las únicas

[167] Ob. Cit. Téllez Valdes Julio. Pág. 104.
[168] Ob. Cit. Peña Helen. Palazuelos Silvia, Alarcón Rosalía. Delitos Informáticos Pág.3.
[169] Jijena Leiva, Renato Javier: "La Criminalidad Informática": Situación de Lege Data y Lege Ferende en Chile. Actas de III Congreso Iberoamericano de Informática y Derecho". Médira España. Según cita Viega Rodríguez María José. Doctora en Derecho y Ciencias Sociales. Escribana Pública. Integrante del CINADE (Centro de Investigaciones de Informática aplicada al Derecho). Facultad de Derecho de la Universidad de la República. (Uruguay). " Delitos Informáticos". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. (www.yahoo.com). Pág. 1.
[170] Ob. Cit. Viega Rodríguez María José. Delitos Informáticos. Pág. 1.

herramientas que el forajido necesita son una terminal de computadora y teléfono, no tiene que acercarse en absoluto al escenario del crimen.[171]

El delito informático es conveniente delimitarlo jurídicamente en forma inicial definiéndolo como "la realización de una acción que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea de hardware y software". [172]

Por ello podemos decir que los Delitos Informáticos son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese 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, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.[173]

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

Al respecto podemos ver los diferentes términos que toman, para definir a este tipo de delitos entre los que podemos destacar:

---

[171] Amoroso Fernández Yarina, Algunos problemas puntuales. Experiencias legislativas y jurisprudenciales en laitnoamérica. Informática y Derecho. Revista Latinoamericana de Derecho Informárico VOL. II UNED, Centro Regional de extremadura, Medira, España, 1998. Según cita de Riestra Gaytán Emma. Pág. 30.

[172] Nuñez Ponce Julio. Catedratico de Derecho Informático en la Universidad de Lima.(Perú) " Los delitos informáticos". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. (www.yahoo.com). Pág. 1.

[173] Líbano Manzur Claudio. Abogado Profesor. Director Secretario Ejecutivo de la Asociación de Derecho Informático de Chile (ADI-CHILE) "Los Delitos de Hacking en sus Diversas Manifestaciones". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. (www.yahoo.com). Pág. 1.

a) Delincuencia informática.

La define GÓMEZ PERALS como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos. [174]

b) Criminalidad informática.

ALESTUEY prefiere hablar de "delincuencia o criminalidad informática". [175]

BAÓN RAMÍREZ define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad). [176]

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.[177]

---

[174] Gómez Perals, Miguel. "Los Delitos Informáticos en el Derecho Español", Informática y Derecho nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi, págs. 481 a 496. Según Cita Cuervo Alvarez José. Abogado, especializado en temas de Derecho Informático. (España) " Los delitos informáticos: protección penal de la intimidad". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. (www.yahoo.com).Pág. 3.

[175] Alestuey Dobón, María del Carmen. "Apuntes sobre la perspectiva criminológica de los delitos informáticos", Informática y Derecho nº; 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. Según Cita Cuervo Alvarez José.Pág. 3.

[176] Baón Ramírez, Rogelio. "Visión general de la informática en el nuevo Código Penal", en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, págs. 77 a 100. Según cita de Cuervo Alvarez José.Pág. 3.

[177] Tiedemann, Klauss. "Poder económico y delito", Barcelona, 1985. Idem..Pág. 3.

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. [178]

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. [179]

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.

[178] Romeo Casabona, Carlos María. "Los llamados delitos informáticos", Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995. Idem. Pág. 4.
[179] Davara Rodríguez, Miguel Ángel. "Manual de Derecho Informático", Editorial Aranzadi, Pamplona, 1997, págs. 285 a 326. Idem. Pág. 4.

d) Computer crimen.

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

e) Delincuencia de cuello blanco.

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

Para SUTHERLAND la delincuencia de cuello blanco es la violación de la ley penal por una persona de alto nivel socio-económico en el desarrollo de su actividad profesional.[180]

f) Abuso informático.

RUIZ VADILLO recoge la definición que adopta el mercado de la OCDE en la Recomendación número R(81) 12 del Consejo de Europa indicando que abuso informático es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos. [181]

La misma definición aporta CORREA incidiendo en la Recomendación (89) 9,. del Comité de Ministros del Consejo de Europa considerando que la delincuencia informática suele tener carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es

[180] Ob. Cit. Cuervo Alvarez José. Delitos Informáticos. Pág. 4.

[181] Ruiz Vadillo, Enrique. "Responsabilidad penal en materia de informática", Informática y Derecho nº 9,10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996, págs. 443 a 460.Según cita de Cuervo Alvarez José. Pág. 4.

necesario llevar a cabo una armonización más intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el ordenador. [182]

2.3.2. CLASIFICACIÓN DE LOS DELITOS INFORMATICOS.

De igual forma los delitos informáticos han sido objeto de múltiples clasificaciones entre las cuales tenemos a:

JULIO TÉLLEZ VALDES, quien clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio, o como fin u objetivo.

1. Como instrumento o medio.

    - Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.

2. Como fin u objetivo.

    - En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.[183]

MARÍA DE LA LUZ LIMA, presenta una clasificación, de lo que ella llama "*delitos electrónicos*", diciendo que existen tres categorías, a saber:

---

[182] Idem. Pág. 5.
[183] Ob. Cit. Delitos Informáticos. Pág. 105.

1. Los que utilizan la tecnología electrónica como método,
2. Los que utilizan la tecnología electrónica como medio y
3. Los que utilizan la tecnología electrónica como fin.

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

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

Como fin. Conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla. [184]

JORGE PACHECO KLEIN distingue:

1.- Delitos informáticos internos: Ej.: sabotaje de programas.
2.-Delitos a través de telecomunicaciones. Ej.: hacking.
3.- Manipulación de computadoras. Ej.: apropiación indebida, peculado y fraudes informáticos. Es la más vinculada a delitos de cuello blanco.
4.- Utilización de computadoras en apoyo a empresas criminales, como el lavado de dinero y la distribución ilícita de drogas.
5.- Robos de sftware (pirateria). [185]

[184] Ob. Cit. Lima de la Luz, María. "Delitos Electrónicos" Pág. 5.
[185] Pacheco Klein, Jorge. "Introducción a los delitos informáticos en el ciberespacio. Normas y Jurisprudencia comentada. Según cita Viega Rodríguez María José. Delitos Informáticos. Pág. 3.

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.

Según BARRIUSO RUIZ los podemos clasificar en:

1. Delitos contra la intimidad.
2. De los robos.
3. De las estafas.
4. De las defraudaciones.
5. De los daños.
6. Relativo a la protección de la propiedad industrial.
7. Relativos al mercado y a los consumidores. [186]

De acuerdo con PÉREZ LUÑO podemos hacer la siguiente clasificación: [187]

a) Desde el punto de vista subjetivo.

Ponen el énfasis en la pretendida peculiaridad de los delincuentes que realizan estos supuestos de criminalidad

[186] Barriuso Ruiz, Carlos. "Interacción del Derecho y la informática", Dykinson, Madrid, 1996, págs. 245 a 252. Según cita de Cuervo Alvarez José. Pág. 5.
[187] Pérez Luño, Antonio-Enrique. "Manual de informática y derecho", Editorial Ariel S.A., Barcelona, 1996, págs. 69 a 81. Según cita de Cuervo Alvarez José. Pág. 6.

b) Desde el punto de vista objetivo.

Considerando los daños económicos perpetrados por las conductas criminalistas sobre los bienes informáticos:

- Los fraudes.

Manipulaciones contra los sistemas de procesamiento de datos. Podemos citar:

- Los daños engañosos (Data diddling).
- Los "Caballos de Troya" (Troya Horses).
- La técnica del salami (Salami Technique/Rounching Down).
- El sabotaje informático:
  - bombas lógicas (Logic Bombs).
  - Virus informáticos.
- El espionaje informático y el robo o hurto de software:
- Fuga de datos (Data Leakage).

El robo de servicios:

- Hurto del tiempo del ordenador.
- Apropiación de informaciones residuales (Scavenging).
- Parasitismo informático (Piggybacking).
- Suplantación de personalidad (impersonation).

El acceso no autorizado a servicios informáticos:

- Las puertas falsas (Trap Doors).
- La llave maestra (Superzapping).
- Pinchado de líneas (Wiretapping).

c) Funcionales

La insuficiencia de los planteamientos subjetivos y objetivos han aconsejado primar otros aspectos que puedan resultar más decisivos para delimitar la criminalidad informática.

Atentados contra la fase de entrada (input) o de salida (output) del sistema, a su programación, elaboración, procesamiento de datos y comunicación telemática.

Para BAÓN RAMÍREZ dentro de la criminalidad informática podemos distinguir dos grandes grupos de delitos: [188]

Un primer grupo se refiere a los delitos que recaen sobre objetivos pertenecientes al mundo de la informática. Así distinguiremos los delitos:

- Relativos a la destrucción o sustracción de programas o de material,
- Relativos a la alteración, destrucción o reproducción de datos almacenados,
- Los que se refieren a la utilización indebida de ordenadores,

En un segundo grupo se encuadraría la comisión de los delitos más tradicionales como los delitos contra:

- La intimidad,
- La propiedad,
- La propiedad industrial o intelectual,
- La fe pública,

[188] Ob. Cit. Baón Ramírez, Rogelio. "Visión general de la informática en el nuevo Código Penal", Según cita de Cuervo Alavarez. Pág. 7.

- El buen funcionamiento de la Administración,
- La seguridad exterior e interior del Estado.

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: [189]

- 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,
- Agresiones a los sistemas o elementos informáticos.

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. [190]

SIEBER hace una clasificación que responde no sólo a un criterio sistematizador vinculado a las características del procesamiento automático de datos, sino al mismo

[189] Romeo Casabona, Carlos María. "Poder informático y seguridad jurídica. La función tutelar del Derecho Penal ante las Nuevas Tecnologías de la información" ,FUNDESCO, Colección impactos, Madrid, 1987, págs. 25 a 34. Idem. Pág. 8.
[190] Ob. Cit. Cuervo Alvárez Jose. Pág. 8.

tiempo a una separación de diversos tipos criminológicos de conducta. Las conductas más significativas desde esta perspectiva podrían agruparse en estas cinco modalidades principales: [191]

a) Manipulaciones de datos y/o programas, o "fraude informático",
b) Copia ilegal de programas,
c) Obtención y utilización ilícita de datos, o "espionaje informático",
d) Destrucción o inutilización de datos y/o programas, o "daños o sabotaje informático" y
e) Agresiones en el hardware o soporte material informático, principalmente "hurto de tiempo del ordenador".

Por último, siguiendo a DAVARA RODRÍGUEZ dentro de un apartado en el que incluye "La informática como instrumento en la comisión de un delito", distingue dentro de la manipulación mediante la informática dos vertientes diferentes: [192]

a) Acceso y manipulación de datos y
b) Manipulación de los programas.

Atendiendo a ello, considera que determinadas acciones que se podrían encuadrar dentro de lo que hemos llamado el delito informático, y que para su estudio, las clasifica, de acuerdo con el fin que persiguen, en seis apartados:

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,

[191] Idem. Pág. 9
[192] Ob. Cit. Davara Rodríguez, Miguel Ángel. "Manual de Derecho Informático" Idem. Pág. 9.

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 persona, 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.

También encontramos una clasificación por las conductas informáticas ilícitas[193].

a) Intercepción de comunicaciones sin autorización.
b) Aprovechamiento de sistematización de la información contenida en bases de datos de sistemas o equipos de informática.
c) 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)
d) 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.
e) Difusión, distribución y reproducción mediante sistemas o equipos de informática de información relativa a la pornografía infantil (corrupción de menores) y lenocinio.
f) Difusión, distribución y reproducción mediante o no sistemas o equipos de informática de información (sofware) contenida en otros sistemas informáticos, lo que actualmente se concibe como fraude informático, espionaje industrial.
g) Aprovechamiento indebido o violación de un código para penetrar un sistema introduciendo instrucciones inapropiadas.

[193] Ob. Cit. Riestra Gaytán Emma. Págs. 37-38.

h) Negación de acceso si autorizado a sistemas y equipos de informática.
i) Abuso y daño de información en introducción falsa de información al sistema o equipo informático.
j) Copiar y distribuir programas de cómputo en equipos o sistemas informáticos.

Por otro lado al hablar de un delito, no podríamos omitir a los sujetos que intervienen en los mismos como son:

a) Sujeto Activo.

Las personas que cometen los "*Delitos Informáticos*" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

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

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

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "*delitos informáticos*", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano EDWIN SUTHERLAND en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros".[194]

Entre las características en común que poseen el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Por lo que en el capitulo siguiente hablaremos del Sujeto Activo con el objeto de aportar un estudio más profundo, así como detallar todos los aspectos que encierra este tema.

b) Sujeto Pasivo.

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

[194] Ob. Cit. Peña Helen, Palazuelos Silvia, Alarcón Rosalía. Delitos Informáticos. Pág.9.

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

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

De igual manera al hablar de un delito informático es importante saber cual es el ***Bien Jurídico Tutelado.***

Siendo este el honor, la intimidad, la propiedad, la fe pública, la seguridad, la información. Y de igual forma se puede plantear en extremos factibles incluso la vida o la integridad física. Pudiendo llegar a ser bienes jurídicamente tutelables al sancionar tipos informáticos.

También es importante señalar que ***elementos integran*** a un delito informático.

DIEGO CASTRO FERNANDEZ, comenta la existencia de dos tipos de elementos en estos casos. [195]

[195] Cfr.Castro Fernández Diego, "El delito informático" Revista Jurídica número 41 en San Jose, Costa Rica.

El elemento objetivo, la acción, tanto la que afecta los componentes de la computadora (hardware y software), como medio o instrumento para perpetrar el delito, así como la consumación de un acto ilícito autónomo como es el uso indebido y sin autorización de una computadora (robo de tiempos).

El elemento subjetivo de la conducta, consistente en el dolo, culpa o preterintención en la comisión del delito.

DAVARA RODRÍGUEZ, señala que si bien es cierto que no son delitos determinadas actuaciones dolosas realizadas por medios informáticos, lo cierto es que a través de estos medios existe la posibilidad de causar un mayor daño o mal, atentando en mayor medida contra el bien jurídico protegido. De esta forma, se puede hablar, no solamente del delito informático, sino también de circunstancias modificativas de la responsabilidad criminal.[196]

Otro aspecto muy importante es la **tipificación** del delito informático.

Destacando que la tipificación de estos delitos se ha dado acorde a las necesidades de los sistemas jurídicos, políticos y sociales de cada uno de los países que han regulado la prevención, regulación y sanción de los delitos informáticos, tomando en cuenta los requisitos y los elementos necesarios para su acreditación y sanción.

El Derecho Penal, siempre se ha dado a la tarea de regular aquellas conductas que son sancionadas como delitos, pero además tiende la necesidad de actualizar sus figuras jurídicas, al tipificar nuevas conductas que son cometidas con o por computadoras y que traen como consecuencias sociales, económicas y políticas. Y que vemos plasmados en los diversos ordenamientos jurídicos de muchos países.

[196] Davara Rodríguez, Miguel Angel. Derecho Informático. Edit. Aranzadi. Pamplona, España. 1993.

Podemos generalizar una enumeración que se ha realizado de los diversos tipos[197] de delitos informáticos que se conocen.

1) Robos, hurtos, vaciamientos, desfalcos, estafas o fraudes cometidos mediante manipulación y uso de computadoras.

a) Manipulación de los datos de entrada - insiders.

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

b) La manipulación de programas.

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

[197] Ob. Cit. Viega Rodríguez María José. Delitos Informáticos. Pág.4.

c) Manipulación de los datos de salida - outsiders.

El caso de manipulación más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, sin embargo, hoy en día se usan equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

d) Fraude efectuado por manipulación informática. Técnica del Salami.

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salami" en la que cantidades de dinero muy pequeñas, se van sacando repetidamente de una cuenta y se transfieren a otra. Esta modalidad de fraude informático se realiza sin grandes dificultades y es muy difícil de detectar. Uno de los casos más ingeniosos en el "redondeo hacia abajo", que consiste en una instrucción que se le da al sistema informático para que transfiera a una determinada cuenta los centavos que se descuenten por el redondeo.

2) Fraudes contra sistemas, daños o modificaciones de programas o datos computarizados.

a) Sabotaje informático.

Consiste en borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

b) Los Virus.

Un virus es un programa que puede ingresar en un sistema a través de cualquiera de los métodos de acceso de información externa, se instala, se reproduce y causa daño. La gravedad de los virus es variable, puede ser simplemente una molestia en la pantalla, como el caso del "ping-pong" y también existen aquellos que pueden llegar a eliminar el contenido de una base de datos.

Entre los virus más conocidos tenemos, a modo de ejemplo:

- ping-pong: consiste en un punto que se mueve por toda la pantalla y parece rebotar en los bordes.
- Datacrime o virus del viernes 13: el virus Jerusalem estaba destinado para destruir todas las memorias militares y científicas de Israel el 13 de mayo de 1988.
- Michelangelo: este último de fama más reciente.

Actualmente existe una gran carrera entre aquellos que crean los virus y los que desarrollan los antivirus. Hasta ha llegado a decirse que los virus son desarrollados por los mismos productores de antivirus, ya que hoy en día es fundamental adquirir antivirus y los mismos deben ser renovados constantemente, por supuesto que no existe ninguna prueba concreta.

c) Gusanos.

Se fabrica de forma análoga al virus, se infiltra en los programas ya sea para modificar o destruir los datos, pero se diferencia de los virus porque no pueden regenerarse. Las consecuencias del ataque de un gusano pueden ser graves, por ejemplo un programa gusano puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego se destruya.

d) Rutinas cáncer.

GUIBOURG las define como aquellas que "distorsionan el funcionamiento del programa y se autorreproducen al estilo de las células orgánicas alcanzadas por un tumor maligno".[198]

e) Bomba lógica o cronológica.

Consiste en la introducción en un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha o circunstancia, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo.

Las bombas lógicas son difíciles de detectar antes de que exploten, son las que pueden resultar más dañinas y prever que exploten cuando el delincuente ya se encuentre lejos. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla.

f) Acceso no autorizado a Sistemas o Servicios.

Puede darse por motivos diferentes: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático. Estos ingresos no autorizados comprometen la integridad y la confidencialidad de los datos. Podríamos llegar hasta actos de atentados terroristas, por ejemplo en el caso de intervenir sistemas de tráfico aéreo.

[198] Guibourg, Ricardo. "Manual de Informática Jurídica" Según cita de Viega Rodríguez María José. Delitos Informáticos. Pág.7.

g) Espionaje - Acceso telemático no autorizado a un sistema - Hackers - Fuga de datos.

El acceso puede darse en forma directa, por ejemplo cuando un empleado accede en forma no autorizada, estamos frente a un riesgo interno. Pero se puede acceder en forma indirecta, o sea a través de una terminal remota.

El delincuente puede aprovechar la falta de medidas de seguridad para obtener acceso o puede descubrirle las deficiencias a las medidas existentes de seguridad. A menudo, los hackers se hacen pasar por usuarios legítimos del sistema, esto suele suceder debido a la frecuencia en que los usuarios utilizan contraseñas comunes.

La fuga de datos consiste en la versión informática de las tradicionales prácticas de "espionaje industrial".

El acceso no autorizado a sistemas informáticos reviste diversas modalidades, que son:

- Puertas falsas. Se trata de intromisión indebida a los sistemas informáticos aprovechando los accesos o "puertas" de entrada, que no están previstas en las instrucciones de la aplicación, pero que facilitan la revisión o permiten recuperar información en casos de errores de sistemas. También llamadas "puertas trampa" porque permiten a los programadores producir rupturas en el código y posibilitar accesos futuros.

- Llave maestra (Superzapping). Consiste en el uso no autorizado de programas para modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático. El nombre proviene de un programa de utilidad que se llama superzap, que permite abrir cualquier archivo de una computadora aunque se halle protegido por medidas de seguridad.

- Pinchado de líneas. Se realiza a través de la interferencia de las líneas telefónicas o telemáticas a través de las cuales se transmiten las informaciones procesadas en las bases de datos informáticas.

h) Reproducción no autorizada de programas informáticos - Piratería.

"Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual."[199]

3) Falsificaciones Informáticas.

Como objeto.

Es cuando se alteran datos de documentos que se encuentran almacenados en forma computarizada. Pueden falsificarse o adulterarse también microformas, microduplicados y microcopias; esto puede llevarse a cabo en el proceso de copiado o en cualquier otro momento.

Como instrumentos.

Las computadoras pueden utilizarse para realizar falsificaciones de documentos de uso comercial. Las fotocopiadoras computarizadas en color a base de rayos láser dio lugar a nuevas falsificaciones. Estas fotocopiadoras pueden hacer copias de alta resolución, modificar documentos, crear documentos falsos sin tener que recurrir a un original, y los

[199] Pérez Luño, Antonio. "Manuel de informática y derecho. Ariel Derecho. Según cita de Viega Rodríguez María José. Delitos Informáticos. Pág.8.

documentos que producen son de tal calidad que solo un experto puede diferenciarlos de los documentos auténticos.

4) Datos personales. Delito de violación a la intimidad.

Consiste en la violación de la intimidad de la vida personal y familiar ya sea observando, escuchando o registrando hechos, palabras, escritos o imágenes, valiéndose de instrumentos, procesos técnicos u otros medios.

También se podría tipificar como delito el que organiza, proporciona o emplea indebidamente un archivo que tenga datos referentes a las convicciones religiosas, políticas o a la vida íntima de las personas.

5) Homicidio.

Aunque no parezca creíble es posible cometer homicidio por computadora. Se daría en los casos en que a un paciente que está recibiendo un determinado tratamiento, se modifican las instrucciones en la computadora, que puede hacerse incluso desde una terminal remota.

6) Interceptación de comunicaciones (browsing).

Mediante la conexión en paralelo de terminales no autorizadas se puede acceder a datos e incluso manipular la información.

7) Robo de servicios.

a) Robo de servicios o Hurto de tiempo de ordenador. Cuando los empleados utilizan en una empresa horas de máquina sin autorización para realizar trabajos personales. Hoy en día este tipo de delito ha caído en desuso, ya que con la existencia de las PC y lo que ha bajado su costo, resulta sencillo tener acceso a una computadora, pero

esto no era así hace unos años cuando las grandes computadoras eran propiedad de las empresas debido al alto costo de las mismas.

b) Apropiación de informaciones residuales, que han sido abandonadas por sus legítimos usuarios de servicios informáticos como residuo de determinadas operaciones.

c) Parasitismo informático. Se alude a las conductas que tienen por objeto el acceso ilícito a los equipos físicos o a los programas informáticos, para utilizarlos en beneficio del delincuente. Suele asociarse a esta figura la de la Suplantación de personal que se refiere a toda la tipología de conductas en las que los delincuentes sustituyen a los legítimos usuarios informáticos. Un ejemplo es él referente al uso ilícito de tarjetas de crédito.

8) Hurto calificado por transacciones electrónicas de fondos.

Este es el caso del hurto que se comete mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o también cuando se viola el empleo de claves secretas. Este es un delito tipificado en otros países, que en la doctrina y legislación comparada está tipificado como fraude informático.

9) Delitos de daño aplicable al hardware.

El robo de un establecimiento comercial de una o varias computadoras no constituye un delito informático, pero sí el daño o sabotaje al hardware que impide la puesta en marcha de un sistema informatizado de diagnóstico médico. Este tipo de delitos está pensado para bienes materiales y no inmateriales.

2.3.3. LEGISLACIÓN DE OTROS PAISES EN RELACION A LOS DELITOS INFORMATICOS.

Se ha visto que en muchos de los casos de abusos relacionados con la informática son combatidos con adecuaciones a los ordenamientos jurídico-penales. No obstante, de las medidas preventivas que sean tomado.

En los Estados industriales como Europa y Norte America existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años.

Pocos son los países que disponen de una legislación adecuada para enfrentar los problemas informáticos, sin embargo con objeto de enriquecer nuestros conocimientos, presentamos algunas de las legislaciones que contemplan a los delitos informáticos.

a) Alemania.

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

- Espionaje de datos (202 a).
- Estafa informática (263 a).
- Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).
- Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Sabotaje informático (303 b) destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b).

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

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

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

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

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

b) Austria.

En este caso la Ley de reforma del Código Penal de Austria de fecha 22 de diciembre de 1987, contempla los delitos de:

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

- 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. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

En igual sentido, en este país, se pronunciaron disposiciones jurídicas de mayor rango, aprobadas durante las décadas de los 70´s y 80´s. En donde se establecieron sanciones de multa y de privación de libertad hasta un año, para los incumplidores de las disposiciones relacionadas con la obtención, almacenamiento y procesamiento de datos por medios informáticos.

c) Francia.

También Francia retoma en su Ley número 88-19 de fecha 5 de enero de 1988, al fraude informático.

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

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

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

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

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

d) Estados Unidos.

Es importante mencionar la adopción que hace 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.

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

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

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

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

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

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

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

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

e) Inglaterra.

Es otro país en donde su Ley Computer Misuse Act del año 1990, introdujo el delito de acceso no autorizado. Dice PACHECO KLEIN que: "Esta cláusula de la ley fue, principalmente, una reacción a la publicidad y al medio en torno a los virus de las computadoras. El artículo 3º inciso 2º establece que la persona tiene que tener intención de "modificar el contenido de cualquier computadora", y de esa manera:

a) Impedir la operación de cualquier computadora; o
b) Impedir o dificultar el acceso a cualquier programa, o la confianza de esos datos.

d) Impedir la ejecución de cualquiera de esos programas, o la confianza en esos datos."[200]

La Ley fue criticada por su amplitud, sin embargo la obtención de evidencia desde lugares remotos ha creado problemas en la legislación inglesa.

En 1994 la Ley fue reformada para permitir el acceso a la policía y a las agencias especializadas del orden a los boletines informativos.

f) España.

País que ha tenido avances significativos, sobre la regulación de los sistemas informáticos en su Constitución como la protección de un derecho fundamental[201]. Así como su respectiva actualización a su Ley Penal y la regulación de conductas por medio de Ley Orgánica de Protección y Seguridad de Datos, además de la Ley Orgánica 10/1995 del Código Penal.

El honor y la intimidad de las personas son derechos fundamentales para su ordenamiento jurídico, tal como queda recogido en el artículo 18 de la Constitución Española[202], y como ocurre en la totalidad de los ordenamientos considerados democráticos en la actualidad.

---

[200] Ob. Cit. Viega Rodríguez María José. " Delitos Informáticos". Pág. 11.

[201] García Aguilar, Nicolás Licenciado en Informática. Diplomado en Derecho. Titulado Superior de Telefónica de España. Miembro de la Asociación de Licenciados en Informática (ALI) y de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI). (España) "La cuestión de la responsabilidad en el Derecho Informático". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. (www.yahoo.com). Págs. 1 y ss.

[202] Sánchez Goyanes Enrique "Constitución Española Comentada". 21ª Edición . Edt. Pararninfo. Madrid, España, 1998. Pág.259.

Precisamente este objetivo garantista que persigue el legislador español, al desarrollar el articulado de la norma fundamental en sucesivas leyes. Como señala CASTÁN al referirse a estos derechos, "son aquellos derechos fundamentales de la persona humana -considerada tanto en su aspecto individual como comunitario- que corresponden a ésta por razón de su propia naturaleza (de esencia, a un mismo tiempo, corpórea, espiritual y social) y que deben ser reconocidos y respetados por todo Poder o autoridad y toda norma jurídica positiva, cediendo, no obstante, en su ejercicio ante las exigencias del bien común", lo que nos muestra dos características esenciales de este tipo de derechos: su vocación de universalidad y su subordinación a los intereses generales, a pesar de su consideración como derechos subjetivos. Ambas características son manifiestas en la adaptación de la intimidad, como derecho fundamental especialmente protegido, por la legislación informática. [203]

De este derecho inicial a la intimidad la doctrina ha diseñado un derecho a la privacidad (lo que algunos autores han llamado derecho a la autodeterminación informativa) con el que se pretende no sólo rechazar cualquier intromisión a la vida privada de cada cual, sino también introducir mecanismos de control del sujeto afectado sobre las informaciones relativas a su persona o a su familia.

El esquema normativo de la protección de datos responde al esquema normativo típico, tal como señala LUCAS MURILLO : "se prohíbe una conducta amenazando con una sanción el incumplimiento de esa prohibición".[204] A partir de aquí, hablar de responsabilidad es evidente.

[203] Fernández-Galiano Antonio, De Castro Cid Benito;"Lecciones de Teoría del Derecho y Derecho Natural"; Ed. Universitas S.A., 1994 Pág. 423. Según cita de Garcia Aguilar Nicolas. Pág. 2.
[204] Murillo; Pablo Lucas. "El derecho a la autodeterminación informativa"; Edit. Tecnos, 1990 Pág. 117. Según cita de de Garcia Aguilar Nicolas. Pág. 2 y ss.

La Ley española de protección de datos, que desarrolla el mencionado artículo de la Constitución Española es principalmente la LORTAD, Ley Orgánica 5/1992[205], aunque existen otras normas, incluso anteriores, que vinculan a los ciudadanos y a los poderes públicos en lo referente a la protección de datos.

La LORTAD en su Exposición de Motivos (alineándose con las opiniones de algunos autores anglosajones) separa el concepto de intimidad del de privacidad superponiendo este último al mencionado artículo de la Constitución Española y dándole un sentido más acorde con las posibilidades deductivas del procesamiento informático, al considerar la privacidad como un conjunto de facetas de la personalidad del individuo potencialmente extraíbles de una serie de datos no necesariamente significativos, pero que quizás puedan emerger al quedar sometidas a un tratamiento automático.

Sin embargo, sí es cierto que al hablar de privacidad en lugar de intimidad se pretenden resaltar los peligros que se pueden derivar del tratamiento automatizado. Con la informática "lo que está en juego no es solamente la intimidad, sino la identidad del hombre y su propia libertad" [206].

Por otra parte, esta postura ya ha quedado patente con anterioridad a través de la doctrina formulada por el Tribunal Constitucional Español. Incluso, según conclusión de RUIZ MIGUEL, en la jurisprudencia emanada del propio Tribunal Europeo de Derechos Humanos se diferencian varios grados de intimidad dentro de la privacidad, teniendo ésta una mayor amplitud. [207]

[205] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal; BOE de 31 de octubre de 1992.
[206] Ob. Cit. Murillo, Pablo Lucas. Pág. 2 y ss.
[207] Ruiz Miguel, Carlos."El derecho a la protección de la vida privada en la jurisprudencia de Tribunal Europeo de Derechos Humanos"; Cuadernos Civitas, Ed. Civitas, 1994 Pág. 34. Según cita de García Aguilar Nicolas. Pág. 3.

La Exposición de Motivos de la LORTAD aclara que el ánimo de la ley es "implantar mecanismos cautelares que prevengan las violaciones de la privacidad que pudieran resultar del tratamiento de la información", para atribuir después a la Administración cierta potestad sancionadora complementaria a la reconocida por el Código Penal.

Así pues, junto a las sanciones de carácter civil, existirán las administrativas y las penales (éstas incluso podrán suponer privación de libertad). No obstante, y como señaló del PESO NAVARRO, el sistema de responsabilidad ha sido edificado principalmente en torno a la idea de indemnización [administrativa] como requisito para la reparación del daño. [208]

Señalando en su Artículo 1. Objeto.- La presente Ley Orgánica, es desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso e la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.[209]

La LORTAD comenzó por introducir dentro de su artículo 3 d), dedicado a las definiciones, el concepto de lo que llama "responsable del fichero" en relación directa con el artículo 2 d) del Convenio 108[210], aunque éste último nos habla de "autoridad controladora del fichero"; en ambos casos se refiere a la persona física o jurídica (pública o privada) que decide sobre la finalidad, contenido y uso del tratamiento del fichero. El paralelismo entre ambos textos legales no se detiene aquí (de hecho el citado Convenio sirvió de base para la elaboración de la LORTAD) independientemente de que aquél

[208] Del Peso Navarro, Emilio. "La responsabilidad civil del profesional informático"; Base Informática nº22, abril 1993. Pág. 46. Idem. Pág. 3.

[209] Legislación básica de informática. Edición preparada por Alvarez Rico Manuel, Catedrático de la Universidad Pontificia de Salamanca, Heredero Higueras Manuel, Doctor en Derecho, Abogado; Alvarez Rico Isabel, Universidad Poncificia de Salamanca, Facultad de Informática, Abogada. Madrid, Edit. Tecnos, S.A., Madrid. España 1999. Pág. 25

[210] Convenio núm. 108 del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; BOE de 15 de noviembre de 1985.

haya entrado a formar parte de dicho ordenamiento jurídico en virtud del artículo 96 CE y por lo tanto goce de un trato de aplicación preferente[211].

También el Convenio 108 admite la posibilidad (artículo 8 d) de que cualquier persona disponga de un recurso con el que hacer frente a determinados supuestos de responsabilidad de la autoridad controladora del fichero (tales supuestos se refieren a que la persona interesada controle sus datos personales ejercitando claramente su derecho a autodeterminarse informativamente, concretamente sobre las operaciones de confirmación, comunicación, ratificación o borrado de dichos datos).

Por otro lado, el artículo 10 del Convenio asegura el compromiso de cada parte para establecer las sanciones y los recursos convenientes, en clara relación con la depuración de responsabilidades. Finalmente, el artículo 26 considera la posibilidad de que una de las Partes denuncie a la otra por incumplimiento del Convenio.

Volviendo a la LORTAD, hay que mencionar que también toca artículos donde emerge la cuestión de la responsabilidad para la autoridad controladora del fichero.

En particular, se destacara que el artículo 7.5 (obligación de incluir en ficheros públicos los datos de carácter personal relativos a la comisión de infracciones penales o administrativas); el artículo 10 (deber de secreto profesional); el artículo. 12 (reconoce la posibilidad de que el afectado impugne los actos administrativos o decisiones privadas); el artículo 17 (tutela de los derechos por la Agencia de Protección de Datos -APD- y mención de la Ley 30/1992[212]; también reconoce la posibilidad de indemnización); el artículo 21.3 (intervención del Director de la APD o de los órganos competentes de las Comunidades Autónomas en determinados supuestos de ficheros responsabilidad de las Fuerzas y Cuerpos de Seguridad y de los de la Hacienda Pública); y también el artículo

[211] Pérez Royo, Javier. "Las Fuentes del Derecho" Ed. Tecnos. 1988 Pág. 164 y ss. Según cita de García Aguilar Nicolas. Pág. 3.

[212] Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común; BOE de 27 de noviembre de 1992.

25 (necesidad de comunicación de la cesión de datos por parte del responsable del fichero al afectado, referida específicamente a los ficheros de titularidad privada).

Finalmente, todo el Título VII de la LORTAD está dedicado a la cuestión de las infracciones y sanciones a que se verán sometidos los responsables de los ficheros por incumplimiento de sus funciones (mención especial cabe hacer del artículo 47, que emplaza al legislador a establecer por vía reglamentaria el procedimiento a seguir para la determinación de las infracciones y de las sanciones).

Hemos comentado la referencia de la LORTAD (artículo 17.4) a la Ley 30/1992, cuando establece que la responsabilidad para ficheros de titularidad pública se exigirá de acuerdo con la legislación reguladora para las Administraciones Públicas. El artículo 45 de la citada Ley 30/1992 consagra la utilización de medios técnicos por parte de las Administraciones Públicas (con especial referencia a la informática y a la telemática) para ocuparse en otro lugar (Títulos VIII, IX y X) de cuestiones referentes a la exigencia de responsabilidad de los organismos públicos.

Haremos también un breve comentario al RD 1332/1994[213] que desarrolla algunos preceptos cuyo contenido la LORTAD difería a la vía reglamentaria, como ya anunciamos en líneas anteriores al hablar del Título VII de la LORTAD. Cómo no, este RD toca ciertos aspectos referentes a la responsabilidad: artículo 3 (responsabilidad solidaria de cedente y cesionario en el régimen de transferencia internacional de datos); artículo 7 (inscripción de ficheros); el artículo 10 (recurso contencioso-administrativo contra el Director de la APD); artículo 16 (reclamación ante el Director de la APD por el bloqueo de los datos acordado por el responsable del fichero); artículo 17 (procedimiento de reclamación ante la APD); y finalmente el Capítulo V dedicado al procedimiento sancionador.

[213] Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la LORTAD; BOE de 21 de junio de 1994.

Por último mencionaremos la Ley 16/1993[214] que recoge para España la preocupación internacional sobre la protección jurídica de los programas de ordenador, considerando las infracciones que al respecto se puedan producir como ataques a los derechos de autor bajo la aplicación directa de la Ley 22/1987[215].

A todo esto podemos ver que los últimos avances relacionados con la protección de datos se tiene contemplado en la Ley Orgánica 15/999, del 13 de Diciembre, de Protección de Datos de Carácter Personal. (BOE núm298, de 14 de diciembre de 1999).[216]

También se señala que LA AGENCIA DE PROTECCION DE DATOS en su artículo 13 del Convenio 108 obliga a las partes a concederse asistencia mutua para lo que exige designar una autoridad en cada una de ellas. La LORTAD en su Título VI crea la APD, haciendo en el artículo 36.I referencia a la obligación impuesta por el Convenio 108.

Además del papel de la APD respecto al movimiento internacional de datos, es clara la misión de la Agencia en lo referente a la exigencia de responsabilidad: el citado artículo 36 (funciones de la APD); el artículo 38 (custodia del Registro General de Protección de Datos); el artículo 39 (responsabilidad de los funcionarios que ejercen la potestad de inspección en nombre de la APD); en fin, el artículo 41 (exigencia de responsabilidad por el Director de la APD a las Comunidades Autónomas).

El propio artículo 34.2 de la LORTAD prevé la creación de un Estatuto propio de la APD con el objetivo de completar la materia regulada. Este Estatuto fue efectivamente creado por RD 428/1993[217], completando como ya se ha dicho la citada LORTAD también en lo referente a la cuestión de responsabilidad: el artículo 12 (funciones del Director de la

[214] Ley 16/1993, de 23 de diciembre, de incorporación al Derecho español de la Directiva 91/250/CEE, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador; BOE de 24 de diciembre de 1993.
[215] Ley 22/1987, de 11 de noviembre, de Propiedad Intelectual; BOE de 17 de noviembre de 1987.
[216] Datos proporcionados por Miraut Martín Laura. En el curso Introducción a los Delitos Informáticos. "La Experiencia Española". Impartido en el Instituto Nacional de Ciencias Penales. Julio del 2000.
[217] Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos; BOE de 4 de mayo de 1993.

APD); el artículo 23 (Registro General de Protección de Datos); o finalmente, el artículo 27 (Inspección de datos).

Por otro lado tenemos que el 26 de octubre de 1995 se aprobó, por el pleno del Senado, la nueva Ley Orgánica del Código Penal 10/1995, de 23 de noviembre (B.O.E. número 281 de 24 de noviembre) que entró en vigor el 24 de mayo de 1996.

Al ser la tipicidad uno de los principios imprescindibles en materia penal era necesaria una regulación específica que permitiese enjuiciar las nuevas formas de delincuencia en un marco adecuado, ya que los nuevos delitos no recogidos en el anterior texto penal implicaban el riesgo de caer en la atipicidad, problema que la Jurisprudencia ha venido solucionando gracias a artificiosas construcciones, a veces muy lógicas, si bien otras un tanto forzadas.

Ya en la exposición de motivos del nuevo texto penal se reconoce la necesidad de introducir nuevas figuras delictivas para dar respuesta a las exigencias de la sociedad actual, provocando esta última también la desaparición o modificación de aquellas figuras, ya desfasadas, que habían perdido su razón de ser.

El ordenamiento ha deslindado la legislación específica penal, diferenciando la pena criminal de la sanción administrativa. El Código Penal[218] en su artículo 34.2 indica que no se reputarán penas "las multas y demás correcciones que, en uso de atribuciones gubernativas o disciplinarias, se impongan a los subordinados o administrados".

No obstante, no debe pensarse que es sólo norma penal la que se encuentra recogida en el Código Penal. También existe en el Derecho Español una legislación penal que recogiendo delitos y faltas, y que se encuentra fuera de las fronteras del Código Penal, reguladas por leyes especiales, a las que se aplican las disposiciones del Código Penal como supletorias, excepción hecha de las que figuran en el Título Preliminar "De las garantías penales y de la aplicación de la Ley Penal". Este fenómeno lo reconoce el

[218] Código Penal. Edición 2000. Edt. Biblioteca Nueva, Madrid. España. Pág. 41.

propio Código Penal en su artículo 9, al indicar que "Las disposiciones de este Título se aplicarán a los delitos y faltas que se hallen penados por leyes especiales. Las restantes disposiciones de este Código se aplicarán como supletorias en lo no previsto expresamente por aquéllas.

g) Portugal.

La Ley de Protección de Datos Personales Informatizados de 29 de abril de 1991, prevé en Portugal también penas de multa y privación de libertad para los que utilicen datos ilegalmente, consigan acceso no autorizado a las bases de datos, realicen interconexiones ilegales y otras conductas.

h) Perú.

El ordenamiento jurídico peruano tipifica los siguientes delitos, los cuales se encuentran dentro del concepto de delitos informáticos, y son:[219]

- Delito de violación a la intimidad (artículo 154 del Código Penal).
- Delito de hurto calificado por transferencia electrónica de fondos (artículo 186 segundo párrafo numeral 3 del Código Penal, modificado por Ley 16.319).
- Delitos contra los derechos de autor (artículo 216 Código Penal).
- Delito de falsificación de documentos informáticos (Decreto Legislativo 681, artículo 19 - artículo. 427 del Código Penal).
- Delito de fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos (artículo 198 inc. 8 del Código Penal).
- Delito de daños aplicable al hardware (artículo 205 del Código Penal) .

[219] Idem. Pág. 12.

l) Cuba.[220]

En Cuba, ya se han dado los primeros pasos en este sentido, con la promulgación de textos legales como el Reglamento de Seguridad Informática emitido por el Ministerio del Interior, en vigor desde Noviembre de 1996, y el Reglamento sobre la protección y seguridad técnica de los sistemas informáticos, emitido por el Ministerio de la Industria Sideromecánica y la Electrónica, también en vigor desde Noviembre de 1996.

Al inicio de 1989, se registraban 15 virus en el mundo, existiendo en la actualidad más de 8000. En Cuba han sido detectados, más de 125 virus, algunos de los cuales han sido hechos en Cuba, o especialmente para Cuba.

El Comité de Informática de la UNESCO hizo público, en ocasión de la XIV Conferencia de Autoridades Iberoamericanas de Informática, celebrada en La Habana del 13 al 18 de noviembre de 1995, un llamamiento acerca de los virus informáticos, en el que se exhortó a los gobiernos a tomar las medidas legales para que la creación y la distribución de virus informáticos fueran consideradas delitos y penadas por la ley; asimismo, se acordó que la ONU propusiera la implementación de una solución legal a este problema.

El vigente Código Penal o Ley No. 62 de 29 de diciembre de 1987, puesta en vigor el 30 de abril de 1988 y modificada por el Decreto Ley No. 150 de junio de 1994, reúne un conjunto de figuras que, tal como se encuentran redactadas, son aplicables a delitos cometidos en contra de los medios de computación o contra la información que en ellos se procesa o a delitos cometidos a través de dichos medios.

---

[220] Gómez Pérez, Mariana. Organización Nacional de Bufetes Colectivos. CUBA. Editora en jefe de Revista Electrónica de Estudios Jurídicos (CubaLex) (Cuba) "Criminalidad informática: un fenomeno de fin de siglo". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), (www.yahoo.com). Págs. 2, 7, 8-10.

Entre las conductas realmente nuevas nacidas de la interacción hombre-máquina, se encuentran las siguientes:

1. El creador de virus informáticos o programas destinados a realizar acciones con fines de lucro u otros.

2. El distribuidor de virus informáticos o de informaciones sobre la elaboración de programas con la intención de provocar daños.

3. El intruso o persona a la que no se autoriza el acceso a las redes de información electrónica y a los sistemas informáticos.

En la descripción hecha por el Código del delito de Sabotaje (artículos 104 y 105), se hace referencia al que se comete contra las fuentes de comunicaciones (inciso a) del artículo 104), entre las que podrían subsumirse las electrónicas. Habría que pensar que las acciones realizadas contra otras instalaciones pudieran efectuarse utilizando como medios las técnicas o equipos de computación.

Asimismo, en el caso del delito de Revelación de Secreto Administrativo, de la Producción o de los Servicios (artículos 129 al 131), la obtención ilegítima de un secreto administrativo de la producción o los servicios a la que se refiere el artículo 130, puede lograrse a través del uso de técnicas de computación, por ejemplo, mediante el acceso no autorizado a redes, conducta que en sí misma podría constituir otro delito.

El uso cada vez más generalizado de las técnicas informáticas en función de los planes sociales y económicos propicia, que dichas técnicas puedan ser utilizadas como medios para cometer también el delito previsto en el artículo 140, incisos a) y b), que engloba los actos en perjuicio de los planes económicos o la contratación estatal.

En el caso de la infidelidad en la custodia de documentos u otros objetos, la redacción del Código Cubano prevé la sustracción, alteración, ocultación, deterioro o destrucción de éstos. (artículo 168, apartados primero, segundo y tercero, literales a) y b) y artículo 169, apartados primero y segundo). En tales casos se refiere a los soportes magnéticos de la información, pues al sufrir los mismos cualquiera de estos daños, ello provocaría el mismo efecto sobre la información que contienen.

Puede suceder también que la información sea obtenida sin que se provoque daño alguno a los medios; como en definitiva se produciría el mismo efecto que quiere el legislador evitar (la pérdida o deterioro de la información), tal situación pudiera expresamente preverse en el articulado. Es el caso del apartado tercero del artículo 168 que recoge los daños provocados a los envíos de correspondencia postal o telegráfica. Cabría aquí agregar los daños a las informaciones que se envían a través del correo electrónico.

Asimismo, consideramos que, entre los artículos destinados a la protección de la economía nacional, el referido a la obligación de preservar los bienes de las entidades económicas estatales deberá incluir la preservación de los medios técnicos de computación (artículo 222).

En los casos de delitos contra la fe pública, como en los otros casos ya analizados de delitos en que entran en juego documentos, es necesario detenerse en punto a la teoría y la práctica de la validez del documento electrónico. Las alteraciones o falsificaciones de los datos contenidos en soporte magnético, pueden dar lugar a un documento que, aún cuando no presente signos evidentes que hagan presumir su falsedad, contenga datos inciertos.

Por otra parte, se tiene la falsificación de despachos de los servicios postales y telegráficos o de los transmitidos por las redes de comunicaciones, previsto y sancionado en el artículo 253, que alcanza una nueva dimensión con las transmisiones por redes electrónicas a las que pueden tener acceso múltiples personas, dadas las propias

características de estas redes y las facilidades de uso que proporcionan las modernas vías de comunicación puestas "al alcance de todos".

Por todo ello, sería muy difícil controlar, por ejemplo, la violación o la revelación del secreto de la correspondencia, previstos y sancionados en los artículos 289 Y 290, respectivamente, del Código Penal Cubano.

En cuanto al robo con fuerza en las cosas, previsto y sancionado en el artículo 328 del Código Penal, primeramente habría que definir qué se entenderá por fuerza, ¿violar el password?, cuando se trate de sustracción de información en las conocidas variantes, con copia o sin copia, de la información contenida en el soporte. Igualmente, será necesario determinar, en el caso de sustracción del soporte magnético duro - hard disk -, qué figura será la aplicable, si el robo con fuerza del artículo 328 o el hurto del artículo 322, toda vez que el hecho se puede cometer sin el empleo de fuerza, pero es indiscutible que tal conducta acarrearía un daño a la disponibilidad del equipo y a la integridad y disponibilidad de la información y, en definitiva, un incuestionable perjuicio.

j) Brasil.[221]

También, los autores brasileños acompañan la tendencia internacional que protege al "software" en el entendimiento de que es un derecho autoral. El legislador acepta esa posición. Por ello, la Ley 7.646, de 18 de Diciembre de 1987, define en sus artículos 35 y 37 dos delitos que expresan ese entendimiento:

Artículo. 35 - Violar derechos de autor de programas de ordenador: Pena: Detención, 6 (seis) meses a 2 (dos) años y multa.

[221] Rodrigues da Costa, Marco Aurélio. Abogado de Uruguaiana. (Brasil) "El Derecho Penal informático vigente en Brasil" El presente trabajo corresponde a una parte del ensayo publicado por el autor en Jus Navigandi ("Crimes de Informática"), traducción de Luis Miguel Reyna Alfaro, bajo autorización del autor. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), (www.yahoo.com). Págs. 1 y ss.

Artículo. 37- Importar, exportar, mantener en depósito, para fines de comercialización, programas de ordenador de origen externo no registrados: Pena: Detención, de 1 (un) año a 4 (cuatro) años y multa.

El sistema legal contempla ahora la protección contra los crímenes contra el orden económico y las relaciones de consumo. En el ámbito del orden tributaria, la Ley n. 8.137. de 27 de Diciembre de 1990, define una nueva forma de uso ilícito del ordenador, que sería la acción de utilizar o divulgar programas de procesamiento de datos que permita al contribuyente poseer información contable diversa que es, por ley, proporcionada a la Hacienda Pública, siendo penado con detención de seis meses a dos años y multa. Es pues, un programa de ordenador destinado a permitir un fraude fiscal.

Ante esa paupérrima legislación, el operador del derecho esta obligado a servirse de los delitos tradicionales para combatir los crímenes informáticos. Se tiene que muchas de las conductas que caracterizan los crímenes informáticos, podrían ser encuadradas en la figura típica del estelionato. La velocidad del desarrollo tecnológico en el sector de informática, no garantiza que se pueda, eternamente, mantener la aplicación del Código Penal Brasileño, o sea, la subsunción de los delitos comunes en las conductas típicas de los delitos informáticos. Súmese a esa dificultad presente, las diversas doctrinas y corrientes que pululan en materia de la criminalidad informática, es mas, las propias divergencias en torno a la aplicación del Derecho Alternativo es una corriente que defiende un programa de descriminalización, que origina profundas dificultades a los aplicadores del derecho.

La propuesta de nueva Parte Especial del Código Penal, que deberá ser presentada por el Ministerio de Justicia al Congreso Nacional, nos señala que, respecto a la tutela penal de los intereses y los bienes nuevos o redefinidos en su importancia por la Sociedad de Información Post-Industrial, se caracteriza por establecer un camino propio.

Los crímenes informáticos están contenidos en un Capítulo del Código Penal denominado como "Los Crímenes contra el Orden Socio-económico", de la Parte Especial del Código Penal. El precitado Capítulo consta de apenas ocho artículos. Tres de estos artículos tratan, específicamente, de los delitos informáticos, en tanto otros tres dispositivos tratan sobre la adecuación de las normas ya existentes a los bienes intangibles redefinidos en su importancia, otros dos tienen la finalidad de reprimir atentados considerados especialmente graves pará la privacidad de los individuos y perpetrados a través del computador.

k) Chile.[222]

En junio de 1993 entró en vigencia en Chile la Ley n°19.223, sobre delitos informáticos.

Es así como se entiende por delito informático a la acción típica, antijurídica y dolosa cometida mediante el uso normal de la informática, contra el soporte lógico o software, de un sistema de tratamiento automatizado de la información. Por lo tanto, únicamente se estará ante un delito informático cuando se atenta dolosamente contra los datos digitalizados y contra los programas computacionales contenidos en un sistema; otros casos parecidos, serár sólo delitos computacionales que no ameritan la creación de un nuevo ilícito penal.

En la moción presentada al Congreso se indicó que se buscaba proteger un nuevo bien jurídico: la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan.

[222] Ob. Cit. Huerta Miranda, Marcelo "Figuras delictivo-informáticos tipificadas en Chile" Págs. 1 y ss.

Artículo 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, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

Artículo 2. "El que con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

Artículo 3. "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio".

Artículo 4. "El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

2.3.4. LEGISLACIÓN INTERNACIONAL EN RELACION A LOS DELITOS INFORMATICOS.

Por otro lado presentamos, todos aquellos elementos que han sido considerados por organismos gubernamentales internacionales, sobre los delitos informáticos.

En este orden, debe mencionar que durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los

problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

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

La OCDE. Es una organización internacional intergubernamental que reúne a los países más industrializados de economía de mercado. En la OCDE, los representantes de los países miembros se reúnen para intercambiar información y armonizar políticas con el objeto de maximizar su crecimiento económico y coadyuvar a su desarrollo y al de los países no miembros.

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

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

autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

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

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

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

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

nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

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

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

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

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

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

En general, se supuso que habría un gran número de casos de *delitos informáticos* no registrados.

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

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

Teniendo presente esa situación, consideramos que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad

y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

En otro orden de ideas, debe mencionarse que la *Asociación Internacional de Derecho Penal* durante un coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los *delitos informáticos.* Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta que punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

Considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que puede entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la "lista facultativa", especialmente la alteración de datos de computadora y el espionaje informático; así como que por lo que se refiere al delito de acceso no autorizado precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Además, se señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

También se tiene entre otro el *Tratado de Libre Comercio de América del Norte (TLC).* Instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y

Canadá en 1993, que contiene un apartado sobre propiedad intelectual, a saber la 6ª parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

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

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

También destacaremos el contenido del párrafo primero del artículo 1717 titulado procedimientos y sanciones penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.

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

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

Otro de los acuerdos importantes fue realizado por la institución del GATT, la cual se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), siendo que todos los acuerdos que se suscribieron en el marco del GATT siguen siendo vigentes.

En este entendido, cabe mencionar que el Gobierno de México es parte de este acuerdo que se celebró en el marco de la *Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT).* Siendo vigente hasta nuestros días.

Considerando el hecho de que en este acuerdo, en su artículo 10, relativo a los programas de ordenador y compiladores de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el *Convenio de Berna de 1971 para la protección de Obras Literarias y Artísticas*, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

Además, en la parte III sobre observancia de los derechos de propiedad intelectual, en la sección I de obligaciones generales, específicamente en el artículo 41, se incluye que los miembros del acuerdo velarán porque en su respectiva legislación nacional se establezcan procedimientos de observancia de los derechos de propiedad intelectual.

Asimismo, en la sección 5, denominada procedimientos penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales además de que " los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias".

Finalmente, en la parte VII, denominada disposiciones institucionales, disposiciones finales, en el artículo 69 relativo a la cooperación internacional, se establece el intercambio de información y la cooperación entre las autoridades de aduanas en lo que se refiere al comercio de mercancías de marca de fábrica o de comercio falsificadas y mercancías pirata que lesionan el derecho de autor.

Como podemos ver, el tratamiento de los dos instrumentos internacionales que se han descrito otorgan a las conductas ilícitas relacionadas con las computadoras en el marco del derecho de autor.

También La UNESCO, en sus pronunciamientos relativos a las Autopistas de la Información, ha declarado que el aumento del acceso a redes y bases de datos interconectadas incrementa el valor de los principios éticos y legales, incluyendo:

- La privacidad de la información y el derecho que tiene cada individuo a chequear sus propios datos como derecho humano fundamental.
- La lucha contra la piratería internacional y otros delitos.
- La protección de los derechos de los creadores de software.

En fecha muy reciente, la propia UNESCO se ha pronunciado en contra del uso que se está dando a estas redes de alcance global para la difusión de pornografía, y el comercio de mujeres, e incluso de niños.

Como podemos ver la gran importancia de la regulación de los delitos informáticos y la preocupación que ha tenido la comunidad internacional, con la visión de que todos los países cuenten con ordenamiento jurídicos aplicables aquellas conductas ilícitas relacionadas con la computadora.

Siendo todo esto que ha dado lugar a realizar reuniones de expertos gubernamentales sobre delito cibernético, promovido por el Consejo Permanente de la Organización de los Estados Americanos.[223]

Por lo que en el mes de marzo de 1999 los Ministros de Justicia o Ministros o Procuradores Generales de las Américas recomendaron establecer un grupo de expertos intergubernamentales sobre delito cibernético con el mandamiento de:

1) Hacer un diagnostico de la actividad delictiva vinculada a las computadoras y la información en los Estados miembros;
2) Hacer un diagnóstico de la legislación, las políticas y las prácticas nacionales con respecto a dicha actividad;
3) Identificar las entidades nacionales e internacionales que tienen experiencia en la materia, y
4) Identificar mecanismos de cooperación dentro del sistema interamericano para combatir el delito cibernético.

Para este fin, se convoco la Primera Reunión de Expertos Gubernamentales en Delito Cibernético en mayo de 1999 con el fin de cumplir las metas fijadas por los Ministros de Justicia o Procuradores Generales. Para facilitar el cumplimiento de sus mandatos, la Primera Reunión del Grupo de Expertos preparó un cuestionario solicitando información a todos los Estados miembros sobre su experiencia con varios tipos de delitos cibernéticos, las leyes sustantivas, los principios de jurisdicción y de extradición que los rigen, las leyes que rigen la conservación y recolección de pruebas en dichos casos, y la existencia de programas especializados de capacitación o entidades y/o expertos en cumplimiento de las leyes para combatir el delito cibernético. Y con posterioridad se

[223] Ojales, Rodolfo. Abogado del Ministerio de Justicia de los Estados Unidos. CCIPS (Computer Crime and Intellectual Property Section) U. S. Departmen of Justice. Informe Final de la Segunda Reunión de Expertos Gubernamentales sobre Delito Cibernético. Págs. 1 y ss. "La expericencia Estadounidense" Curso Introducción a los Delitos Informácticos, Instituto Nacional de Ciencias Penales, Julio del 2000.

llevaría acabo la Segunda Reunión que se llevo a cabo los días 14 y 15 de octubre de 1999.

Reuniones que han servido para aportar las siguiente *recomendaciones:*

Dentro del marco de lo establecido en la resolución AG/res.1615/99 (XXIX- 0/99) y reconociendo la amenaza global que plantea el delito cibernético y la necesidad de una respuesta adecuada y rápida por parte de las autoridades nacionales competentes, la Reunión de Expertos formula las siguientes recomendaciones que serán sometidas, a través del Consejo Permanente, a la Tercera Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas:

1.- Instar a los Estados miembros que establezcan una entidad o entidades públicas con al autoridad y función específica para llevar adelante la investigación y persecución del delito cibernético.

2:- Que los Estados, que aún no cuenten con legislación sobre delitos cibernéticos emprendan acciones en éste sentido.

3.- Solicitar a los Estados miembros que realicen todos los esfuerzos necesarios para armonizar sus legislaciones en materia de delito cibernético, a fin de facilitar la cooperación internacional para preservación y combate de éstas actividades ilícitas.

4.- Que los Estados miembros identifiquen sus necesidades de capacitación en materia de delito cibernético, propiciándose esquemas de cooperación bilateral, regional y multilateral en este campo.

5.- Propiciar la formulación de lineamientos generales para orientar los esfuerzos legislativos en materia de delito cibernético.

6.- Considerar diversas medidas incluyendo el establecimiento de un Fondo Específico Voluntario, para apoyar el desarrollo de la cooperación en el Hemisferio sobre la materia.

7.- Propiciar entre los Estados miembros el intercambio de información en materia de delito cibernético.

8.- Apoyar la difusión de información sobre las actividades desarrolladas en el ámbito de la OEA en esta materia, incluyendo la página Web sobre el particular.

9.- Que los Estados miembros consideren la posibilidad de sumarse a mecanismos de cooperación o intercambio de información ya existentes, tales como el "Grupo de contacto de 24 horas/7 días a día de iniciar y recibir información.

10.- Que los Estados miembros tomen medidas para sensibilizar al público, incluyendo a los usuarios del sistema educativo, del sistema legal y administración de justicia sobre la necesidad de prevenir y combatir el delito cibernético.

2.3.5. LEGISLACIÓN NACIONAL EN RELACION A LOS DELITOS INFORMATICOS.

En nuestro país a sido poca la legislación que regula las relaciones y avances de la computadora, a pesar del enorme crecimiento de la tecnología informática, la conciencia que se ha dado a nivel mundial, ha dado enormes avances en sus respectivas legislaciones, como los países Europeos y Estados Unidos, considerando que este tipo de problemas no tiene fronteras, pero además que causa enormes daños económicos, sociales y políticos. Y tomando en cuenta que hoy en día México cuenta con una red mundial de información en la que circula enormes cantidades de datos en sus sitemas informáticos, es urgente e imperiosa la necesidad de prevenir y sancionar todas aquellas conductas que lesionen bienes jurídicos tradicionales como bienes jurídicos de reciente tutelación.

La problemática de los delitos informáticos requiere un estudio especial en nuestro país con finalidad de adecuar todas aquellas conductas ilícitas, tomando todo tipo de medidas en nuestra legislación local y federal.

Encontrando como antecedente, que ya algunas leyes especiales y locales contemplan a los delitos informáticos:

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

Sobre el particular, y por considerar de interés el contenido de la exposición de motivos cuando esta ley se presentó ante la Cámara de Diputados, se tenia la debida atención a la problemática de los derechos de autor en nuestro país.

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

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

Al respecto, se consideró conveniente la inclusión de la materia en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas y por otro en un instrumento más adecuado para la procuración y la administración de justicia, al poderse disponer en la investigación

de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.

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

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

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

Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, Artículo 424, fracción IV "*a quien fabrique con fines de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de*

computación" [224] del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal del que se infiere la sanción al uso de programas de virus. Código Penal Para el Distrito Federal, que fue reformado el 17 de septiembre de 1999, derogando los delitos en Materia de Derechos de Autor, pasándolos a competencia solo del Fuero Federal.

Si bien pudiera pensarse que la inclusión de las sanciones a la fabricación de programas de virus en el Código Penal antes de las reformas de septiembre de 1999, llevaba implícito el reconocimiento de un *delito informático* debiendo tenerse presente que los delitos que se regulaban en ese título eran en materia de derecho de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los *delitos informáticos* el bien jurídico tutelado son entre otros la información, intimidad, patrimonio, etcétera.

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

Por su parte, el artículo 231, fracciones III y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por esta Ley" y "usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular". [225]

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

---

[224] Agenda Penal 98. Compendio de Leyes Penales. Edt. ISEF. "Código Penal". Pág. Pág. 114.
[225] Ley Federal del Derecho de Autor. Secretaria de Educación Pública. México, 1997. Págs. 46 y 47.

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

En otro orden, el Artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información. Así, el acceso no autorizado a una base de datos de carácter personal.

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

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

Esta Ley, además establece en el Título X, en su capítulo único, artículo 208, que el Instituto Nacional del Derecho de Autor es la autoridad administrativa en materia de derechos de autor y derechos conexos, quien tiene entre otras funciones, proteger y

fomentar el derecho de autor además de que está facultado para realizar investigaciones respecto de presuntas infracciones administrativas e imponer las sanciones correspondientes.

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

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

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

Con las reformas al Código Penal Federal se especifica que:

Artículo. 424 bis....
I. A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende, copias de obras, fonogramas, viedogramas o libros protegidas por la Ley Federal del Derecho de Autor en forma dolosa, a escala comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.[226]

Por otro lado también tenemos que algunos de los Estados de la República Mexicana se a dado a la tarea de legislar sobre los delitos informáticos.

[226] Código Penal Federal. Edit. Sista. México 1999. Pág. 204.

Dada la importancia que tiene al respecto este tipo de conductas, el *Congreso Local del Estado de Sinaloa* hace una importante aportación al legislar sobre la materia de delitos informáticos, considerados en el *Código Penal Estatal.*

Título Décimo
"Delitos contra el patrimonio"

Capítulo V
Delito Informático.

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

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

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

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.[227]

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

[227] Código Penal y Procedimientos Penales de Sinaloa.Edt. Anaya Editores, S.A. México 1998. Pág.69.

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

También encontramos que existen tipos penales que han visualizado a los delitos informáticos, y que son regulados en nuestros Ordenamientos Legales. De los que hace alusión la Mtra. Emma Riestra Gaytán en el curso de Introducción a los Delitos Informáticos:[228]

Conductas En base al acceso	Adecuación al tipo penal existente
A) Interceptación de comunicaciones sin autorización. • Derecho a la privacidad. • Protección de datos personales.	• Constitución Política de los Estados Unidos Mexicanos: Artículo 16 último párrafo, 20 • Ley Federal de Derechos de Autor. Título IV de la Protección al Derecho de autor Artículo 109 Código Penal Federal. Titulo Noveno Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática. Artículo 211- Bis.
B) Aprovechamiento de sistematización de la información contenida en Bases de datos de sistemas o equipos de informática.	Código Penal Federal. Titulo Noveno Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática. Capitulo II. Acceso ilícito a Sistemas y Equipos de Informática. Artículo 211- Bis-4. Artículo 211- Bis-5.

[228] Ob. Cit. Los Delitos Informáticos en el Derechos Positivo Mexicano, Págs. 32 y SS.

C) Utilización de segmentos de red de sistemas o equipos informáticos (correo electrónico, página, web, etc).	Código Penal Federal. Titulo Décimo Octavo. Delitos Contra la Paz y Seguridad de las Personas. Capitulo II. Allanamiento de Morada. Artículo 285.
D) Utilización indebida del equipo 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).	Código Penal Federal. Titulo Vigésimo Segundo. Delitos en Contra de las Personas en su Patrimonio. Artículo 368 fracción II.
E) 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.	Código Penal Federal. Titulo Vigésimo Sexto. Delitos en Materia de Derechos de Autor. Artículo 424 Bis fracción II.
F) Difusión, distribución y reproducción mediante sistemas o equipos de informática de información relativa a la pornografía infantil (corrupción de menores), y el lenocinio.	Código Penal Federal. Titulo Octavo. Corrupción de Menores e Incapaces, Pornografía Infantil y Prostitución Sexual de Menores.
G) Difusión, distribución y reproducción mediante o no sistemas o equipos de informática de información (Software) contenida en otros sistemas informáticos, lo que actualmente se concibe como fraude informático, espionaje industrial.	Código Penal Federal. Titulo Noveno. Revelación de Secretos y Acceso Ilícito, Sistemas y Equipos de Informática. Capitulo. I Revelación de Secretos. Artículos 210, 211, 211-Bis. Titulo Vigésimo Segundo. Delitos en Contra de las Personas en su Patrimonio. Artículo 386.
H) Aprovechamiento indebido o violación de un Código para penetrar un sistema introduciendo instrucciones inapropiadas.	Código Penal para el Distrito Federal. Capitulo II. Falsificación de Títulos al Portador y documentos de Crédito Público. Artículo 240- Bis. Fracción IV.- Altere los medios de identificación electrónica de tarjetas títulos y documentos para el pago de bienes y servicios.

	Capitulo III. Falsificación de Sellos, llaves... Artículo 242 fracción I.- Al que falsifique llaves.
I) Negación de acceso si autorizado a sistemas y equipos de informática.	Ley de Información, Estadística y Geografía. Derecho de acceso, cancelación y rectificación.
J) Abuso y Daño de información en introducción falsa de información al sistema o equipo informático.	Código Penal para el Distrito Federal. Capitulo II. Falsificación de Títulos al Portador y documentos de Crédito Público. Artículo 240- Bis. Fracción V.- Acceso indebidamente a los equipos electromagnéticos de las instituciones emisoras de tarjetas títulos y documentos para el pago de bienes y servicios a sabiendas de que son alterados o falsificados.
K) Copiar y distribuir programas de cómputo en equipos o sistemas informáticos.	Código Penal Federal. Titulo Vigésimo Sexto. Delitos en Materia de Derechos de Autor. Artículos 424 y 424 Bis.
L) Organizar los elementos humanos y materiales para la comisión de los delitos relativos a la delincuencia organizada.	Lavado de Dinero. Código Penal Federal. Titulo Vigésimo Tercero. Encubrimiento y Operaciones con Recursos de Procedencia Ilícita. Capitulo II. Operaciones con Recursos de Procedencia Ilícita. Artículo 400- Bis.

De igual forma tenemos que en las reformas presentadas al Código Penal del Distrito Federal del mes de septiembre de 1999, se contempla ya en su artículo 387 en su fracción XXII, "Al que, para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero o indebidamente realice operaciones, transferencias o

movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución".[229]

2.4. EL DERECHO PENAL Y LAS TÉORIAS DEL DELITO.

El Derecho Penal nace de la necesidad imperante de regular la conducta del individuo en sociedad, función que ha tenido que adecuar, acorde al tiempo y lugar en que se aplican, orientada siempre a castigar al sujeto que realiza una conducta sancionada como delito, tomando en cuenta los aspectos culturales y sociales que se presentan en cada país.

La idea de que el Derecho Penal responde a una concepción puramente platónica y, por tanto, coloca fuera del tiempo y del espacio, vive aún en la mente de muchos penalistas, no obstante que debe tenerse muy en cuenta que el Derecho Penal constituye uno de los aspectos de la vida cultural y, por ende, de la historia de un pueblo.[230]

Thomas Wurtenberger ha afirmado que en ningún lugar resulta tan necesaria, para la existencia del Derecho, una consideración histórica cuanto en el ámbito propio del Derecho Penal: no puede existir ninguna ciencia válida del Derecho Penal haciéndose abstracción de la Historia del mismo.[231]

El Derecho Penal, es ciertamente, la rama jurídica que más ha padecido la intromisión en su esfera de otras ciencias. Puede afirmarse que caso no ha habido rama especial del conocimiento que no haya pretendido (y en algunos casos logrado) determinar los principales conceptos jurídico-penales.[232]

---

[229] Código Penal para el Distrito Federal, con las disposiciones legales conocidas hasta octubre de 1999, Edit. Sista, Pág. 126.

[230] Bettiol Giuseppe, Derecho Penal, Edit. Temis, Bogotá 1965. Pág. XIII. Según cita de Reynoso Dávila Roberto en su obra Teoría General del Delito. Edit. Porrúa. México, 1997. Pág. 2.

[231] Polaino Navarrete Miguel. Los Elementos Subjetivos del Injusto en el Código Penal Español, Publicaciones de la Universidad de Sevilla. 1972. Pág. 85. Idem. Pág. 2.

[232] Klein Quintana Julio, Ensayo de una Teoría Jurídica del Derecho Penal, Librería de Manuel Porrúa, México 1951. Pág. 5. Idem. Pág. 3.

Por lo que el Derecho Penal es el conjunto normativo perteneciente al derecho público interno, que tiene por objeto al delito, al delincuente y a la pena o medida de seguridad, para mantener el orden social mediante el respeto de los bienes jurídicos tutelados por la ley.[233]

Sin omitir que la teoría del delito tiene como objeto analizar y estudiar los presupuestos jurídicos de la punibilidad[234] de un comportamiento humano sea a través de un acción o de una omisión, en estos términos dicho análisis no sólo alcanza a los "delitos" sino incluso a todo comportamiento humano del cual pueda derivar la posibilidad de aplicar una consecuencia jurídico penal, entonces, será objeto de análisis de la teoría del delito aquello de lo cual derive la aplicación de una pena o una medida de seguridad, así como los casos extremos en los que no obstante existir una lesión o puesta en peligro de un bien jurídico, el comportamiento humano resulte justificado, no reprochable o bien, no punible.

La teoría del delito es una parte de la ciencia del Derecho Penal; comprende el estudio de los elementos positivos y negativos del delito, así como sus formas de manifestarse.[235]

La teoría del delito "atiende al cumplimiento de un cometido esencialmente práctico, consistente en la facilitación de la averiguación de la presencia o ausencia del delito en cada caso concreto".[236]

---

[233] Amuchategui Requena Irma. Derecho Penal. Edt. Harla México 1993. Pág. 14.

[234] Jesheck, Hans Heinrich, Tratado de derecho penal, trad. Santiago Miru Puig, Barcelona, Bosch, 1978, págs 263 y ss. Según cita de Plascencia Villanueva Raúl. Teoria del delito. Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México. México 1998. Pág. 15.

[235] López Batancourt Eduardo. Teoría del Delito, Edit. Porrúa, México, 1998. Pág. 3

[236] Zaffaroni, Eugenio Raúl. Manuel de Derecho Penal. Parte General, 2ª Ed., Edit. Cárdenas Editores y Distribuidores, México 1991. Pág. 333.

Para referir la teoría del delito es necesario establecer con precisión su ubicación. En virtud de constituir un concepto eminentemente penal, se encuentra inmerso en la ciencia penal, ya que es ésta la que engloba al conjunto de teorías explicativas de los conceptos penales fundamentales.[237]

Para Maggiore " la teoría del delito, es la ciencia con los mismos títulos que la ciencia general del derecho, debe tener una estructura sistemática y organización lógica que responden a criterio de rigurosa necesidad; determinar esa estructura, señala la organización interna- íbamos a decir la articulación- de la doctrina del delito, es la parte más delicada de la ciencia del derecho penal y también a causa de esta delicadeza, la parte más controvertida" [238]

Por lo que antes de hablar de las diferentes teorías del delito, es importante señalar que es delito y cuales las causas que lo originan, en sus respectivas concepciones y corrientes.

2.4.1. DELITO.

Al estudiar el delito nos daremos cuenta que cada tratadista expresa su concepto del mismo en forma muy diversa y puntualiza características esenciales del mismo.

Ya que el delito a lo largo de los tiempos, ha sido entendido como una valoración jurídica, objetiva o subjetiva, la cual encuentra sus precisos fundamentos en las relaciones necesarias surgidas entre el hecho humano contrario al orden ético-social y su especial estimación legislativa.[239]

---

[237] Idem. Pág.26.

[238] Maggiore Giuseppe. Derecho Penal. Vol I 2da edición Edit. Tamis Bogota 1989. pág. 268.

[239] Pavón Vasconcelos Francisco. Derecho Penal Mexicano. Decimasegunda Edic., Edit Porrúa S.A. México. 1995. Pág.177.

Por lo que empezaremos hablando de la noción etimológica del termino delito:

En atención a sus raíces, el vocablo delito deriva del verbo latino "delinquere" que significa: abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley.[240]

2.4.2. CONCEPCIÓN TEÓRICA.

Esta concepción del delito se realiza desde el punto de vista causal explicativa o la luz del deber ser.

La concepción causal explicativa se realiza desde diferentes vértices tanto sociológica, filosófica, antropológica. Todas con el propósito de encontrar una explicación a las causas del delito.

a) Corriente Sociológica.

La corriente sociológica del pensamiento que dentro del campo criminológico, asigna al medio social, el carácter de factor decisivo o fuerza causal del fenómeno criminal, constituye la dirección sociológica.

La Sociología Criminal recorre un camino paralelo al de las investigaciones de este campo; es decir, los sociólogos en ocasiones se ocupan del fenómeno criminal, como uno de los tantos fenómenos que ocurre en la sociedad.

La corriente sociológica se nutre de varios exponentes quienes explican en atención a diversos criterios sociológicos al delito, así la escuela geográfica o cartográfica, representada por Adolfo Quetelet, quien llega a tres conclusiones fundamentales en cuanto al problema de la delincuencia.

---

[240] Castellanos Tena Fernando. Lineamientos Elementales de Derecho Penal. Edt. Porrúa México. 1989.Pág. 126.

1) El delito es un fenómeno social que puede conocerse y determinarse estadísticamente.

2) Los delitos se cometen año tras año, con una absoluta regularidad y precisión.

3) Los factores que intervienen como causas de la actividad delictuosa son variadas entre las que se tiene: el clima, la pobreza, la miseria, el analfabetismo etc.

Por su parte Gabriel Tarde señala que todo fenómeno social tiene su base o asiento en la imitación y esta es un fenómeno sociológico.

Refiriendo que el fenómeno criminal, es una manifestación social, es un proceso de imitación reprobado por el grupo social como negativo. Existe en el delincuente una inadaptación social, una predisposición psíquica y biológica hacía el crimen, que puede manifestarse en el grupo social como un medio negativo de imitación.

Según Enrique ferri es inaceptable el criterio del libre albedrío, como fundamento de la responsabilidad penal, ya que el delincuente obra en virtud de factores sociales, individuales, físicos por lo cual debe ser sujeto a medias de seguridad, no apenas, pues no debe ser castigado, sino confinado en virtud de su peligrosidad.

Para Emilio Durkheim la criminalidad es un fenómeno normal, porque deriva de la estructura misma de la sociedad, es un producto cultural. Como producto normal de toda sociedad, evoluciona y se trasforma en la misma medida que lo hace la propia sociedad.

El estudio de la criminalidad, solamente se podrá realizar, analizando la cultura que lo ha producido en un tiempo y espacio determinado.

Pata la corriente sociológica el delito no es otra cosa más que un fenómeno social.

b) Corriente Psicológica.

Para esta corriente la compresión del fenómeno criminal, no solo es individual o general, como consecuencia de un factor, social, biológico, físico, o psicológico, sino es un conocimiento integral del individuo, de su personalidad, dentro del medio social y físico determinado.

Uno de los exponentes de esta corriente es Wilhelm Wundt fundador de la escuela psicológica denominada "estructuralismo" ya que se suponía que estudiaba la estructura de la conciencia.

Otro exponente fue Ivan Petrovich Pavlov, principal exponente de la reflexología y quien explica que existe un conflicto entre el proceso de excitación y uno de inhibición, el que por lo común el individuo, resuelve, optando por establecer un equilibrio entre ambos, pero cuando la elección es tan difícil, el equilibrio se rompe y aparece un estado total de excitación o inhibición que altera profundamente el comportamiento.

El más destacado exponente fue Sigmundo Freud, quien aportara su teoría del psicoanálisis, afirmaba que la parte ocular de la personalidad es el inconsciente, cuya explicación le atribuyć una base sexual.

Para Freud el psicoanálisis revela al paciente lo que oculta su inconsciente y pone en manifiesto la represión de los traumas sexuales de su infancia, y es conocimiento doloroso sin duda, permite que el paciente lo supere en bien a su salud psíquica y fisiológica.

Para el psicoanálisis el hombre actúa por motivos de orden sexual y desde la más tierna infancia hasta su muerte está dominado por los instintos, sexuales o de la vida, y el de tanatos o de la muerte.

Algunos estudios relacionados por seguidores de esta corriente señalan que el psicópata es un individuo que no logra ajustarse a la vida en sociedad, se revela contra las normas colectivas, porque chocan contra sus deseos, e incurre en delitos o conductas antisociales.

La concepción psicológica, descansa en el reconocimiento de la relación psicológica existente entre el hecho concreto antijurídico y su autor, que hace posible la aplicación de las consecuencias penales.

c) Corriente Filosófica.

Realmente en la antigua Grecia, donde se señala con mayor frecuencia las causas de la delincuencia desde el punto de vista filosófico.

Para Platón el crimen es un producto del medio ambiente. La pobreza y la miseria son factores criminógenos y acuña una frase de indudable valor "no castigamos porque alguien haya delinquido, sino para que los demás no delincan", principio fundamental de la penalogía.

Aristóteles conviene con platón en estimar que la pobreza inclina al delito, pero agrega que los crímenes más graves no cometen para adquirir lo necesario, sino lo superfluo. Agrega que las pasiones pueden llevar al hombre virtuoso a cometer delitos.

d) Corriente Antropológica.

Uno de los principales exponentes de la corriente antropológica fue Cesar Lombroso, quien trata de explicar la conducta delictiva en base al estudio de la estructura del hombre.

Su obra más importante la denominó el hombre delincuente, misma que le atribuyó el título de padre de la criminología.

Cesar lombroso decía que el delincuente era un ser atávico con fondo epiléptico, señalaba que el atavismo consistía en retomar conductas salvajes y la epilepsia constituía una causa de los crímenes en aquellos casos donde se presentaba la ferocidad, la falta de cómplices, la aparente normalidad de la conducta procedente y subsecuente al crimen del delincuente la amnesia del acto cometido, o recuerdo vago, o su referencia a él con toda indiferencia.[241]

Lombroso clasifico a los delincuente en:

1.- Delincuente nato.
2.- Delincuente loco o matto.
3.- Delincuente habitual.
4.- Delincuente pasional.
5.- Delincuente ocasional.

Otros seguidores de Cesar Lombroso fueron Enrique Ferri y Rafael Garófalo.

Enrique Ferri con una tendencia sociológica pero con influencia de lombroso hace la afirmación de que no hay delito sino delincuentes.

Este estableció al lado de la corriente antropológica, la sociológica, como causa de la delincuencia pero no en forma aislada sino rotunda y además consideró los factores físicos.

Rafael Garófalo, destacado jurista y sociólogo planteó el concepto de delito.

[241] Cfr. Castellanos Tena Fernando. Lineamientos Elementales de Derecho Penal.

El cual lo define como "La violación de los sentimientos altruistas de piedad y probidad en la medida media indispensable para la adaptación del individuo en la sociedad ".[242]

Siendo estos exponentes el pilar de la escuela positivista.

Desde el punto de vista del deber ser, la concepción teórica del delito se relaciona íntimamente con el deber jurídico penal, que implica la subordinación del gobierno a la norma penal establecida por el legislador, concretamente al imperativo y a realizar o dejar de hacer lo que la norma establezca.

2.4.3. LA CONCEPCIÓN JURÍDICA.

Desde el punto de vista jurídico se han elaborado definiciones del delito, las cuales explicaremos.

a) Noción Jurídico Formal.

Para varios autores la verdadera noción formal del delito la suministra la ley positiva mediante la amenaza de una pena para la ejecución o la omisión de ciertos actos, pues formalmente hablando, expresan, que el delito se caracteriza por su sanción penal; sin una ley que sancione una determinada conducta, no es posible hablar de delito.

La noción jurídico formal se refiere a " las entidades típicas que traen aparejada una sanción; no es la descripción del delito en concreto, sino la enunciación de que un ilícito penal merece una pena" [243]

El artículo 7º de nuestro Código Penal para el Distrito Federal, establece: " Delito es el acto u omisión que sancionan las leyes penales".[244]

---

[242] Ob. Cit. Reynoso Dávila Roberto. Teoría General del Delito. Pág. 17
[243] Ob. Cit. Amuchategui Requena Irma. Derecho Penal. pag. 43.
[244] Ob. Cit. Código Penal para el Distrito Federal. Pág.12.

b) Noción Jurídico Sustancial.

Esta consiste en hacer referencia a los elementos de que integran al delito.

Son dos los sistemas principales para realizar el estudio jurídico esencial del delito: el unitario o totalizador y el atomizador o analítico.

Según la corriente *unitaria o totalizadora*, el delito no puede dividirse no para su estudio, por integrar un todo orgánico, un concepto indisoluble.

Señala Antolosei que para los seguidores de esta doctrina, el delito es como un bloque monolítico el cual puede presentar aspectos diversos, pero no es el modo alguno fraccionable.[245]

Para la corriente *analítica o atomizadora*, es factible el estudio del ilícito penal por sus elementos constitutivos. Evidentemente para estar en condiciones de entender el todo, precisa el conocimiento cabal de sus partes; ello no implica, por supuesto, la negación de que el delito integra una unidad. Ya Francisco Carrara hablaba del ilícito penal como una disonancia armónica; por ende, al estudiar el delito por sus factores constitutivos, no se desconoce su necesaria unidad.

En cuanto a los elementos integradores del delito no existe una doctrina con uniformidad de criterios, mientras unos especialistas señalan un número, otros lo configuran con más elementos; surgen así las concepciones bitómicas, tritómicas, tetratómicas, pentatómicas, exatómicas, heptatómicas etc.

[245] Antolisei Francisco. "El estudio analítico del delito", traducción del italiano de Ricardo Franco Guzman, Edic. de Anales de Jurisprudencia, México, 1954. Pág. 78. Según cita de Orellana Wiarco Octavio Alberto. Teoría del Delito. Sistema Causalista y Finalista. 3ª Edic., Edit. Porrúa México 1996. Pág. 7.

Para Ernesto Von Beling el delito es una acción típica o jurídica, culpable, subsumible bajo una sanción penal adecuada y satisfaciendo las condiciones objetivas de punibilidad.[246]

Para Edmundo Mezger, el delito es una acción típicamente antijurídica y culpable.[247]

Para Cuello Calón, el delito es un acción humana antijurídica, típica, culpable y punible.

Para Jiménez de Asúa el delito, es el acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción.[248]

Según Eugenio Florian, el delito es el hecho culpable del hombre, contrario a la ley y que está amenazado por una pena.

Para Franz Von Liszt lo define al delito como un acto humano, culpable, antijurídico y sancionado con una pena.[249]

Max Ernesto Meyer, define al delito como un acontecimiento típico, antijurídico, e imputable.[250]

Por lo tanto al hablar del estudio de estos elementos estaremos hablando de la teoría del delito, que es aquella que estudia los elementos positivo como negativos del delito, así como sus formas de manifestarse.

---

[246] Ob. Cit. Pavón Vasconcelos Francisco. Pág. 180.
[247] Idem. Pág. 180.
[248] Idem. Pág. 180.
[249] Idem. Pág. 180.
[250] Idem. Pág. 180.

Aspectos Positivos.	Aspectos Negativos.
Conducta.	Ausencia de conducta.
Tipicidad.	Atipicidad.
Antijuridicidad.	Causas de Justificación.
Imputabilidad.	Inimputabilidad.
Culpabilidad.	Inculpabilidad.
Condiciones Objetivas.	Falta de Condicionalidad objetiva.
Punibilidad.	Excusas absolutorias.

1) Conducta.

"La conducta es el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito". [251]La conducta también llamada acto o acción, lato sensu, puede también manifestarse mediante haceres positivo o negativos, es decir por actos o por abstenciones.

El acto o la acción, estricto sensu, 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; en dejar de ejecutar.

[251] Ob. Cit. Castellanos Tena Fernando. Pág. 182.

2) Tipicidad.

La tipicidad es el encuadramiento de una conducta con la descripción hecha por la ley; la coincidencia del comportamiento con el descrito por el legislador. Es en suma, la acuñación o adecuación de un hecho a la hipótesis legislativa.

3) Tipo.

Es la descripción de la conducta prohibida que lleva a cabo el legislador en el supuesto de hecho de una norma penal.[252]

Elementos Objetivos o Externos. Son aquellos que el autor puede conocer a través de sus sentidos, es decir oído, tacto, vista (ejemplo. la "cosa" en el delito de robo)[253] En otras palabras incluye elementos externos que constituyen la materialidad del hecho que la ley señale como delito o sea que son aquellos que pueden ser captados por medio de los sentidos.

Elementos normativos. Son aquellos que solo pueden ser determinados mediante una especial valoración de la situación del hecho, valoración que es realizada por el juzgador, la cual puede ser jurídica de acuerdo con el contenido *iuris* del elemento normativo, o bien cultural, cuando se debe realizar de acuerdo a un criterio extrajurídico.

> **De valoración jurídica.** Como ya se menciono esta valoración nace de la propia ley, es decir, cuando la ley lo expresa, por ejemplo "cosa ajena" en el robo; "funcionario"; "servidor público", documento público o documento privado, "bien mueble", "derechos reales", etc.

[252] Muñoz Conde Francisco. Teoría General del Delito, Temis, Bogotá 1990, pág. 40
[253] Artículo 367 del Código Penal para el Distrito Federal.

De valoración cultural. Existe valoración cultural cuando el Código refiere una situación extralegal pero que para su comprensión se necesita su comprobación, ejemplo: "acto erótico sexual".

Elementos subjetivos diferentes al dolo. En algunas ocasiones los tipos penales hablan de ánimos, propósitos, deseos, intenciones, etc., ejemplo de lo anterior es cuando la ley refiere: "al que con propósito de..."; al que con la finalidad de..."; " al que con deseo de ..." Estos elementos son diferente al dolo y son exigidos por el Legislador para la integración del cuerpo del delito. Se podría pensar que estos elementos podrían ser parte del dolo, pero esto es equívoco, pues por ejemplo la diferencia entre el robo genérico y el robo de uso lo constituye el elemento subjetivo diferentes al dolo, es decir, mientras en el robo genérico además del dolo se requiere el "ánimo de apropiación", en el robo de uso solo se requiere el dolo y se encuentra ausente de dicho ánimo de apropiación.

5) Antijuridicidad.

La antijuridicidad es un concepto negativo, comúnmente se acepta como antijurídico lo contrario a derecho. Según Beling, es una contradicción entre el hecho del autor y el derecho tutelado por la ley.[254]

6) Imputabilidad.

Es la posibilidad condicionada por la salud mental y por el desarrollo del autor, para obrar según el justo conocimiento del deber existente. Es la capacidad de obrar en Derecho Penal, es decir, de realizar actos referidos al Derecho Penal que traigan consigo las consecuencias penales de la infracción.

En pocas palabras, podemos definir la imputabilidad como la capacidad de entender y de querer en el campo del Derecho Penal.[255]

---

[254] Ferreira Delgado Franciso. Teoría General del Delito.Edit. Temis, S.A. Bogotá- Colombia, 1988. Pág. 232.
[255] Ob. Cit. Amuchategui Requena Irma G. Derecho Penal. Pág. 78.

7) Culpabilidad.

Es el nexo intelectual y emocional que liga al sujeto con su acto. La culpabilidad reviste dos formas: dolo y culpa, según el agente dirija su voluntad consciente a la ejecución del hecho tipificado en la ley como delito, o cause igual resultado por medio de negligencia o imprudencia.

a) El Dolo.

Se define como el actuar consciente y voluntario, dirigido a la producción de un resultado típico

"las acciones u omisiones delictivas solamente pueden realizarse dolosa o culposamente"[256]. "...Obra dolosamente el que, conociendo los elementos del tipo penal, o previendo como posible el resultado típico, quiere o acepta la realización del hecho descrito por la ley..."[257]

Elementos del dolo.

Elemento intelectual. Para actuar dolosamente, el sujeto de la acción debe saber qué es lo que hace y los elementos que caracterizan su acción, como acción típica. Es decir, ha de saber, por ejemplo en el homicidio, "que mata a otra persona"; en el robo, "que se apodera de una cosa ajena mueble"; en la violación "que copula con alguien sin su consentimiento", etc. no es necesario en cambio que conozca otros elementos pertenecientes a la antijurídicidad, a la culpabilidad o a la penalidad. El elemento intelectual del dolo, se refiere por tanto a los elementos que caracterizan objetivamente la acción como típica (elementos objetivos del tipo): sujeto, acción, resultado, relación causal o imputación objetiva, objeto material, etc.; y

[256] Artículo 8° del Código Penal para el Distrito Federal.
[257] Artículo 9 del Código Penal para el Distrito Federal.

Elemento volutivo. Para actuar dolosamente no basta con el mero conocimiento de los elementos objetivos del tipo, es necesario, además, querer realizarlos. Este querer no se confunde con los deseos o con los móviles del sujeto.

Clases de dolo:

Dolo Directo: Consiste en que el sujeto quiera y acepte el resultado producido, no obstante haberlo previsto.

Dolo Eventual: Este se presenta cuando el sujeto prevé el resultado en un principio y no quiere que se produzca, y a pesar de tal representación, no renuncia a la ejecución del hecho, aceptando sus consecuencias.

Dolo de Consecuencias Necesarias: Este consiste en que el sujeto activo quiera el resultado, el cual necesariamente trae consigo otro resultado que el sujeto no prevé.

b) La Culpa.

Para Cuello Calón, existe culpa cuando se obra sin intención y sin la diligencia debida, causando un resultado dañoso, previsible y penado por la ley. Para Edmundo Mezguer, actúa culposamente quien infringe un deber de cuidado que personalmente le incumbe y cuyo resultado puede prever.

"obra culposamente el que produce el resultado típico, que no previó siendo previsible o previó confiando en que no se produciría, en virtud de la violación a un deber de cuidado, que debía y podía observar según las circunstancias y condiciones personales."[258]

[258] Idem. Artículo 9 del Código Penal.

Elementos de la culpa. Por ser necesaria la conducta humana para que exista el delito, ella constituye:

El primer elemento (un actuar voluntario, es decir positivo o negativo).

El segundo elemento, se requiere que esa conducta voluntaria se realice sin las cautelas o precauciones exigidas por el Estado.

El tercero, los resultados del acto han de ser previsibles y evitables y tipificarse penalmente.

El cuarto, precisar una relación de causalidad.

Clases de culpa.

Culpa con representación. Es aquella en la cual el sujeto activo se representa el resultado y tiene la esperanza que no se produzca

Culpa sin representación. Es aquella en que el sujeto no prevé el resultado, siendo previsible.

8) Punibilidad.

Consiste en el merecimiento de una pena en función de la realización de cierta conducta. Un comportamiento es punible cuando se hace acreedor a la pena; tal merecimiento acarrea la conminación legal de aplicación de esa sanción.

La punibilidad es: a) merecimiento de penas; b) conminación estatal de imposición de sanciones si se llenan los presupuestos legales; y c) aplicación fáctica de las penas señaladas en la ley.

9) Condiciones Objetivas de punibilidad.

Son aquellas exigencias ocasionalmente establecidas por el legislador para que la pena tenga aplicación.

A lo anterior señalado y descrito brevemente como elementos que integran al delito, siendo de mucha importancia hablar de las teorías que los estudian.

2.4.4. TEORIAS DEL DELITO.

2.4.4.1. LA TEÓRIA CLÁSICA DEL DELITO.

El modelo de la teoría clásica del delito nace a partir de las ideas propuestas inicialmente por Carrara en Italia y, posteriormente, a partir de la separación iniciada por Rodolf Von Jhering en 1867 de la contrariedad de acción con las normas jurídicas y la censura a la disposición anímica de' sujeto, utilizando algunos postulados de Bechmer.[259]

La dogmática jurídica penal clásica (causalimo), iniciada por Liszt, Beling presenta una particular estructura, basada en el concepto causal mecanisista de la acción humana, es decir, la acción es el sostén, o como pauta Bustos Ramírez: La acción aparece como lo sustantivo, las demás características como simples adjetivaciones.[260]

---

[259] Welzel, Hans, Derecho Penal Aleman, 11ª ed., trad. Juan Bustos Ramiréz y Sergio Yámez Pérez, Chile, Editorial Jurídica de Chile, 1976, págs. 60 y 73. Según cita de Plasencia Villanueva Raúl Teoría del Delito Pág.36.

[260] Daza Gomez Carlos Juan Manuel. Teoría General del Delito. Edit. Cardenas Editores Distribuidor. México. 1998. Págs. 39 y 40.

A principios de este siglo, Liszt propuso una definición del delito como "acto punible, contrario al derecho y sancionado con una pena" esta idea fue completada por Beling, a partir de dos puntos fundamentales: a) el proceso material causal, y b) el contenido objetivo de la voluntad situaciones ambas que producen su impacto en el desarrollo de todo sistema y en las construcciones dogmáticas derivadas del mismo.[261]

La concepción clásica se encuentra caracterizada por concebir a la acción de una manera simple y clara, lo cual tiene términos totalmente naturalísticos, como es el caso de una acción compuesta por un movimiento corporal (acción en sentido estricto) y la consecuente modificación del mundo exterior (resultado) unidos por la relación de causalidad.[262]

Esta doctrina hace la distinción entre el aspecto externo y interno. El aspecto objetivo o externo, comprende: la acción, tipicidad y antijuricidad, el aspecto subjetivo o interno: la culpabilidad. Para el primero, hay un sentido naturalista en la acción, como la causación del mundo exterior por la conducta corporal deseada. El aspecto externo representa el tipo y de no existir causa de justificación habrá antijuricidad. El aspecto subjetivo del delito culpabilidad. En el causalimo naturalista es comprendida la culpabilidad como " La relación psíquica del autor con el aspecto externo del hecho", teniendo como formas al dolo y culpa, la imputabilidad es entendida como presupuesto de la culpabilidad consideramos que el aspecto objetivo-subjetivo, es igual a antijuricidad-culpabilidad.[263]

La acción es un aspecto del delito para la teoría causalista "es un comportamiento humano dependiente de la voluntad (voluntario), que produce una determinada consecuencia en el mundo exterior. Dicha consecuencia puede consistir tanto en el puro movimiento corporal (delitos de mera actividad), como en este movimiento corporal seguido del resultado ocasionado por él en el mundo exterior (delitos de resultado)" [264]

---

[261] Ob. Cit. Plasencia Villanueva Raúl Teoría del Delito Pág.36
[262] Idem. Pág. 36.
[263] Ob. Cit. Daz Gomez Carlos. Teoría General del Delito. Pág.40.
[264] Jascheck Hans Heinrich. Tratado de Derecho Penal, Parte General. Vol I 3ra. Edición Edit. Bosch Barcelona 1989 pág. 262.

Esta teoría visualiza a la acción como un factor causal del resultado, sin tomar en cuenta la intención que llevó al sujeto a cometerla, de la acción sólo le importa si el comportamiento movido por la voluntad, causó el resultado y no así, si la voluntad iba dirigida a éste.

Los causalistas explican la existencia de la acción delictiva, cuando un sujeto tiene la voluntad de realizarla, sin tomar en cuenta necesariamente la finalidad que se propina al hacer dicha acción.

La acción se le considera como un hacer voluntario, pero en esa voluntad no hay contenido. No contempla el actuar lleno de sentido, sino la simple producción de dicha situación referida al mundo exterior, a la que llama resultado.[265]

El contenido de la voluntad separado, declarado irrelevante para la acción, debe aparecer en otro lugar de la construcción del delito, en la configuración del dolo, en el sentido propio de un dolus malus, será albergado como característica de la culpabilidad, en el ultimo piso del edificio del delito.[266]

Para la teoría causal, la acción es una (inervación muscular), es decir un movimiento voluntario -no reflejo-, pero en el que carece de importancia o prescinde del fin a que esa voluntad se dirige.[267]

La teoría causalista considera el delito como un comportamiento humano dependiente de la voluntad que produce una determinada consecuencia en el mundo exterior; trata a la conducta como factor casual del resultado, sin tomar en cuenta la intención que llevó al sujeto a cometerla.

[265] Ob. Cit. Lopéz Betancourt Eduardo, Teoría del delito. Pág. 6
[266] Maurach, Reinhart, Tratado de Derecho Penal, tomo I, Ed. Ediciones Ariel, Barcelona 1962, pág. 202.
[267] Ob. Cit. Zaffaroni, Eugenio Raúl, Manuel de Derecho Penal. Págs. 369 y 370.

Los causalistas explican la existencia de la acción delictiva, cuando un sujeto tiene la voluntad de realizarla, sin tomar en cuenta necesariamente la finalidad que se proponía al hacerlo, porque ésta no pertenece a la conducta. Se concibe a la acción como un proceso causal natural y extrajurídico, libre de valor, como simple causación, sin tomar en cuenta la voluntad rectora.[268]

El sistema causalista señala que los subelementos que integran a su vez al elemento del acto o acción son:

a) Manifestación de la voluntad, que consiste en la inervación voluntaria del cuerpo humano que se traduce en un movimiento corporal, o en su inactividad (cuando nos hallamos frente a la omisión).

b) Un resultado, que es la mutación en el mundo exterior, causado por la manifestación de la voluntad, o la no mutación de ese mundo exterior por la acción esperada y que el sujeto no realiza, y

c) Un nexo causal, que radica en que el acto, acción o conducta ejecutada por el sujeto, produzca el resultado previsto en la ley de la manera que entre uno y otro exista una relación de causa efecto.[269]

2.4.4.2. LA TEÓRIA NEOCLÁSICA DEL DELITO.

A esta concepción se le ha llamado teoría normativa, o cuasalismo valorativo.

En cuanto al concepto de acción, se debilito su concepción mediante el uso del término comportamiento, el cual englobaba la actuación de la voluntad humana en el mundo exterior, con lo que se transformó en comportamiento voluntario, realización de voluntad,

---

[268] Ob. Cit. Reyno Dávila Roberto, Teoría General del Delito. Pág. 11

[269] Consultar al respecto a Guiseppe Bettiol, "Derecho Penal", Parte General, Edit. Temis, Colombia, 1965; y Luis Jiménez de Asúa "Tratado de Derecho Penal", tomo III. Según Cita de Orellano Wiarco Ocatio Alberto. Teoría del Delito. Pág. 11.

comportamiento espontáneo o sencillamente comportamiento humano (concepto causal e acción), y se pretendió suprimir el concepto acción e iniciar el análisis de la estructura del delito por la tipicidad.[270]

Reinhard Frank[271] en su teoría Normativa de la Culpabilidad[272] enfrenta el concepto de la culpabilidad psicologista, según la cual ésta se agota con sus formas dolo y culpa. Descubre que en el estado de la necesidad el sujeto activo actúa con dolo, por ello la culpabilidad no sólo era una relación psíquica del autor con el aspecto objetivo; lo cual demuestra que el estado de necesidad no desaparece el dolo y que la culpabilidad psicologista era insuficiente para determinados supuestos. Abunda al señalar que la culpabilidad no está en la psique del autor, sino que tal culpabilidad es un juicio que une a la conducta antijurídica, por hechos dados en la realidad, le serían reprochados; fundamenta su doctrina en la libertad interior y dominio del hecho por la voluntad, elementos que integran la imputabilidad, entendida ésta como presupuesto de la culpabilidad.

Reinhard Frank, profesor de la Universidad de Munich, es señalado como el padre de esta escuela; para tal doctrina la acción es comprendida:[273]

1) Acción.

La teoría normativa y clásica conciben como la conducta humana, manifestación de la voluntad en el mundo exterior.

El acto interno de voluntad y manifestación externa de ese acto, son requisitos de la acción.

---

[270] Ob. Cit. Plascencia Villanueva Raúl.Teoría del Delito. Pág. 38

[271] Véase Reinhard , Frank. Estructura del Concepto de Culpabilidad, Trad. Sebastián Soler, publicaciones del Semanario de Derecho Penal de la Universidad de Chile, Santiago, 1966. Según Cita de Daza Gomez Carlos. Pág. 11.

[272] Véase a Raúl Goldstein. Culpabilidad e Inculpabilidad, Trillas, México, 1977. Córdoba Roa, Juan, Culpabilidad y Pena, Bosch , Barcelona 1977, infra, pág. 57. Según Cita de Daza Gomez carlos. Pág. 11.

[273] Ob. Cit. Daza Gomez Carlos. Teoría General del Delito. Pág.45.

2) Tipicidad.

Se le considera como Rattio Essendi, de la antijuricidad. Se habla así del tipo de injusto. En su condición de mera descripción, exenta la valoración, que pugnaba la teoría clásica, se ve afectada por el descubrimiento de los elementos normativos del tipo y los elementos subjetivos del injusto.

3) Antijuricidad.

Refiere Bustos Ramírez, en relación a la afirmación de Beling que el tipo es ajeno al valor. Explica que la antijuricidad es una lesión objetiva de las normas de valoración; la acción típica surge como la creación de una lesión, en la medida que no hay causas de justificación, con lo cual se verifica la existencia de elementos normativos específicos del tipo.

4) Culpabilidad.

La concepción normativa, es un juicio de reproche al autor por haber realizado un hecho típico y antijurídico, pudiendo haber actuado conforme a lo que ordena el derecho. La culpabilidad además de tener un contenido determinado de carácter psicológico (dolo y culpa), es un juicio de desvalor, la culpabilidad es reproche. Para este doctrina la imputabilidad, el dolo y la culpa son formas de ella.

Para este autor la culpabilidad no se agota en una relación psicológica subjetiva; si no que es, antes que nada, un reproche al sujeto, porque no utilizó si capacidad para actuar conforme al derecho. Por lo tanto, la culpabilidad es un problema valorativo.[274]

[274] Ob. Cit. Daza Gomez, Carlos Pág. 12.

2.4.4.3. LA TEÓRIA FINALISTA DEL DELITO.

Esta teoría nace con la publicación del libro "Derecho Penal Aleman" de Hans Welzel.

El planteamiento del finalismo se vio determinado por la separación entre el mundo de lo real y el derecho- propia del neokantimo- a la realidad del ser social. Por tal motivo se elaboraron las "estructuras lógico-objetivas" previas a toda regulación jurídica y en edificar el derecho sobre la base de la "naturaleza de las cosas". De dicho modo, la teoría de la estructura final de la acción humana se apoyó de forma inmediata en observaciones de la modema sociología sobre el comportamiento de los actos síquicos. Incluso para el conocimiento de los valores acudió la nueva teoría a lo que precede a la existencia humana "el deber ser condicionado, el sujeto responsable, el carácter ordenado del actuar ético social y la concordancia de los órdenes ético sociales".[275]

La teoría de la acción final dio un nuevo contenido al delito; la acción es final y no causa como afirma Welzel "...La finalidad o el carácter final de la acción se basa en que el hombre puede prever, dentro de ciertos limites, las consecuencias de su actividad, proponerse por tanto, fines diversos y dirigir su actividad conforme a su plan. Actividad final es obrar orientado conscientemente a un fin, mientras que el acontecer causal no está dirigido a un fin, sino que es resultante de los componentes causales en cada caso. Por eso la finalidad es vidente, la causalidad es ciega.[276]

Para el finalismo, la acción es el ejercicio final de la actividad humana. En dichas condiciones, la acción no es ciega, sino final, negando la posibilidad de que existan acciones ciegas, o más bien, sin una finalidad determinada de obrar conscientemente.

La fase interna de la acción se plantea con los siguientes elementos:[277]

---

[275] Ob. Cit. Plasecencia Villanueva Raúl. Pág. 40
[276] Ob. Cit. Hans Wlzel. Derecho Penal Aleman" Págs 53 y 54.
[277] Idem. Plascencia Viilanueva Pág. 40

a) El objeto que pretende conseguir;
b) Los medios empleados para su consecución;
c) Las posibles consecuencias secundarias que se vinculan al empleo de los medios que pueden ser relevantes o irrelevantes, desde la perspectiva jurídico penal.

La fase externa se integra de la siguiente manera:[278]

a) Es la puesta en marcha, la dinámica de los medios para realizar el objetivo principal;
b) El resultado previsto y el o los resultados concomitantes, y
c) El nexo o relación causal.

La conducta humana es ejercicio de acción final, por ello, posee una estructura lógico objetiva final: debe ser concepto ontológico.[279] La acción es conducta humana, conducida por la voluntad del sujeto, forman parte de la acción.

La teoría finalista de la acción parte de esta idea: en los tipos de los delitos dolosos o en los culpsos nos hallamos ante dos categorías autónomas, en las cuales la acción presenta diversas estructura ontológica.

Sus elementos son:[280]

1) Acción.

En la teoría finalista, el dolo pertenece a la acción siendo natural y final, apartándolo de la culpabilidad. La antijuricidad es un predicado de la acción.

---

[278] Idem. Pág. 40.
[279] Ontológico (gr on. el ser y logra) Parte de la metafícica que estudia al ser en general y sus propiedades trascendentales. Palomar de Miguel "Diccionario para juristas" Pág. 940. Según cita Daza Gomez Carlos. Pag.48.
[280] Idem. Pag. 49.

2) Tipicidad.

En la tipicidad hay una parte objetiva y una subjetiva del tipo. La primera es la objetivización de la voluntad integrante del dolo, comprende características externas del autor; la parte subjetiva, está formada por el dolo y los elementos subjetivos. El dolo se agota en la finalidad dirigida al tipo objetivo; la antijuricidad no es un elemento del tipo, el dolo no se extiende sobre ella, no comprende el conocimiento de la antijuricidad.

3) La antijuricidad.

Es un juicio de valor el cual expresa que la acción puede ser contraria a la norma y lo será cuando no exista justificación. Toma en cuenta la conducta externa del autor.

Al injusto sólo le importa el fin que el sujeto se ha propueto. Injusto es la acción antijuridica personal referida al autor.

4) Culpabilidad.

Es un juicio de reproche que se formula al autor por no haber adecuado su conducta al derecho, a pesar de que estaba en situación de hacerlo.

Sus componentes son:

a) Imputabilidad.
b) Conocimiento de la antijuricidad.
c) Exigibilidad.

Par los finalistas, la acción es conducida, desde que el sujeto anticipadamente piensa su objeto, eligiendo los medios para lograrlo, finalmente constituye su objetivo con la realización de la acción manifestada en el mundo externo.

La acción humana es el ejercicio de la actividad finalista. La acción es por lo tanto, un acontecimiento "finalista" y no solamente "causal". La finalidad o actividad finalista de la acción se basa en que el hombre, sobre la base de su conocimiento causal, puede prever en determinada escala las consecuencias posibles de una actividad, ademas de proponerse objetivos de distinta indole y seguir su actividad para la obtención de esos objetivos.

Como la finalidad se basa en la capacidad de la voluntad de prever en determinada escala las consecuencias de la intervención causal, y con ello dirigirla hacia la obtención de un objetivo, la voluntad consciente del objeto que dirige el acontecimiento causal, es la espina dorsal de la acción finalista. Ella es el factor de dirección, que sobre determina el acontecimiento causal externo, sin el cual éste, destruido en su estructura material, degeneraría en un proceso causal ciego. Por eso, pertenece también a la acción, la voluntad finalista, como factor que conforma objetivamente el acontecimiento real.

En esta dirección objetiva el acontecimiento causal la voluntad finalista se extiende a todas las consecuencias que el autor debe realizar para la obtención del objetivo; es decir, a:

a) El objeto que quiere alcanzar
b) Los medios que emplea para ello y,
c) Las consecuencias secundarias, que están necesariamente vinculadas con el empleo de los medios.

La actividad finalista no sólo comprende la finalidad de la acción, sino también los medios necesarios y las consecuencias secundarias necesarias vinculadas. La acción finalista es una construcción comprensiva y dividida del acontecimiento, en la cual el objetivo es solamente la parte, al lado de los medios puestos en movimiento y las consecuencias secundarias vinculadas con ellos.

Naturalmente, la dirección finalista se extiende también a la ejecución exterior de la acción misma, de modo que el resultado de la dirección finalista puede agotarse en la actividad simple.

La dirección finalista del acontecer causal es una prestación por la cual el hombre estructura, consciente de su finalidad, las obras de su vida de relación civilizada mismos que pueden ser empleados como objetivos socialmente positivos o negativos.

Por lo que al intercalarse con el derecho penal, prohibiendo la concreción finalista de objetivos socialmente negativos. Acciones finalistas, cuya voluntad de concreción esta dirigida hacia la realización de resultado socialmente negativos, son calificados de antijurídicas por el derecho penal en los tipos de los delitos dolosos, como en los delitos de sangre homicidio y el dolo, como una concepto jurídico, es aquella voluntad finalista de acción que está dirigida hacia la concreción de las características objetivas de un tipo de injusto.

Las acciones que, contempladas en sus consecuencias causales, no observan el mínimo indicado jurídicamente de dirección finalista, son comprendidas por los tipos de los delitos culposos como los delitos de lesiones imprudenciales o negligentes de bienes jurídicos, y por el contrario su tipo de injusto consisten más bien en determinadas lesiones causales de bienes jurídicos, ocasionadas por aquellas acciones que no llevan consigo la cantidad de diligencias necesarias en el intercambio de dirección finalista.

Actualmente el delito es comprendido desde una doble perspectiva: como juicio de desvalor que recae sobre un hecho o acto humano; y también como juicio de desvalor que se hace sobre el autor de ese hecho.

Francisco Muñoz Conde[281] llama al primero injusto o antijuridicidad; al segundo lo denomina culpabilidad o reprochabilidad. Injusto o antijuridicidad. Es, pues, la desaprobación del acto; culpabilidad en cambio es la atribución de dicho acto a su autor para hacerle responsable del mismo.

La acción prohibida y no autorizada es designada por Bacigalup[282] mediante la expresión ilícito (injusto)[283]. Existen dos posiciones para fundamentar el concepto de ilícito; la primera, considera que lo decisivo es la lesión o puesta en peligro de un bien jurídico independientemente de la voluntad del autor (concepto causal de lo ilícito); y la segunda, señala que lo decisivo para el concepto de ilícito es lo que el sujeto quiso realizar (concepto personal del ilícito). A decir de este autor, en la primera postura considera que la verificación de un hecho ilícito se agota en la comprobación de la lesión del bien jurídico que la segunda postura, especifica que la sola comprobación de la lesión del bien jurídico es insuficiente para determinar la existencia de un ilícito penal, ya que la causación de una lesión (resultado) no se diferencia de los hechos de la naturaleza; lo ilícito penal debe expresar un hecho social, y por lo tanto, deberá tomarse en consideración elementos personales.

Siendo entonces para la teoría finalista, " La acción no es sólo un proceso causalmente dependiente de la voluntad, sino por la propia esencia, ejercicio de la actividad final. La finalidad obedece a la capacidad del hombre de prever, dentro de los limites, las consecuencias de su comportamiento causal y conducir el proceso según un plan a la meta perseguida médiente la utilización de recursos" [284]

---

[281] Muñoz Conde, Francisco. Teoría General del Delito. Temis. Bogotá. Colombia 1990. Pág. 189. Según cita de Daza Gomez Carlos. Pág.51.

[282] Bacigalupo, Enrique. Lineamientos de la Teoría del Delito. Hammurabi SLR. Buenos Aires, Argentina 1989. Pág 11.

[283] Generalmente la Teoría del Delito se designa como Teoría del Injusto, expresión de la voz alemana Unrecht que, literalmente significa negación del derecho.

[284] Ob. Cit. Jascheck Hans. pág. 293.

2. 4.4.4. LA TEÓRIA LÓGICO MATEMÁTICO.[285]

Esta posición teórica se base en postulados finalistas, a través de los cuales propone la introducción de un modelo de análisis de los tipos penales, en tal virtud se redimensionan los presupuestos y elementos fundamentales del tipo penal, precisando su contenido y ordenándolos de una mejor manera para facilitar su análisis.

Los principales exponentes son Elpidio Ramírez y Olga Islas.[286] Sus mayores aportaciones se plantean dentro de la estructura general del tipo penal, entendido como "una figura elaborada por el legislador, descriptiva de una clase de eventos antisociales, con un contenido necesario y suficiente para garantizar la protección de uno o más bienes jurídicos"[287], contenido reductible, por medio de análisis, a unidades lógico jurídicas denominadas elementos.

Los elementos del tipo penal son clasificados como únicamente descriptivos o no valorativos, descriptivos y a la vez valorativos, subjetivos y objetivos. Los elementos puramente descriptivos constituyen el objetivo sobre el cual recae la valoración dada en los propios tipos por el legislador. Los valorativos contienen precisamente la valoración legal de ese objeto. Son valorativos: el bien jurídico penal y la violación del deber jurídico penal. Todos los demás son puramente descriptivos.

También se puede hablar de elementos subjetivos y elementos objetivos. Son subjetivos: la voluntabilidad, la imputabilidad, la voluntad dolosa y la voluntad culposa. Son objetivos todos los restantes.

---

[285] Ob. Cit. Plascencia Villanueva Raúl. Teoría del Delito. Págs. 42 y 43.
[286] Islas de Gonzalez Mariscal, Olga y Ramírez Elpidio, La lógica del tipo en el derecho Penal. México, Jurídica Mexicana. 1970. Nota 44. Idem. Plascencia Villanueva raúl Pág. 42
[287] Islas de Gonzalez Mariscal, Olga. Análisis lógico de los delitos contra la vida y la integridad corporal. 2ª Ed., México. Trillas.1985 Pág. 25. Idem. Plascencia Villanueva raúl Pág. 42.

2.4.4.5. LA TEÓRIA DEL FUNCIONALISMO DEL DELITO.[288]

Esta doctrina se fundamenta en la función político criminal del Derecho Penal. Claux Roxin es el máximo exponente de esta doctrina; retoma el pensamiento de Von Liszt sobre la política criminal, utilizando esta postura para sustentar: "El fin de la pena es la prevención general".

Lo más sobresaliente de esta teoría es que pone en tela de juicio la culpabilidad normativa, aportando la imputación personal, sustentada en la prevención general como fin de la pena. Es decir, proponen un cambio en la fundamentación de la culpabilidad al señalar que se supera la pugna entre el libre albedrío y determinismo. Destacando la imputación objetiva y subjetiva a nivel de tipicidad.

Günther Jakobs es radical al proponer un funcionalismo que sustituye la base ontológica del finalismo, por un fundamento normativo.

2.4.4.6. LA TEORÍA DE LA IMPUTACIÓN OBJETIVA.[289]

Se ocupa de problemas principales de la estructura general del delito. Según la opinión de sus partidarios, ella se ha convertido en la teoría ampliamente dominante en la ciencia del derecho penal posrfinalista. En la jurisprudencia de los altos tribunales alemanes, por el contrario, ella busca aún, en vano, un reconocimiento.[290] Sus partidarios, en verdad, se broncean anticipadamente de la media luz de expresiones de la Corte Suprema argumentativamente débiles y que necesitan ser interpretadas.

---

[288] Ob. Cit. Daza Gomez Carlos. Teoría General del Delito. Pág. 50.

[289] Eberhard Struensee. Temas sobre Teoría del Delito. Instituto Nacional de Ciencias Penales. México. 1999.Pág. 11 y ss.

[290] De otro modo en Autria, cfr., triffterer, Klug- Festschrift, 1983, pp. 419, 423. Según cita Eberhard Struensee. Temas sobre Teoría del Delito. Pág.11

En un viraje decisivo en contra del presunto (subjetivismo) de la teoría finalista del tipo e ilícito[291], la teoría de imputación objetiva propaga el grito de guerra (¡regresemos al tipo objetivo!) Junto a ello conduce, sin embargo, la consecuencia más manifiesta del finalismo: el dolo es un elemento constitutivo del tipo del delito. Con ello vale: quien cuenta al dolo en tipo subjetivo, es finalista.[292]

En el nivel de tipo, la teoría de la imputación objetiva no queda, por lo tanto, atrás de la teoría final de la acción. Ello, por el contrario, puja en un (hiper-subjetivismo), dentro del cual- forzosamente- toma en cuenta (lo subjetivo en la imputación objetiva)[293], es decir, lo admite como elemento conceptual del tipo objetivo. El finalismo nunca se atrevió en misterios semejantes.

Karl Larenz atribuye al concepto de imputación objetiva, la función de separar entre hecho propio y accidente, denominado imputación objetiva al (juicio sobre la cuestión de sí un suceso puede ser atribuido a un sujeto como propio), juicio este independiente del que decide sobre la existencia o no de nexo causal.[294]

La imputación objetiva se convierte en un juicio teleológico. Habrá que determinar si el acontecer puesto en marcha por el autor estuvo o pudo estar dirigido a la voluntad de éste hacia la consecución de un determinado fin. Las características individuales del autor sólo serán tomadas en cuenta al llegar a la culpabilidad. Con esto, Larenz evita la confusión entre imputación a hecho e imputación a la culpabilidad de la que adolecía la Teoría de la Acción de los Hegelianos.[295]

---

[291] Roxin, Strafrecht, Allgemeiner Teil, Band I, 2ª ed. 1994. Págs. 24 y 25. Idem Pág. 11

[292] Cfr., Niese, finalität, Vorsatz und Fahrlässigkeit, 1951, pág. 11. Idem. Pág. 12

[293] Roxin, Chengchi law Review, vol 50, 1994, pág. 232. Idem. Pág. 12.

[294] Martínez Escamilla, Margarita. La imputación objetiva del resultado. Edersa, Madrid, España. 1992. Págs 19 y 20. Según cita de Daza Gomez Carlos. Pág. 97

[295] Idem. Pág. 21 Según Cita de Daza Gomez. Pág. 97.

2.4.4.7. LA TEORÍA DE LA ACCIÓN SOCIAL.[296]

Esta teoría es exclusivamente una teoría de la acción, es decir, su objetivo exclusivo es ofrecer un concepto unitario de la acción, en el que habrían fracasado tanto los casusalistas como los finalistas, y no una estructura sistemática del delito distinta a las ya vistas y deducida de su nuevo concepto de acción. Por eso suele decirse que la teoría de la acción social es una síntesis ente el concepto causal y el concepto final de acción, aunque con respecto a los restantes elementos del delito nada dice, o mejor dicho, sus principios defensores dicen que (no es posible derivar del concepto social de acción consecuencias dogmáticas para la estructura de los conceptos de antijuricidad y culpabilidad) (Jeschek). No extraña, por tanto, que ese concepto social de acción haya sido asumido tanto por causalistas como por finalistas ("heterodoxos" en ambos casos, por haber renunciado al concepto de acción de su propia Escuela).

La acción se define directamente como comportamiento humano socialmente relevante. Acción es, pues, conducta dotada de significación social. Y ello es, ciertamente común a las tres formas de aparición del delito: en los delitos dolosos de comisión ese comportamiento humano socialmente relevante consiste en la finalidad actual o ejercicio de actividad final; en los imprudentes de comisión consiste en la causación de resultados con posibilidad de dirigir el proceso causal (se acentúan así sus componentes causales); en los de delitos omisivos, el comportamiento humano socialmente relevante consiste en la inactividad frente a la acción esperada: hay una dirección contra la acción que el Derecho espera que se realice, y que podía realizarse. Es, pues, una capacidad de acción, puesto que el punto de referencia es la "acción esperada por el Derecho", y no la mera omisión o inactividad.

---

[296] Gómez Benitez José Manuel. Teoría Jurídica del Delito. DerechoPenal. Parte General. Edt. Civitas, Madrid, 1988. Pág. 54.

Resulta evidente que este concepto de la acción se confunde con el de tipicidad, puesto que la relevancia social se deduce precisamente de la tipicidad de un hecho. En tal caso, la teoría de la acción social no está ofreciendo una teoría de la acción, sino de la tipicidad. Desde luego que nada hay que objetar contra una concepción del tipo que lo dota de contenido de relevancia social. Sólo que esa no es la pretensión de la teoría de la acción social: su pretensión era definir la acción y no la tipicidad de la acción. Para el estudio de la acción es intrascendente la forma de la acción (dolosa, imprudente u omisiva); lo único que es trascendente es que se dé su denominador común, es decir, que se trate de comportamientos humanos. Es exactamente lo que dijo el concepto neoclásico de acción causal, aunque pueda discreparse en cuanto a lo que se entiende por "comportamiento".

CAPITULO III.

CONSIDERACIONES SOBRE EL SUJETO ACTIVO EN LOS DELITOS INFORMÁTICOS.

3. GENERALIDADES DE LOS DELINCUENTES INFORMATICOS.

Se ha podido observar que los delitos por computadora se cometen por un amplio rango de personas: estudiantes, aficionados, empleados, terroristas y miembros de grupos del crimen organizado. Lo que los distingue es la naturaleza del delito cometido. El individuo que logra el acceso a un sistema de computación sin intención criminal es muy diferente al empleado de una institución financiera que toma pequeñas cantidades de dinero de las cuentas de los clientes.

El típico nivel de destreza del delincuente informático es un tema de controversia. Ya que algunos afirman que el nivel de destreza no es un indicador, mientras que otros aseguran que este tipo de criminales son sujetos brillantes, ambiciosos, altamente motivados y dispuestos a aceptar un reto tecnológico, características que también son altamente deseables en un empleado en el campo de la informática y procesamiento de datos.

Es real que la conducta delictiva en este ramo atraviesa un amplio espectro de la sociedad, la edad de los ofensores va desde los 10 hasta los 60 años y su nivel de destreza va desde el aficionado hasta el profesional. Estos delincuentes, por tanto, son personas promedio más que super criminales que poseen habilidades y talentos únicos.

Cualquier persona con un mínimo de destreza, motivada por el reto tecnológico, lucro, notoriedad o venganza, o por la promoción de creencias ideológicas, podría ser un sujeto activo en potencia.

De acuerdo a varios estudios, podemos ver que los empleados representan la mayor amenaza y por lo mismo el delito por computadoras es frecuentemente referido como delito interno. Un estudio calculó que el 90 por ciento de los delitos económicos cometidos por computadora fueron realizados por empleados de las compañías víctimas. Una investigación reciente efectuada en Norteamérica y Europa indicó que el 73 por ciento del riesgo en la seguridad en computación era atribuible a fuentes internas y sólo el 23 por ciento a actividad criminal externa.[297]

Conforme continúan los avances en el procesamiento de datos a distancia, la amenaza de fuentes externas se a incrementado. Con el aumento de sistemas de conexiones y de programas más accesibles, puede cambiar el perfil sociológico de los ofensores.

Debido a la gran complejidad de ciertas rutinas de computación y el aumento en las medidas de seguridad, es difícil que cualquier persona posea toda la información necesaria para usar un sistema con propósitos criminales. Los grupos de delincuencia organizada, compuestos por miembros de todo el mundo, están empezando a surgir. En correspondencia a este incremento en la cooperación en la actividad criminal, se ha detectado el cada vez más frecuente uso de pizarrones electrónicos para la comunicación clandestina criminal o la encriptación de sonidos o imágenes que contiene información utilizada por esta delincuencia. La rápida escalada de la tecnología en telecomunicaciones ha añadido una amenaza de las fuentes externas. Los sistemas de correo de voz basados en sistemas de computación, por ejemplo, están siendo usados para cambiar números de acceso robados, contraseñas y programas.

Como podemos ver claramente la delincuencia organizada, se esta valiendo de esta tecnología para llegar a sus fines, entre lo que podemos señalar.

[297] Manual de Naciones Unidas sobre la Prevención y control de delitos relacionados con la computadora. Revisión internacional de política criminal. 9 de mayo de 1996. Area de Traducción e Idiomas del Instituto de Formación Profesional de la Procuraduría General de Justicia del Distrito Federal. Coordinadora Beatriz Macin Lara. Julio del 2000. Pág. 18.

Que hay factores transnacionales de "Globalización" relacionados con:[298]

La Delincuencia Organizada.
- Soberanía Nacional.
- Factores Sociales y Político.
- Estructura y Efectos Económicos.
- Efecto de Dispersión.
- El creciente Mercado.
- Lucro.

Además de otros aspectos importantes que tienen repercusión mundial relacionados con delitos cometidos por el Crimen Organizado Transnacional, siendo entre otros.

a) El Trafico de Armas.
b) Ilícitos de Emigrantes.
c) Trata de Mujeres y Niños.
d) Narcotráfico.
e) Corrupción.
f) Lavado de dinero.

Los criminales en computación han ganado notoriedad en los medios y parece que han obtenido más aceptabilidad social que los criminales tradicionales. La idea de que estos delincuentes son individuos menos dañinos, sin embargo, se ignora lo obvio. La amenaza actual es real. La amenaza futura será directamente proporcional a los avances hechos en la tecnología computacional.

Por lo que al hablar del Sujeto Activo de un delito informático, no es hablar de un delincuente común. Dichos sujetos tienen como características: [299]

[298] Seminario México-EUA sobre" Crimen Organizado Trasnacional", celebrado en el auditorio Alfonso Quiroz Cuarón del Instituto Nacional de Ciencias Penales el día 11 de Agosto del 2000. Presentado por el Dr. Alan Brock, Universidad Estatal de Pennsylvania. Así como los Penalistas. Lic. Eduardo Ibarrola y Mtro. José Trinidad Larrieta de la Procuraduría General de la República, Dr. Jorge Chabat del Centro de Investigación y Docencia Económica, Dra. Celia Toro, Colegio de México, Ernesto López Portillo, Instituto Nacional de Ciencias Penales y Lic. Raúl Roldan, Agregado Jurídico de la Embajada de los Estados Unidos de América.
[299] Ob. Cit. Viega Rodríguez, María José "Delitos informáticos". Pág. 4.

a) Poseen importantes conocimientos de informática.

b) Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible, se les ha denominado delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema.

c) A pesar de las características anteriores debemos tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

d) Las opiniones en cuanto a la tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional a nivel informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

e) Estos delitos se han calificado de "cuello blanco", porque el sujeto que comete el delito es una persona de cierto status socioeconómico.

La "cifra negra" es muy alta. No es fácil descubrirlo ni sancionarlo, en razón del poder económico de quienes lo cometen y también es importante destacar que los daños económicos son altísimos. Se habla de pérdidas anuales por delitos informáticos y otros tecno-crímenes, que van desde los U$S 100 millones (Cámara de Comercio de los Estados Unidos) hasta la suma de U$S 5.000 millones, de acuerdo a un estudio de 1990 hecho por una firma auditora. [300]

[300] Idem. Viega Rodríguez, María José "Delitos informáticos".Pág. 5

PACHECO KLEIN nos dice: "Otro estudio estimó que sólo el 1% de los robos de computadora son detectados, y quizá sólo un 15 % de ellos sean denunciados. Cuando los delitos informáticos son denunciados y llevados a juicio, muchos de ellos son negociados fuera del juzgado; sólo alrededor del 24 % van realmente a juicio, y alrededor de dos tercios de esos juicios resultan en la absolución y el archivo del expediente."[301]
Un punto importante es que la opinión pública no considera delincuentes a estos sujetos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario el autor de estos delitos distingue entre el daño a las personas (que es inmoral) y el daño a las organizaciones, porque en este último caso sienten que "hacen justicia", se le ha llamado a este punto de vista el síndrome de Robin Hood.[302]

3.1. CLASIFACACION DE LOS DELINCUENTES INFORMATICOS.

Para algunos autores el sujeto activo del delito informático tiene un nombre y una clasificación, según sus características y finalidad del sujeto.

a) Hacker.

Hackers, es un término en inglés con el que se define a las personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, y apenas constituyen una muestra de la nueva faceta de la criminalidad: El delincuente silencioso o tecnológico.[303]

---

[301] Idem. Pág. 5
[302] Idem. Pág. 6.
[303] Jiménez Dan, Rafael Ricardo Gerente de Tecnologías del Proyecto de Modernización de la Corte Suprema de Venezuela. (Venezuela) "Crimen Silencioso". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), (www.yahoo.com). Pág. 1.

Según alguna opinión [304] la actividad del Hacker consiste en interceptar en forma dolosa un sistema informático para apoderarse, interferir, dañar, destruir, conocer, difundir o hacer uso de la información que se encuentra almacenada en los ordenadores pertenecientes a instituciones públicas y privadas, de seguridad, entidades financieras y usuarios particulares.

Otra definición más menos agresiva los cataloga como "auténticos genios de la informática, entran sin permiso en ordenadores y redes, husmean, rastrean y a veces, dejan tarjetas de visita. Los Hacker, posmodernos corsarios de la red, son la última avanzada de la delincuencia informática de este final de siglo."[305]

Entre otras aportaciones y definiciones que se han hecho de los hacker, señalaremos las siguientes:

No sólo es hacker aquel que decide utilizar su conexión a un sistema de red para acceder a todo tipo de datos, por ocultos que éstos se encuentren. También puede serlo el que es capaz de modificar el código de un programa para adaptarlo a sus necesidades. Y ya fuera de la informática, y en la línea de lo que mantiene ERIC S. RAYMOND en el documento "Cómo transformarse en un hacker", podríamos considerar hacker a cualquier heterodoxo, que ya desde niño quiere ir más allá del libro de instrucciones, y es capaz de desmontar un reloj para volver a montarlo. Los investigadores científicos que viven para su trabajo, los genetistas que son capaces de explorar hasta la última cadena de ADN en busca del gen que causa una enfermedad concreta, también han de merecer nuestra consideración. Quizás Leonardo da Vinci fue un hacker de su tiempo.[306]

---

[304] Rudi, Jorge Adrián. "Introducción al Derecho Penal Informático", ED, T° 157, pág. 856. Según cita de Villalba Díaz, Federico Andrés. Abogado y Secretario Judicial de la Fiscalía de Primera Instancia en lo Contravencional N° 10. Titular de Derecho de Autor y Marca de la Facultad de Ciencias Jurídicas de la Universidad Abierta Interamericana. "Argentina: Los delitos y contravenciones informáticas. Los Hackers y el Código Contravencional de la Ciudad de Buenos Aires". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), (www.yahoo.com). Pág. 2.

[305] Ricardo Levene (nieto) y Alicia Charavalloti en "Delitos Informáticos (segunda parte) en el diario La Ley del día 11 de noviembre de 1998, pág. 1.- Según cita de Villalba Díaz, Federico Andrés. Pág. 2

[306] Almeida, Carlos Sánchez. Bufete Almeida "El Hacking ante el Derecho Penal. Una visión Libertaria". http://www.bufetalmeida.com (España) Pág. 3.

Es hacker la persona que es capaz de explorar un sistema hasta sus lugares más recónditos, en busca del conocimiento. Es aquel que no se conforma con lo obvio, que tiene una visión de las cosas que pasan por desapercibidas al resto de los mortales. Es aquel que puede tener una comprensión de la totalidad, que no está mutilada por el conocimiento específico. Es aquel que puede ver lo que otros no han podido imaginar, ni tan siquiera soñar. [307]

"El computador es un factor criminógeno de primera magnitud que aporta a la conducta criminal, unas veces, un nuevo objeto (la información misma, potenciada y revaluada por los nuevos sistemas de procesamiento de datos y los programas), y otras, un nuevo instrumento: ofreciendo un inmenso abanico de técnicas y estrategias que pueden ponerse al servicio del delito, enriqueciendo el repertorio criminal." Esta acertada distinción permite precisar cuando la tecnología es medio y cuando objeto del delito.[308]

Es común la expresión "La información cuesta", lo que refleja la apetecibilidad y atractivo que en la actualidad representa el manejar datos claves, es la información como elemento de conocimiento, poder y fortuna. Cuando la información se convierte en objeto de apropiación y en blanco lucrativo del delincuente, se ven afectados valiosos bienes jurídicos como la intimidad, el orden socioeconómico, la fe pública y la seguridad del estado, entre otros.

En el mismo sentido, debemos señalar que las nuevas tecnologías se convierten en instrumentos del delito, cuando sus técnicas y sofisticadas herramientas para el tratamiento automatizado de la información se utilizan como medio de comisión de acciones generadoras de importantes daños y lesiones, patrimoniales o no, a personas y organizaciones.

---

[307] Idem. Pág. 3

[308] Evento celebrado en Caracas, la Profesora Española Mariluz Gutiérrez Francés refería en su ponencia titulada "Incidencia de las Nuevas Tecnologías de la Información en el Derecho Penal", Según cita de Jiménez Dan, Rafael Ricado. "Crimen Silencioso". Pág. 1.

Son varios los elementos que hacen atractiva la comisión de estos delitos. El primero de estos elementos es la relativa facilidad con que un experto informático puede perpetrar estas acciones, las cuales requieren del manejo de conocimientos y herramientas especiales que, en la mayoría de los casos, son de dominio exclusivo de personal técnico.[309]

Una aproximación al perfil criminológico del delincuente informático apunta hacia un individuo normalmente del sexo masculino, en edades comprendidas entre los catorce y treinta años, experto en el manejo de nuevas tecnologías, con un altísimo potencial intelectual y en muchos casos empleado de confianza habituado a trabajar sobre tiempo. El delincuente tecnológico comúnmente asume una actitud de reto con los sistemas a que se enfrenta, de modo tal que considera suficientemente justificado el lucro que obtiene, como recompensa a su pericia e inteligencia. [310]

El Profesor Chileno Claudio Líbano Manzur nos señala que:[311]

El delito de hacking, por constituir fundamentalmente es un acceso indebido o no autorizado, induce a la creencia, no errada por cierto, de que este ilícito se presentará como medio o herramienta de comisión de otros delitos informáticos ya tratados, y que, por lo tanto, su característica podría ser la de configurarse como un hecho delictivo necesario para la comisión de otros.

Es indudable que muchas veces el hacker (persona que comete el delito de hacking) utiliza el acceso indebido a un sistema de tratamiento de la información con el fin de cometer un fraude informático, un espionaje de datos, piratería o sabotaje en sus distintas manifestaciones. En estos casos el ánimo del delincuente será cometer estos delitos y la violación a la prohibición de acceso no será más que un medio de consumación. Ante esta primera situación motivacional es necesario precisar que para que exista hacking, éste debe estar tipificado de alguna forma en una ley.

---

[309] Ob. Cit. Jiménez Dan, Rafael Ricado. "Crimen Silencioso". Pág. 2
[310] Idem. Pág. 2.
[311] Ob. Cit Líbano Manzur, Claudio. Pág. 1.

Un segundo supuesto motivacional del hacker estará determinado por un ánimo que podríamos llamar "no dañoso". En efecto, es posible, y así ha ocurrido muchas veces, que el delincuente busque la violación de la negativa al acceso, entiéndase códigos, passwords, etc., como una forma de autoratificación de sus capacidades técnicas e intelectuales. El hacker perseguirá la satisfacción de lograr vencer un obstáculo y de demostrar que los programadores que dispusieron las medidas de seguridad no pudieron contra su inteligencia. Asimismo, dentro de esta motivación "no dañosa", se encuentran los hackers que buscan burlar los códigos de acceso con la finalidad del simple divertimiento o por razones de curiosidad. Estas conductas, a pesar de no causar un daño directo y tangible, son delitos en si mismas y deben, necesariamente, estar reguladas y sancionadas.

Por otro lado el Uruguayo Andrés Fígoli Pacheco son señala que:[312]

La realidad obliga a hacer una distinción, muy frágil en algunos casos. El hacker es una persona que disfruta de explorar los detalles de los sistemas programables y aprendiendo a usarlos al máximo, al contrario del usuario común, que prefiere aprender el mínimo necesario.[313] Infringe las medidas de seguridad, pero no destruye, no daña. El hacerlo iría en contra de su prioritaria intención de mezclarse con el usuario normal y atraería la atención sobre su presencia, haciendo que su puerta de ingreso sea cerrada.

b) Craker.

El cracker es "hacker malicioso" que utiliza sus conocimientos para obtener beneficios, o simplemente por causar daños. En realidad se trata de una división artificial (acuñada en 1985 por los hackers para diferenciarse), puesto que la línea que los separa es muy débil. En efecto, la intencionalidad aunque en un inicio puede ser sólo el ingresar, puede derivar en obstaculizar el sistema informático, a través de un sabotaje.

---

[312] Ob. Cit. Fígoli Pacheco, Andres. Págs. 3 y ss

[313] Eric S. Raymond, "The New Hacker's Dictionary", tercera edición, noviembre de 1996 Según cita de Fígiolo Pacheco Andrés Pág. 4.

Las motivaciones que mueven tanto a un hacker como a un cracker pueden ser variadas:

a) Sociales: Tratan de ganar la aceptación de su propio grupo social. Aquí se confunden el sentimiento de superioridad con el poder de control sobre los demás, compitiendo y a su vez cooperando entre ellos.

b) Técnicas: El fin perseguido es demostrar las fallas de los sistemas que, según ellos, fueron dejadas intencionalmente. A la vez que ellos mismos aprenden, exponen las puertas abiertas halladas luego de su "investigación científica". Ayudan al progreso de la tecnología, forzando a la industria tecnológica a mejorar sus productos. Estos son los menos y muchos tratan de esconderse tras esta excusa.

c) Políticas: Son los que tienen firmes convicciones políticas. Así lo confirman las intrusiones a los sites de Palacio de Planalto y del Supremo Tribunal Federal brasileño en Julio de este año, o al Centro de Investigaciones Atómicas de Bombay durante los incidentes indo-pakistanies, para dejar sus manifiestos políticos en las páginas web. Generalmente, tiene amplia difusión periodística lo que ayuda a propagar su causa. Se le llama hacktivismo político, pudiendo derivar en ciberterrorismo.

d) Económicas : Se aprecia en el fraude y el espionaje informático tanto por parte de empresas competidoras, como por aquellos que se valen del chantaje para no revelar secretos o sabotear el sistema vulnerado.

Sin embargo, la mayor amenaza no proviene de afuera, sino de los llamados insiders, el propio empleado de la empresa que es movido usualmente por la venganza. Serían los responsables de la mayoría de los ataques frente a un 17% asignados a los hackers, según una encuesta realizada a 148 instituciones brasileñas durante el mes de julio de este año, por parte de Modulo Security Solutions..[314]

[314] "Raio X do Hacker brasileiro", Revista Veja, Brasil, 14 de julio de 1999, pág. 82. Según Cita de Fígiolo Pacheco Andrés Pág. 4.

Últimamente, se ha detectado intentos de hurto informático de las listas de usuarios de los servidores. Estas revisten especial importancia para fines político electorales y comerciales.

e) Laborales: Comprende a aquellos que buscan un empleo demostrando que son mejores que los que diseñaron el sistema de seguridad que vulneran. También abarca a los que son contratados o bajo promesa de una recompensa ponen a prueba las nuevas medidas de seguridad de los sistemas informáticos.

f) Gubernamentales: Son los cometidos por un gobierno contra otro. Fue el caso de la guerra del Golfo y la reciente guerra de los Balcanes. Es lo que se llama "Information warfare", como el espionaje por parte de los servicios de inteligencia. Por supuesto, que estos casos raramente salen a la luz.

Un rasgo que ha caracterizado al hacker en estos últimos años es la buena comunicación que muchas veces se mantiene entre ellos. Uno de mejores canales usados es el IRC (Internet Relay Chat). Allí, es donde pueden recibir las primeras lecciones, conocer otras personas para formar grupos e intercambiar información. El IRC es anónimo. El hacker nunca quiere revelar su verdadera identidad ni tampoco quiere ser rastreado (curiosamente este es unos de los problemas que tenían las revistas de hackers on-line para encontrar suscriptores).

Existen cerca de 30.000 paginas web en la Internet dedicadas al hacking. En estas, se puede conseguir cualquier tipo información acerca del "arte del hack". Esto genera como interrogante si sigue vigente el encasillamiento de los delitos informáticos en general como "delitos de cuello blanco" (Sutherland). Se podría decir que ya no es necesario poseer ciertos conocimientos ni disponer de un rico patrimonio para convertirse en hacker, sino tan solo de tiempo. Una persona con medianos conocimientos en Informática, obteniendo los recursos necesarios en cualquier sitio web de la Internet no sería un mal candidato. Incluso, puede optar por cursar en alguna escuela de hacking on-

line, si desea perfeccionarse. Es lo que más de uno no ha dudado en calificar como la "democratización del hacking".

Sin embargo, se puede hablar de otra definición la cual es la que traza una diferencia según los objetivos de quienes invaden la red con fines no permitidos.

En la revista especializada PC USER [315] tratan, con fundamentos éticos y filosóficos, cual es la diferencia entre el que utiliza los recursos informáticos para causar daño y los que hacen uso de ellos a solo efecto de romper las barreras del conocimiento.

Según dicha publicación el CRAKER es la persona que ingresa ilegalmente a un sistema informático para robar o destruir información o simplemente para causar desorden. También se llama cracker a quien descifra los esquemas de protección anti-copia de los programas comerciales para así poder utilizar o vender copias ilegales. La misma edición cataloga a los HACKERS con cinco acepciones, definiendo la primera como personas que disfrutan investigando detalles de los sistemas operativos y los programas, buscando nuevas formas de aumentar sus capacidades.

En el sitio THE HACKER FAQ (www.solon.com), citado por la misma publicación, "se dice que los hackers no son aquellos que violan la seguridad de los sistemas. Estos son los crackers. Los hackers disfrutan jugando con las computadoras. Pasan mucho tiempo observando un sistema para saber todo sobre él, sobre sus medidas de seguridad. Pero no lo hacen con malicia, sino por simple seguridad".[316]

Según esta última definición el accionar de un hacker no es robar, sino obtener información sobre un sistema. El problema surge cuando esa información o acceso a la misma, es restringida. En este caso, el hacker no admite limitaciones y procurará traspasar todas las barreras por medio de técnicas denominadas por ellos mismos como "ingeniería social" que consiste en utilizar cualquier medio informático para acceder a las

[315] Ob. Cit. Villalba Díaz, Federico Andrés " Los delitos y contravenciones informáticas. Los Hackers y el Código Contravencional de la Ciudad de Buenos Aires". Pág. 3.
[316] Idem. Pág. 3

claves de acceso de cualquier fuente de información. En el Manual de cómo Hackear (The How to Hack Manual en www.madnes.org) se acusa que hay muchos en la red (crackers) que se autodenomina hacker y deliberadamente causa daño en los sistemas.[317]

De igual forma la Profesora en Derecho Penal Esther Morón Lerma nos indica que:[318]

El cracker es, aprorísticamente, un autodidacta de la informática, que sin los conocimientos del hacker intenta emularlo. El craking suele ser la conducta posterior a la de haking o de mero intrusismo informático.

El cracker desconoce los sistemas informáticos y sus retos se limitan a la vulneración del sofware comercial cometiendo conductas de (piratería informática). Las conductas habituales de los crackers se basan en la copia in consentida de programas informáticos vulnerando sus derechos de autor.

c) Cyberpunks.

Las conductas que los usuarios de la Red identifican con las propias de los vándalos electrónicos o cyberpunks, suelen venir preordenadas por el específico ánimo de destrucción de datos, programas o soportes informáticos.

Se ha establecido como uno de los parámetros diferenciadores entre el hacker y cracker el de los conocimientos informáticos, el cyberpunk podría diferenciarse como un cracker cuyo único fin es la entrada in consentida en sistemas informáticos (conductas típicas de hack) mediando la corrupción de un password (conducta típica de crack) para destruir datos o implementar en el sistema informático un virus o bomba lógica, que destruya los mismos.

---

[317] Idem. Pág. 3.

[318] Morón Lerma Esther, Profesora de Derecho Penal, Universidad Autónoma de Barcelona. Internet y Derecho: (hacking) y Otras Conductas Ilícitas en la Red. Edt. Arazandi, S.A. 1999. Pamplona España. Pág. 32.

d) Sniffers.

También podemos hablar de los Sniffers, como una forma de invasión de la vida privada particularmente insidiosa es la que puede producirse en Internet a través del uso de programas rastreadores o sniffers, que suelen ser usados para penetrar en el disco duro de los ordenadores conectados a la red, buscando cierto tipo de información.

Los programas sniffers, por lo tanto, se fundamentan en la posibilidad de poder rastrear información en la red. El uso de sniffers permite el control in consentido del correo electrónico en la red.

e) Spamming.

También existen conductas conocidas como spamming, o envío in consentido de mensajes publicitarios por correo electrónico a una multitud de desconocidos.

La técnica del spammig suele llevar aparejada, como ilícito antesala, la monitorización de conductas en la red.

f) Phreacker.

En castellano se denomina pirata, que manipula esencialmente los sistemas informáticos de las compañías de teléfonos, ahorrándose una considerable cantidad de dinero, puesto que activa teléfonos convencionales piratas y además teléfonos celulares, constituyendo un grado de peligro para las empresas que manejan esta línea comercial. [319]

[319] Soto Galvez. Gerardo. La Necesidad de Reforma de la Ley Penal Federal ante la Impunidad de los Delitos Informáticos. Tesis de Licenciatura Universidad del Valle de Atemajac. Guadalajara Jalisco. 1997. Según Cita de Restra Gaytán Emma "Los Delitos Informáticos en el Derecho Positivo Mexicano" Pág. 31.

g) Lammer.

Connota a la persona que su especialidad radica en utilizar códigos fuente de otros programas para beneficio (una especie de plagio electrónico) propio sin hacer mención del copyright (derechos de autor).[320]

h) Rootkis.

Es la persona que se vele de un programa que se encarga de borrar o enmascarar las huellas dejadas después de introducirse en un sistema. Estas huellas se encuentran en los ficheros guardando todas las operaciones hechas por un usuario (entrar, salir, ejecutar un programa, etc).

I) Graffitis.

Deriva de la palabra gráfico, y su conducta esencial estriba en rayar los sistemas informáticos, al igual que en nuestra actualidad se rayan las paredes, estos se dedican a decorar la pagina web (se le denomina así al servidor que sirve de conducto para leer información)con sus creaciones pintorescas.

Por lo que podemos indicar que la fenomenología en la mayor parte de la delincuencia informática platea serios problemas relacionados con una cifra negra relacionada con la criminalidad informática. Toda vez que este tipo de conductas, son en la mayoría de los casos desconocidas por las víctimas por las dificultades de orden técnico o de conocimiento, o muchas de las ocasiones ocultan dichas conductas por el temor de la trascendencia del hecho que en muchas de las veces se traduce al descrédito de su negocio o de la propia empresa y en su mismo prestigio, prefiriendo resolver el problema internamente, sin acudir a la autoridad competente para que investigue dichos hechos.

[320] Idem. Pág. 31.

Teniendo entre otros problemas jurídicos la falta de regulación de este tipo de conductas en nuestros ordenamientos jurídicos, así como su dificultad que se tiene para descubrir, investigar o perseguir este tipo de delitos, aunado a todo esto la falta de conocimiento y capacitación de las autoridades policiales, ministeriales y judiciales.

Por lo que podemos ver que la generalidad de este tipo de conductas tienen distinta calificación o reproche en virtud de la forma o fin en que se cometen este tipo de delitos, por lo que es muy importante tomar en cuenta los estudios criminológicos que se han hecho al respecto apoyando las propuestas de los penalistas y técnicos en seguridad informática.

Siendo de suma importancia hablar de lo que es la criminología y como nos auxilia en este tipo conductas delictivas.

3.2. IMPORTANCIA DE LA CRIMINOLOGÍA EN LOS DELITOS INFORMÁTICOS.

Durante la historia esta ciencia ha sido motivo de discusión el designar a esta rama del conocimiento con el nombre de Criminología, ya que el significado del término es un tanto restringido con relación al enorme campo de estudio de esta materia, es decir, la mención del nombre nos puede inducir a pensar que se refiere exclusivamente al estudio del crimen, lo cual a originado controversias. En efecto, en varios países no existe diferencia entre "crimen" y "delito"; mientras que en otros se hace distinción entre "crímenes", "delitos", y "faltas", considerando que los primeros se refieren a conductas antisociales de gravedad mayor (como el homicidio), y los segundos, están constituidos por aquellas actividades ilícitas de menor importancia (como calumnias y amenazas), entre tanto que las faltas se refieren en términos generales a contravenciones a disposiciones administrativas.

En México, para la Criminología, el crimen es la acción del hombre que lleva a cabo conductas antisociales, e incluye al delito "como la acción u omisión que sancionan las leyes penales".[321]

Los propios criminólogos, parecen apoyar la idea de que la Criminología sólo se ocupa de los crímenes y que estos no comprenden a todos los delitos, pues sus principales investigaciones acerca de la criminalidad las realizan alrededor de homicidios, lesiones, violaciones o robos, marginando gran cantidad de delitos que sin duda también quedan comprendidos dentro del campo de estudio de los factores bio – psico – sociales, como en el caso de los delitos informáticos.

a) Concepto de Criminología.

Puede definirse la Criminología como " Como una disciplina científica autónoma –no jurídica- que estudia las conductas humanas peligrosas y es a la vez investigadora de sus causas. (Francisco P. Laplaza)"[322].

Es una ciencia sintética, causal explicativa, natural y cultural, que analiza e investiga las causas y factores que conforman un pensamiento criminal y su expresión en conductas antisociales.[323]

Es una ciencia, en virtud de que tiene objeto y métodos propios, así como fines específicos.

---

[321] Artículo 7 del Código Penal para el Distrito Federal.

[322] Basile Alejandro, A. Fundamentos de Medicina Legal: deontología y bioética -3ª Ed. Buenos Aires: El ateneo 1999. Pág. 164.

[323] Manual de Fundamentos Técnicos y Científicos para la Investigación Policial. Instituto de Formación Profesional, Procuraduría General de Justicia del Distrito Federal. Mayo del 2000. Pág.46.

Es sintética, ya que se trata de una ciencia a la que concurren varias disciplinas científicas como la Biología, Sociología, Psicología, Antropología, etc. Pero todas en estrecha interdependencia, no es un conjunto de ciencias sino una síntesis, un todo coherente para explicar las causas, factores y motivos de las conductas antisociales.

Se trata e una ciencia causal explicativa, porque pretende descubrir las causas y factores que influyen en el fenómeno criminal y explicar con principios o leyes tales fenómenos y buscar la prevención del delito.

Es natural o cultural, ya que la Criminología estudia la conducta criminal como un hecho o acaecer de orden natural, atribuida al hombre como un ser de la naturaleza; y es cultural porque además de la individualidad biológica natural, el delito (la conducta antisocial) es un producto social, es decir, de orden cultural.

De igual forma García Pablos de Molina define a la Criminología como "La Ciencia interdisciplinaria que se ocupa del crimen, el delincuente, la víctima y el control social del comportamiento desviado".[324]

El carácter interdisciplinario de esta ciencia implica sus relaciones con:

1.- El Derecho, que trata de las penas y medidas de seguridad que se deben aplicar a quienes incurren en conductas tipificadas como delitos en la ley penal.

2.- La Psicología y La Psiquiatría, que estudian la conducta normal y patológica, y, por tanto, la conducta delictiva como forma desviante del comportamiento humano.

3.- La Medicina Legal, en la medida que sirve de puente entre la medicina (en este caso la psiquiatría y la psicología médica) y el Derecho, auxiliando a la procuración y administración de justicia con el concurso del método pericial.

---

[324] García- Pablos de Molina, A. Manual de Criminología (Introducción y teorías de la criminalidad). Espasa- Calpe. Madrid, 1988. Según cita de Gisbert Calabuig Juan Antonio. Medicina Legal y Toxicología. 5ª Ed. Messon, S. A. Barcelona España. 1999. Pág. 911.

4.- La Sociología, que estudia los fenómenos sociales, sus orígenes y manifestaciones globalmente considerados, es decir, con independencia de lo que acontece a nivel individual.

Por consiguiente, aceptando la anterior definición[325], la Criminología debe intervenir como auxiliar en el análisis de:

1.- El crimen o delito que, en su aspecto objetivo, es materia de estudio del Derecho.

2.- El criminal o delincuente, cuya responsabilidad debe quedar establecida por la judicatura, pero cuya imputabilidad es informada por la medicina, particularmente, la psiquiatría forense, disciplina ésta que, además, se encarga de investigar la dinámica personal que se resuelve en la motivación del acto delictivo.

3.- La víctima del delito, por cuanto desde una perspectiva psico-social ha establecido una peculiar forma de relación con el delincuente, sufriendo las consecuencias del acto antijurídico.

4.- El control social de la delincuencia que vuelve a ser competencia del Derecho, del Poder Ejecutivo y de los sistemas de punición y de reinserción social propuestos por éstas instancias, sistemas en los que, de nuevo, habrán de desempeñar un importante papel la psicología y la psiquiatría.

Así mismo López Rey define a la Criminología como "la ciencia que se ocupa de determinar las causas o factores del delito a fines de la prevención y tratamiento del delincuente". [326]

---

[325] Idem. Pág. 911

[326] López Rey. M. Introducción a la Criminología. Universidad Complutense. Madrid. 1981. Según cita de Gisbert Calabuig Juan Antonio. Medicina Legal y Toxicología. Pág. 911.

b) El Objeto de la Criminología

El objeto de la criminología tiene una amplitud mayor de la que le asigna el derecho penal, pues el "estudio de las conductas humanas peligrosas" es más extenso que el de los hechos que la ley califica como delito, aunque debe aclararse que el objeto "delito" si bien es precisado por derecho penal, no constituye un elemento exclusivo de éste.[327]

El objeto de la investigación criminológica- lo constituye la acción humana injusta o peligrosa, aunque no llegue a configurar delito, mediante la aplicación de procedimientos científicos tendientes a explicar fenómenos biológicos, sociales o mesológicos que la generan.

José Ingenieros, nos india que la criminología, como disciplina científica puede dividirse en diferentes capítulos según la concepción.[328]

a) Antropología criminal. Estudia los factores endógenos, biológicos, propios del delincuente. Sus ramas son la psicología criminal, la psicopatología criminal, la morfología criminal, la biotipología criminal y la endocrinología criminal.

b) Mesología criminal (del griego mésos, medio). Considera los factores exógenos propios del ambiente. Sus subcapitulos son: la sociología criminal, la geografía criminal y la meteorología criminal.

De igual forma en su plan original estableció.

1) La etiología criminal, que estudia las causas determinantes del delito.
2) La clínica criminológica, que estudia las múltiples formas en que se manifiestan los actos delictivos y los caracteres fisiopsíquicos de los delincuentes para formar la clasificación de delincuentes, y

[327] Ob. Cit. Basile Alejandro, A. Fundamentos de Medicina Legal. Pág. 164
[328] Idem. Pág. 167.

3) La terapéutica criminal, que considera las medidas, sociales o individuales, de profilaxis o de represión del delito.

De otra forma también encontramos que:

La etiología criminal, en la concepción criminológica, se reconocen como causales del delito no solamente la personalidad del delincuente observada como totalidad por la psicología criminal, sino también los contextos sociales y ambientales que participan en la génesis de la conducta criminal.[329]

La sociología criminal es para Emst Seelig el clima –como condicionante de todo lo ambiental-, las condiciones económicas (individuales y colectivas), la estructura y el movimiento de toda la población (vernácula y migratoria), la marcha de la administración de justicia, el grado de afincamiento del individuo, vinculado todo en interrelación en el lugar del hecho delictivo.[330]

De igual forma señalan López Gómez y G. Calabuig:[331] El delito, independientemente de su calificación moral, es un hecho humano y, como tal, viene determinado por un juego de fuerzas y factores, unos internos, endógenos, y otros externos, ambientales.

Comprender un delito equivale, pues, a hallar el valor de las incógnitas en la actuación responsable de la conducta personal frente a la situación delictiva. La acción antijurídica es la culminación y descarga de un proceso psíquico cuyos momentos iniciales se remontan mucho, a veces, en el pasado individual. Los diversos estadios psíquicos por los que pasa todo delito pueden ser, o no, conscientes. El tipo corriente de trasgresión legal puede decirse que nunca es totalmente impulsivo ni totalmente premeditado, sino que se gesta en un proceso psíquico físico, que va desde la simple sugerencia o intuición del fin posible hasta la realización activa del mismo. La distinta rapidez del proceso y la acentuación de alguna de las fases son el origen de los distintos tipos de delitos. Y,

[329] Idem. Pág-172.
[330] Idem. Pág.173.
[331] Ob. Cit. Gisbert Calabuig Juan Antonio. Medicina Legal y Toxicología. Pág. 912.

siguiendo a Pérez Vitoria, concluye: "El delincuente puede ser, y lo es en la mayoría de las ocasiones un hombre aparentemente normal y su acción delictiva no es sino una resultante de su personalidad completa, en la que es preciso ahondar para poner en evidencia la raíz de su conducta criminal." [332]

La comprensión de la conducta criminal en relación con la personalidad del delincuente y de la situación en la que se encuentra nos remite, invariablemente, al estudio de los factores bio-psico-sociales que configuran dicha personalidad, estudio que debe abordarse mediante la utilización de modelos, que vienen a ser como perspectivas parciales, exigidas por la metodología, pero cuya intervención nos facilita la comprensión de éste " todo" constituido por la conducta humana.[333]

También podemos ver que Hans H. Jascheck. Nos señala que la criminología es una ciencia fáctica que se sirve de los métodos de distintas ciencias de la naturaleza y sociales y pueden, por ello, caracterizarse como un "sector científico interdisciplinario". La criminología se ocupa de la personalidad del delincuente, de su desarrollo, de sus características físicas y psíquicas y de sus posibilidades de educación, así como de las formas de aparición del delito de sus causas, de su significación tanto para la sociedad como para la vida del individuo y, finalmente, de la forma de incidencia de los medios de reacción juridicopenales, sin que, sin embargo, quede vinculada al concepto de hecho punible en sentido jurídico.[334]

La Criminología tiene ante sí la tarea del estudio del delincuente, de quien ha violado la norma jurídico penal, pero su fin va más allá y sin perder de vista el concepto normativo del delito debe también aportar al Estado los estudios que permitan al legislador dictar leyes preventivas o represivo-preventivas, basadas en el conocimiento de las causas o factores de la delincuencia; así como también auxiliar al Agente del Ministerio Público y al Juzgador, permitiéndoles penetrar en el mundo del delincuente para conocer su personalidad.

---

[332] Idem. Pág.912.
[333] Idem. Pág. 912.
[334] Ob. Cit. Jascheck Hans Heinrich. Tratado de Derecho Penal. Pág. 62

c) Conducta antisocial.

Es aquella que rompe con las reglas, normas y valores generales establecidos para el bien común, la convivencia y el bienestar social causando daño al individuo, familia y sociedad.

Conducta Antisocial es todo aquel comportamiento humano que va contra el bien común, siendo aquel que es apto para servir o perfeccionar la naturaleza humana en cuanto tal, independientemente de las condiciones individuales, que provienen en cada ser humano de su raza, nacionalidad, edad, profesión, condiciones sociales o religiosas o económicas.[335]

El orden social es una necesidad para lograr el bien común, pero sólo tiene razón de ser en cuanto logra la realización de éste; no puede entenderse un orden social, jurídico o político sino en función del bien de la totalidad de la colectividad.[336]

Deduciendo con claridad que ni todo delito es una conducta antisocial no toda conducta antisocial es delito. Ya que el objeto del Derecho Penal son las normas que rigen al delito, que es ente y figura jurídica; y por lo tanto el objeto de la criminología es el hecho antisocial, fenómeno y producto de la naturaleza.

Para la criminología es importante distinguir cuatro tipos de conductas[337]:

1) Conducta social. Es la que cumple con las adecuadas normas de convivencia, la que no agrede en forma alguna a la colectividad es que cumple con el bien común.

2) Conducta asocial. La conducta asocial es aquella que carece de contenido social, no tiene relación con las normas de convivencia no con el bien común.

---

[335] Cfr. Códigos de Molinas. Edit. Sal Terrae. Santander, España, 1959. pág. 524 yss. Según cita de Rodríguez Manzanera Luis. Criminología. Edit. Porrúa. México, 1998. Pág. 21.
[336] Ob. Cit. Rodríguez Manzanera Luis. Pág. 21.
[337] Idem. Pág. 22.

3) Conducta parasocial. Se da con el contexto social, pero es diferente a las conductas seguidas por la mayoría del conglomerado social. Es la no aceptación de los valores adoptados por la colectividad, pero son destruirlos; no realiza el bien común, pero no agrede.

4) Conducta Antisocial. Va contra el bien común, atenta contra la estructura básica de la sociedad, destruye su valores fundamentales, lesiona las normas elementales de la convivencia.

También se conoce otro término como el de conducta desviada, tan utilizado actualmente, es de gran utilidad, principalmente por ser descriptivo y no valorativo,[338] y nosotros lo usaremos en forma general, pues una conducta desviada es una conducta diferente de la generalidad, y puede ser parasocial o antisocial o, en algunos casos simplemente asocial.

Cualquier persona puede cometer actos sociales, asociales, parasociales o antisociales, pero cuando prevalece determinado tipo de conducta, podemos utilizar otro nivel de interpretación, y así distinguir sujetos:[339]

1) Sujeto social. Por lo común el concepto de sociabilidad se interpreta como facilidad de interrelación, de comunicación humana; se debe considerar como cumplimiento de las normas de convivencia y realización del bien común.

2) Sujeto parasocial. Se da paralelamente, al lado de la sociedad; no cree en sus valores, pero no se aparta de ella, sino que comparte sus beneficios, en mucho depende de ella para sobrevivir.

3) Sujeto Antisocial. Agrede el bien común, destruye los valores básicos de la sociedad, no respeta las leyes elementales de convivencia, no vive en sociedad sino contra ella.

[338] Cfr. Rock, Paul., Deviant Behaviour. Hutchinson University Library. Londres. G. B., 1973. Pág. 19 y ss. Según cita de Rodríguez Manzanera Luis. Pág. 23.
[339] Idem. Pág. 25.

También hay que saber distinguir que:[340]

a) Crimen. Conducta antisocial propiamente dicha, es un episodio que tiene un principio, un desarrollo y un fin.

En este nivel se analizan todos los factores y causas que concurrieron para la producción del evento. Los aspectos biológicos, psicológicos, antropológicos, que llevaron al "paso al acto"

b) Criminal. Es el autor del crimen, es el sujeto individual, actor principal del drama social.

En el momento actual, el concepto de "criminal" o sujeto antisocial es muy amplio y no se limita al infractor de la ley penal. Pensando que los términos "criminal" y "antisocial" pueden ser estigmatizantes y valorativos.

c) Criminalidad. Es el conjunto de las conductas antisociales que se producen en un tiempo y lugar determinados.

La Criminalidad es el "fenómeno de masas constituido por el conjunto de infracciones que se comenten en un tiempo y lugar dados". Representan "la manifestación total de los fenómenos psicosociales que, en un momento dado de la historia de un país, son considerados como crímenes.[341]

Siendo admisible una clasificación de la criminalidad de acuerdo con la amplitud o restricción con que se tome o según la fuente que lo produce.

---

[340] Idem. Pág. 26.

[341] Reyes Ruiz, Sandoval. La violencia en Colombia. Trabajo presentado al Primer Seminario de investigación comparada del proyecto de violencia en América Latina, agosto 15 al 17 Quito, Ecuador. 1976. Págs. 34 y 105. Según Cita de Reyes Calderón José Alfredo, Criminología, 2ª Ed. Cardenas Editor Distribuidor. México 1998. Pág. 107.

Tomando en cuenta al Criminólogo Alfonso Reyes Echandía[342] quien clasifica a la criminalidad en varias modalidades que son:

a) Criminalidad real.

Es la totalidad de delitos y faltas que efectivamente se realizan en un tiempo y espacio determinados, independientemente de que hayan sido o no investigados o siquiera conocidos por la autoridad o los particulares.

b) Criminalidad aparente.

Está constituida por el conjunto de delitos y faltas fiscales que llegan a conocimiento de la autoridad competente (policías, fiscales y jueces fundamentalmente) en virtud de denuncias formuladas, por conocimiento directo de tales funcionarios, por informaciones confidenciales o mediante cualquier otro medio de comunicación o percepción.

c) Criminalidad oculta.

Resulta de la diferencia que media entre la criminalidad real y la aparente, vale decir entre el número de hechos punibles realmente cometidos y la cantidad de ellos que ha llegado a conocimiento de la autoridad.

Tal fenómeno se presenta por una de los causas: porque el hecho no se denuncia o porque la policía o Ministerio Público no investiga.

Las razones por las que un hecho delictivo no es denunciado a las autoridades suelen ser las siguientes: no llega a descubrirse; no a sido percibido por la víctima o testigo como delictuoso; hay desconfianza o animadversión hacia la autoridad policial o judicial; por simpatía al delincuente; porque la comunidad misma se muestra contraria a denunciar; por temor a represalias; porque se considera la condena imposible como más

[342] Idem. Págs. 108 a la 113.

grave que el daño ocasionado por el delito; para evitar ser implicado en la investigación como testigo o eventual copartícipe; porque se considera una pérdida de tiempo; cuando existe la posibilidad de obtener reparación por otra vía.

Las razones que explican la ausencia de investigación policial podrían sintetizarse en éstas: no aparece víctima alguna o ésta carece de importancia socio-económica; no hay personal disponible para actuar; no existen elementos técnicos adecuados; hay presiones económicas o políticas para que no se adelante la investigación, existe interés de cuerpo para "desinflar" las estadísticas, es decir, se conoce el hecho pero no se investiga no se incluye en las estadísticas policiales para dar la sensación de que la criminalidad ha disminuido.

d) Criminalidad legal.

Es aquella que ha sido realmente investigada por la autoridad competente y en relación con la cual se ha producido una decisión judicial más o menos provisional, tal como el auto prisión provisional.

e) Criminalidad judicial.

Con este nombre denominamos aquellas partes de la criminalidad legal que culmina en sentencias condenatorias. Desde el punto de vista estrictamente jurídico es la única delincuencia reconocida en un estado de derecho que parte del supuesto de que una persona es inocente mientras se haya proferido en su contra sentencia condenatoria irrevocable.

f) Criminalidad impune.

Llámese de esta manera aquella parte de la criminalidad que media entre la aparente y la judicial, o en otras palabras, el número de infracciones penales que habiendo sido conocidas no culminaron en sentencias condenatorias.

g) Criminalidad tratada.

Es aquella parte de la criminalidad judicial que señala las infracciones penales en las que se ha producido sentencia de condena y cuyos responsables efectivamente han cumplido la sanción impuesta.

h) Criminalidad global.

También denominada "inespecífica", es aquella que comprende todo el conjunto de delitos y contravenciones sin discriminación alguna; es pues, la suma de infracciones penales cometidas en un determinado tiempo y espacio.

i) Criminalidad específica.

Con tal nombre se conoce aquella parte de la criminalidad global que se refiere a una determinada categoría o especie de infracciones penales: de esta naturaleza es la criminalidad contra la propiedad o contra la vida o contra la libertad sexual. También lo es, en sentido estricto, la que cuantifica una determinada clase de hechos punibles; así, delitos de robo, de secuestro o peculado. O de acuerdo a la clasificación que en la parte especial " de los delitos" contemplan los códigos penales.

j) Criminalidad anteograda.

Formas delictivas que se generalizarán en el futuro.[343]

[343] Parmelee, Maurice. Criminología. Madrid, Reus 1925. Trad. Julio C. Cerdeiras. Pág. 446. Según cita de Reyes Calderón José Alfredo, Criminología, Pág. 114.

k) Criminalidad convencional.

La cometida por el público en general, sin mayores subterfugios: homicidios, lesiones, robos, pequeñas estafas y defraudaciones, etc.[344]

l) Criminalidad de blusa azul.

La predicable a los obreros en desarrollo de su trabajo.

m) Criminalidad de color caqui.

Denominación que recibe el delito cometido en tiempo de guerra por los militares.[345] Y aquella que cae dentro de lo que se conoce como "fuero militar"

n) Criminalidad evolutiva.

Desarrollo de la delincuencia acorde con el avance cultural, técnico, científico, etc., de una sociedad dada.[346]

ñ) Criminalidad retrógrada.

Nombre con el cual se determina la delincuencia común en un momento dado y que se encuentra superado por la evolución.[347]

---

[344] Aniyar, Lola. Criminología de la Reacción Social. Maracaibo. Universidad de Zulia. 1976. Pág. 82 Según cita de Reyes Calderon José Alfredo. Criminología. Pag 114

[345] Ob. Cit. Aniyar, Lola. Pág. 83. Idem Pág. 114.

[346] Pérez Pinzón, Alvaro Orlando. Diccionario de Criminología. Departamento de Publicaciones. Universidad Externado de Colombia. Bogotá. 1979. Pág. 48. Idem. 115.

[347] Ob. Cit. Parmelle, Maurice. Criminología pág. 466. Idem. Pág. 115.

o) Criminología revelada.

Nombre que recibe el acto delictivo que se exterioriza a raíz de la ingestión de sustancias que, como el alcohol, aflojan los frenos inhibitorios. Se predica de aquellos individuos en que existe una disposición primitiva que sólo aflora mediante el mecanismo referido.[348]

p) Criminalidad de cuello blanco.

Llamada también de Cuello Duro de Guante Blanco. Nivel macrodelictual que radica en la "imposibilidad de denunciar ciertos delitos o en el consenso aberrantemente absolutorio con que en un principio se califican ciertas conductas criminales por razón de la posición social, preeminencia económica o financiera, cultural, distinción o buenos apellidos de quienes incurren en ellas". MIDDEENDORFF ubica en ese rango "los delitos de las grandes sociedades anónimas y mercantiles, las prácticas deshonestas de los comerciantes, las infracciones cometidas por los artesanos, deportistas y aquellos que tienen un titulo académico, así como la corrupción de los funcionarios".[349] SUTHERLAND define el delito de cuello blanco como "el cometido por una persona de respetabilidad y status social alto en el curso de su ocupación". [350]

Podemos ver también que Marcó del Pont, Luis y Nadelsticher Mitrani, Abraham nos definen y dan algunas de las características de la Criminalidad de Cuello Blanco.[351]

Ya que el crimen de cuello blanco ha sido denominado de diferentes formas: criminalidad de los negocios, criminalidad económica, etc.,[352] pero ha prevalecido el término de "white collar crime", que fue acuñado en 1943, por el criminólogo norteamericano Edwin Sutherland en su discurso pronunciado ante la Sociedad Americana de Criminología, y

[348] Ob. Cit. Pérez pinzón, Diccionario de Criminología Pág. 49. Idem Pág. 115.
[349] Gutiérrez Tovar, Gabriel. Estadística y criminalidad, en capítulo criminológico. Maracaibo. Universidad del Zulia. Facultad de Derecho. 1973. Pág. 108. Según cita de Reyes Calderón José Alfredo. Pág. 115.
[350] Pérez Pinzón, Alvaro Orlando. Diccionario de Criminología. Pág. 46. Idem. Pág. 115.
[351] Marcó del Pont, Luis. Nadelsticher Mitrani, Abraham. Delitos de Cuello Blanco y Reacción Social, Instituto Nacional de Ciencias Penales, México 1981. Cuaderno no.8 o págs. 17/23.
[352] Giuseppe Di Genaro y –Eduardo Vetere. La Criminalidad Económica. Problemas de dedinición y pautas de investigación. Pág. 2. Según cita de Reyes Calderón José Alfredo. Pág. 287.

luego recogido en un libro que tituló así y en el que hace un informe sobre setenta de las más grandes empresas mineras y comerciales sobre las que hubo decisiones de tribunales y comisiones administrativas de los Estados Unidos y quince corporaciones de servicio público de ese país.[353]

Este tipo de delincuencia es definido, no de acuerdo al interés protegido, como sucede en los delitos convencionales, sino conforme al *sujeto activo* que lo comete, señalándose que es realizado por una persona de respetabilidad y alto status social en el ejercicio de su profesión.[354] Algunas de las características de esta delincuencia son las siguientes:

1) El sujeto activo del delito es una persona de alto "status socioeconómico" a diferencia de la delincuencia convencional, en donde la víctima es quien posee el mayor status socioeconómico, o tanto ésta como el autor de la conducta pertenecen a sectores bajos.

2) Este delito debe ser cometido en el ejercicio de la actividad económica empresarial de la persona, es decir, que no todo el delito cometido por personas de alto "status" es delito de cuello blanco. Pero no basta su condición socioeconómica, es necesario que su actividad delictuosa haya sido realizada en razón de la profesión y ocupación que se ejerce.

3) En tercer lugar el delito de que tratamos (cuello blanco) no puede explicarse por pobreza, ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional que son los elementos clásicos utilizados para explicar le delito convencional.

4) En cuarto lugar, hay dificultades para elaborar estadísticas. La cifra negra es muy alta en materia de evasiones de impuestos, por ejemplo.

---

[353] Ob. Cit. Aniyar de Castro, Lola. Criminología de la Reacción Social. Págs.80/81. Según cita de Reyes Calderón José Alfredo.Pág. 287.

[354] Edwin Sutherland. El delito de Cuello Blanco. Caracas,1969. Universidad Central de Venezuela. Imprenta Universitaria, pág. 13. Idem. Reyes Calderón. Pág. 290.

5) hay dificultad para descubrirlo y sancionarlo en razón del poder económico de quienes lo cometen, sin embargo, los daños ocasionados son altísimos, y así ejemplifica que en los Estados Unidos sólo por evasión de impuestos hay una pérdida de 25 a 40 billones de dólares anuales.

6) En sexo lugar, hay una gran indiferencia de la opinión pública sobre estos daños ocasionados en sociedad.

7) Otra diferencia apuntada, es que mientras la llamada delincuencia "convencional" es perseguida por medio de la privación de la libertad, en la delincuencia de "cuello blanco" son simplemente multas y otro tipo de medidas administrativas. Además están previstas en "leyes especiales" que en caso de multas afectan muy "levemente" al delincuente.

8) Por último indica que la impunidad se puede explicar en razón de:

a) La tecnificación y complejidad de las leyes especiales que rigen ciertas actividades, tales como la Ley de Impuestos sobre la Renta, leyes aduaneras, de sucesiones, etc., en las que el consejero astuto y hábil puede jugar fácilmente.
b) Influyen igualmente la complicidad de las autoridades, que es muy frecuente, por soborno por estar implicadas en las actividades.
c) Por ausencia de control estatal.
d) Por el hecho de que algunos de estos delitos son cometidos amparándose en la inmunidad diplomática (tráfico de drogas, armas, reclutamiento de mercenarios, espionaje industrial y de los parlamentarios).

Por lo que cualesquiera que sean las razones o justificaciones de los métodos empleados para controlar los delitos de cuello blanco, la ambivalencia de la respuesta social a este tipo de conducta se relaciona también con factores sociales más generales, los cuales presentan dimensiones tanto objetivas como subjetivas. La ambigüedad de los delitos de cuello blanco refleja el hecho objetivo de que éstos representan un índice de

importantes transiciones en la estructura social. Un buen ejemplo de este fenómeno es la práctica del tráfico de información en la bolsa de valores y en otras instituciones financieras, el cual se penalizó recientemente en Inglaterra, aunque no se considera como conducta criminal en el resto de los países europeos.[355] Como señala Clarke:

Hasta los años cincuenta, hubiera desconcertado a los miembros más importantes de estas instituciones el enterarse de que actuaban de manera censurable al manipular así dicha información. Debióse precisamente al acceso a esta información que se formaba parte de la comunidad financiera, y que uno formaba parte de la comunidad financiera con la clara expectativa de amasar una cantidad de dinero considerable.[356]

3.3. CIENCIAS O DISCIPLINAS EN QUE SE AUXILIA LA CRIMINOLOGÍA.

La Criminología es una ciencia abierta a toda nueva conquista del saber, por esto es una ciencia joven que no puede envejecer, ya que se ve continuamente renovada por los descubrimientos científicos.

Por lo que podemos decir que se auxilia de otras ciencias o disciplinas como:[357]

a) Antropología Criminal.

La criminología nace como "Antropología Criminal" (Lombroso, 1876), pretendiendo dar una explicación integral del hombre delincuente.

La Antropología Criminal ha siso definida como "El estudio de las características físicas y mentales particulares a los autores de crimenes y delitos", y como la "ciencia que estudia

[355] Maguire Mike, Morgan Rod y Reiner Robert. Manual de Criminología Volumen 4. Oxford University Press. 1999. Pág. 181.
[356] Clarke, M. "The Control of Insurance Fraud: A Comparative View", British Journal of Criminology, núm 30, 1990". Pág. 162. Según cita de Maguire Mike. Morgan Rod y Reiner Robert ág. 181.
[357] Ob. Cit. Rodríguez Manzanera Luis. Págs.60-69.

precisamente los caracteres específicos y distintivos del hombre en tanto que ser vivo", y en este caso el hombre criminal, considerado este término en su sentido más amplio.[358]

La Antropología Criminal en sí estudia la personalidad del delincuente, mediante método científico que es conllevado dentro de la ciencia biológica y psicológica en general, y la ciencia de la constitución y la biotipología humana en particular; método que considera a la personalidad humana como una unidad imprescindible, dentro de la forma y función, carácter somático y carácter psíquico, fuerza material y fuerza espiritual; estando unidos estrecha y coordinadamente, de manera tal que dentro de esa misma personalidad individual debe corresponder a su propia morfología, su funcionamiento, su psicología.[359]

La costumbre, los tatuajes, las supersticiones, la "moral", el lenguaje, las expresiones artísticas del criminal, las diferencias entre diversos grupos criminales (según edad, religión, hábitat, etc.), el modus operandi en ciertos crímenes, son aportaciones de gran valor de la Antropología Criminológica.

La Antropología Criminológica estudia también el efecto del medio físico y la adaptación del hombre al mismo (Ecología), así como el espacio en que mueve el ser humano, y que puede ser sociópeto, favoreciendo las relaciones sociales, o sociófugo, obstaculizándolas.

b) Biología Criminanológica.

La Biología Criminológica estudia al hombre de conducta antisocial como un ser vivo, desde sus antecedentes genéticos hasta sus procesos anatomo-fisiológicos; la influencia de los fenómenos biológicos en la criminalidad y la participación de los factores biológicos en el crimen.

---

[358] Cfr. Grapin, Pierre. L´Anthropologie Criminelle. Presses Universitaires de France. París, Francia, 1973, págs 5 y 6. Según cita de Rodríguez Manzanera Luis. Criminología. Pág. 60.
[359] Di Tullio, Benigno. Tratado de Antropología Criminal. Editrice "criminalia" Roma MCMXLV,pág. 25. Idem. Pág. 60.

El funcionamiento del organismo, la relación de éste con el medio físico, los efectos de la alimentación, la disfunción glandular, la herencia criminal y sus respectivas relaciones con la criminalidad, son problemas criminológicos que resuelve la Biología Criminológica.

La biología Criminológica extiende sus investigaciones a todos los aspectos anatómicos, fisiológicos, patológicos y bioquímicos de la personalidad criminal.

c) Sociología Criminológica.

Esta materia estudia el acontecer criminal como fenómeno que se da en la colectividad, tanto en sus causas y factores como en sus formas, desarrollo, efectos y relaciones con otros hechos y conductas que se dan en sociedad.

En su "Sociología del Delito", MIDDENDORFF dice que aparentemente hay una contradicción "pues mientras la Sociología investiga de modo rigurosamente objetivo y racional las condiciones y relaciones sociales generales desde una atalaya libre de valoraciones, la palabra delito, por el contrario, implica normalmente una valoración, un juicio de desvalor.[360]

HÉCTOR SOLÍS QUIROGA dice que " Se llama Sociología porque estudia los hechos sociales, las interacciones humanas, el real acontecer colectivo, y busca su comprensión y su entendimiento mediante el descubrimiento de su sentido y sus conexiones de sentido. Se califica de criminal, porque concreta su estudio a los hechos delictuosos, solo que considerados en su masa o totalidad.[361]

[360] Middendorf, Wolf, Sociología del Delito. Revista de Occidente. Madrid, España. 1961, pág. 7. Según cita de Rodríguez Manzanera Luis. Criminología. Pág. 68.
[361] Solís Quiroga, Héctor. Introducción a la Sociología Criminal, Universidad Nacional de México, México, 1962, pág. 28. Según cita de Rodríguez Manzanera Luis. Criminología. Pág. 68.

Actualmente, modernas corrientes criminológicas afirman que el modelo de investigación criminológico debe ser "completamente social", ya que, aunque se pudiera suponer a priori la intervención de factores extrasociales, como los biopsicológicos, estos estarían profundamente modificados por el contexto social particular en el que se manifiestan.[362]

Ahora, la Sociología Criminológica estudia los problemas criminales y trata de dar explicaciones más completas a la conducta antisocial, encontrándose temas que son verdaderos modelos o hipótesis de investigación, como las subculturas criminales, los conflictos culturales, la oportunidad de delinquir, el etiquetamiento, la marginación, etc.

d) Psicología Criminal.

A través de la historia del ser humano, se ha considerado que las conductas diferentes al común denominador son "anormales", es decir, salen de lo establecido por una sociedad dada, salen de la "norma" y en razón de que afectan los valores comunes, se han castigado de múltiples formas, tratando de erradicar el comportamiento dañino.

En nuestra sociedad, algunas de estas conductas anormales[363], son consideradas delitos (afectan los intereses de los particulares así como del Estado mismo en cuanto al patrimonio y la integridad física: bien jurídico tutelado del que se trate) por lo que ésta las castiga e intenta readaptar al delincuente para preservar los valores en que se fundamenta la convivencia; otras conductas, aunque antisociales no son consideradas para su punición. Sin embargo, para poder readaptar a un sujeto delictivo, así como para prevenir la aparición de conductas delincuenciales y predecir hasta cierto punto su actuar, se hace necesario descubrir las motivaciones sociales y de personalidad que llevan a un sujeto a cometer estos actos.

---

[362] Cfr. Taylor, Ian; Walton, Paul; Young, Jock. The New Criminology: For a Social Theory of Deviance. Routledge & Kagan paul, Londres, Inglaterra, 1975. Según cita de Rodríguez Manzanera Luis. Criminología. Pág. 68.

[363] Distinguiremos dos tipos de actos antisociales: el delito como un acto antisocial que castiga la ley a través de la tipificación de la conducta y otros actos antisociales que no son punibles por la ley.

El término de Psicología Criminal, se utiliza para definir a la rama de la psicología que estudia las conductas y los procesos mentales de los sujetos que cometen actos antisociales.

FERRI, reconocía cuatro ramas científicas para la observación psicológica de la personalidad, a saber: la Psicología Criminal, la Psicología Judicial, la Psicología Carcelaria y la Psicología Legal, diciendo que: "la primera estudia al delincuente en cuando es autor del delito; la segunda estudia su comportamiento en cuando es imputado de un delito; la tercera lo estudia mientras está condenado, expiando una pena carcelaria; y la cuarta, en fin, coordina las nociones psicológicas y psicopatológicas que ocurren por la aplicación de las normas penales vigentes sobre las condiciones del menor (discernimiento), del enfermo mental, del sordomudo, del alcohólico, así como de las circunstancias agravantes (premeditación, brutalidad, maldad, etc.) o atenuantes (impulso de ira o de intenso dolor, flagrancia en adulterio, etc)"[364].

Hilda Marchiori opina que " La Psicología trata de averiguar, de conocer qué es lo que induce a un sujeto a delinquir, qué significado tiene esa conducta para él, porqué la idea de castigo no lo atemoriza y le hace renunciar a sus conductas criminales. La tarea psicológica consiste en aclarar su significado en una perspectiva histórico-genética".[365]

Por lo que en definitiva podremos decir que la Criminología estudia todas las causas y formas reales de la comisión de un delito, adoptando una visión integradora de los aspectos causales de la delincuencia y que va más allá de su estricta concepción jurídica del delito.

[364] Ferri, Enrico. En la Prefazione (Prólogo) de la Psicologia Giudiziaria de Enrico Altavilla. Unione Tipográfico-Editrice Torinese. Trín, Italia, 1955. Tomo I, pág. IX. Según cita de Rodríguez Manzanera Luis. Pág. 65.
[365] Marchiori, Hilda. Psicología Criminal. Edit. Porrúa, México, 1975, pág. 1.

Por lo que al hablar del perfil criminológico de un delincuente informático apunta hacia el estudio de las causas, fenómenos y factores, así como las características que lo rigen en forma general o particular al cometer una conducta delictiva utilizando como medio u objeto una computadora con un fin determinado. Ya que el delincuente tecnológico asume una actitud de reto con los sistemas informáticos a que se enfrenta, y con esto se encuentra al margen de que su conducta traspase o no a una conducta delictiva o criminal.

3.4. DESCRIPCIÓN DE RASGOS PSICOLÓGICOS NOTORIOS EN HACKERS.[366]

a) Metodología.

Según Eric Raymond "Los hackers son inteligentes, intensos, abstraídos e intelectualmente abiertos. Se interesan por cualquier sujeto que les pueda proporcionar estimulación mental y es común que tengan una afición extrema al hacking, en el que se desenvuelven competentemente. Les encanta el control, pero no en forma autoritaria sino sobre cosas complicadas, como las computadoras. Se apasionan por lograr que esas máquinas sean instrumentos de lo interesante, siempre y cuando se trate de sus propias ideas y no de una orden de alguien. No les gustan las rutinarias tareas cotidianas que llevan a mantener una existencia normal; por ello, si bien son ordenados en sus vidas intelectuales, son caóticos en el resto. Prefieren el desafío del conocimiento a una recompensa monetaria por un trabajo".[367]

---

[366] Estudio realizado por el Licenciado en Psicología Abizaid Peréz Mauricio Rafael. Encargado del Programa de Psicología Forense en el Instituto de Formación Profesional de la Procuraduría General de Justicia del Distrito Federal. Septiembre del 2000.

[367] Raymond, Eric. The New Hackers Dictionary. The MIT Press, 1991. (La versión electrónica "Jargon File Resources" está disponible en : http:// www.ccil.orgliargonl). recopilación de información hecha por http://renc1. Cjb. Net. " Crimen y Castigo en el Ciberespacio. Hermosillo Sonora, México. Diciembre de 1999. Pág.10.

Invariablemente, para obtener un perfil individual de comportamiento, es necesario entablar una relación terapéutica con el sujeto a evaluar, sin embargo, también es indiscutible que deben existir patrones más o menos generalizados de comportamiento para las personas que se dedican a una actividad en particular. Así por ejemplo, encontraremos dentro de un grupo de abogados, características de personalidad que son al menos similares en determinados aspectos de la vida que los han llevado a elegir dicha profesión.

El presente análisis de personalidad será: basándonos en la definición que de los hackers hace Eric Raymond y en el principio psicodinámico de que toda persona actúa como piensa y en ese sentido, todo acto es simbólico y representativo del pensamiento, por lo tanto analizable. Para elaborar este último punto se tomarán en cuenta algunos casos de personas conocidas como piratas cibernéticos.

b) Estructura de Personalidad.

Desde un punto de vista práctico, podemos decir que la inteligencia de un organismo es fundamentalmente su capacidad psicológica para adaptarse improvisando una reacción ante situaciones nuevas y para utilizar el ambiente. Las especies o individuos que poseen mayor capacidad a este respecto, son los más inteligentes.

Basados en esta definición de inteligencia, la capacidad de adaptación incluye todos los medios en los que el sujeto se desenvuelve, por lo tanto el conocimiento del manejo de un ordenador en combinación con la creatividad del sujeto para utilizarla y la continuidad con que lo hacen, ocasiona que los no expertos o poco dedicados vean a los "hackers" como superdotados en éste ámbito.

Siguiendo con la definición de Raymond, interpretemos "intensos" como dedicados en tiempo y alma a su actividad. En este sentido, debemos inferir la razón por la que una persona omite toda o casi toda actividad para dedicarse a una sola.

Relacionando el siguiente aspecto mencionado por Raymond (abstraído), podemos damos cuenta que cualquier persona que por alguna razón es marginada de su grupo de relación, tenderá a alejarse de este por considerarse a sí mismo inadecuado o mejor dicho inadaptado (caótico) a los valores que en ese medio se manejan. Por ello buscará una actividad que al tiempo que le satisfaga su necesidad de relación (en este caso otros Hackers), disminuya la carga afectiva de sentirse marginado.

Cuando la marginación es muy significativa para el sujeto, le será necesario compararse ahora en su nuevo grupo de relación con el anterior, buscando, mediante mecanismos de defensa, revalorarse. Si el resentimiento resultante de esta dinámica provoca sobre valoración de sí mismo, alimentará el narcisismo característico del que se sabe inteligente o se cree considerado así por otros y en este sentido el control de "algo" será en extremo valioso para el sujeto. Esto último explica claramente la razón por la que Raymond cataloga a los hackers como intelectualmente abiertos e intolerantes a la monotonía; es decir, si de momento se estancaran en el conocimiento tecnológico o dejaran la actividad que les ha hecho "sobresalir", sobrevendría un estado de depresión[368] y se sentirían "vencidos" por quienes los han marginado.

Existe dentro del lenguaje característico de la informática, varias acepciones o calificativos para quienes accesan ordenadores ajenos dependiendo de su actividad específica una vez dentro del universo virtual al que ingresen. Los no letrados en el ámbito informático, podemos pensar que el "hacker" (que significa tajador, cortador, el que divide, o mella) engloba a todas las categorías, incluso en ocasiones utilizamos como sinónimo el de "pirata cibernético". Sin embargo, los expertos en estos ámbitos hacen una división básica entre hacker, cracker, phreacker.

Cabe hacer esta distinción con la finalidad de analizar la motivación que caracteriza a cada actividad específicamente. Esto es, dependiendo de la legislación que al respecto se tenga en cada país en el momento del acto, debemos considerar si el sujeto tiene

[368] Específicamente vacíos, como si nada tuviera sentido. Por el contrario, la acción de "hackear", es vivida por quienes la hacen como una aventura que en otros tiempos podría compararse con buscar oro o viajar al fondo del mar.

conocimiento de que su actividad es ilícita o no. Si en efecto, el sujeto sabe que su acto transgrede la ley y a pesar de ello la lleva a cabo, entonces se trata de un "cracker" (o phreacker en su caso), por lo tanto su conducta tiene rasgos (al menos) de antisocialidad, es decir, agrede deliberadamente lo establecido a pesar del conocimiento de las consecuencias que esto puede traer.

Cuando una persona se expone a hacer esto, no basta que se encuentre molesto por algo que real o imaginariamente haya sentido como agresión. Depende también de su baja tolerancia a la frustración, de los valores que tenga como base ética y de la cantidad de resentimiento que guarde contra su víctima.

En este sentido y con relación al tema tratado, podemos inferir que el daño a larga distancia, es una manifestación de agresividad pasiva, no de encarar la situación específica que causa el problema, sino de hacerlo en forma subrepticia y por lo tanto en el anonimato.

Por supuesto la razón específica por la que alguien guarde resentimiento contra una persona, asociación o compañía no es detectable de manera general, es definitivamente una cuestión muy personal.

La importancia de establecer hipótesis adecuadas durante la investigación de un delito informático, respecto al porqué alguien ha dañado información sustancial de un ordenador. Para esto, es recomendable investigar de primera instancia a las personas internas a la compañía afectada, su grado de limitación de acceso a dicha información y qué posibles razones (reales o imaginarias) pudieran tener para esta manifestación de resentimiento. Una vez descartada la posibilidad de alguien interno, entonces se podrá pensar en alguien externo[369].

[369] Según estadísticas, el 75% de los delitos informáticos cometidos en empresas son realizados desde dentro de la misma y/o por personas que han estado en ella.

La lógica psicodinámica para explicar esto se resume en un sencillo principio: lo que uno no conoce simplemente no le puede afectar. En este sentido, caben dos posibilidades:

1. Que la víctima haya afectado directa o indirectamente al agresor (de manera real o imaginaria); y

2. Que el agresor, mediante algún mecanismo de desplazamiento, dañe algo que le signifique alivio a su frustración[370].

c) Manifiesto Hacker.

> Uno más ha sido capturado hoy, está en todos los periódicos.
> "Joven arrestado en Escándalo de Crimen por Computadora",
> "Hacker arrestado luego de traspasar las barreras de seguridad
> de un banco..."
> Malditos muchachos. Todos son iguales. Pero tú, en tu sicología de tres partes y tu tecnocerebro de 1959, ¿has alguna vez observado detrás de los ojos de un Hacker?
> ¿ Alguna vez te has preguntado qué lo mueve, qué fuerzas lo han formado, cuáles lo pudieron haber moldeado?.
> Soy un Hacker, entra a mi mundo...
> El mío es un mundo que comienza en la escuela...
> Soy más inteligente que la mayoría de los otros muchachos, esa basura que ellos nos enseñan me aburre...
> Malditos subrealizados. Son todos iguales.
> Estoy en la preparatoria.
> He escuchado a los profesores explicar por decimoquinta vez como reducir una fracción.

[370] Como por ejemplo el obrero que es reprendido por su patrón: no enfrentará al patrón por saber que eso redundaría en su empleo, sin embargo, raya la pintura de un vehículo que aunque no sea el de su patrón le significa superioridad. El sentido simbólico sería: "obtengo venganza dañando algo que me significa superioridad"

Yo lo entiendo.

"No, Srta. Smith, no le voy a mostrar mi trabajo, lo hice en mi mente..."

Maldito muchacho. Probablemente se lo copió. Todos son iguales.

Hoy hice un descubrimiento.

Encontré una computadora.

Espera un momento, esto es lo máximo.

Esto hace lo que yo le pida. Si comete un error es porque yo me equivoqué.

No porque no le gusto...

O se sienta amenazada por mí...

O piensa que soy un engreído...

O no le gusta enseñar y no debería estar aquí...

Maldito muchacho. Todo lo que hace es jugar. Todos son iguales.

Y entonces ocurrió...

Una puerta abierta al mundo...

Corriendo a través de las líneas telefónicas

Como la heroína a través de las venas de un adicto, se envía un pulso electrónico, un refugio para las incompetencias del día a día es buscado...

Una tabla de salvación es encontrada.

"Este es... este es el lugar a donde pertenezco....."

Los conozco a todos aquí...

Aunque nunca los hubiera conocido, o hablado con ellos, o nunca vuelva a escuchar de ellos otra vez...

Los conozco a todos...

Malditos muchachos. Enlazando las líneas telefónicas otra vez.

Todos son iguales...

Apuesta lo que sea a que todos somos iguales...

A nosotros nos han estado dado comida para bebés con cuchara en la escuela, cuando estábamos hambrientos de carne...

Las migajas de carne que ustedes dejaron escapar estaban masticadas sin sabor.

Nosotros hemos sido dominados por sádicos, o ignorados por los apáticos.

Los pocos que tienen algo que enseñarnos encontraron alumnos complacientes, pero esos pocos son como gotas de agua en el desierto.

Ahora este es nuestro mundo...

El mundo del electrón y el conmutador, la belleza del baudio.

Nosotros hacemos uso de un servicio que ya existe sin pagar por lo que podría ser barato como el polvo, si no estuviera en manos de glotones hambrientos de ganancias, y ustedes nos llaman criminales.

Nosotros exploramos...

Y ustedes nos llaman criminales.

Nosotros buscamos detrás del conocimiento...

Y ustedes nos llaman criminales.

Nosotros existimos sin color, sin nacionalidad, sin perjuicios religiosos...

Y ustedes nos llaman criminales.

Ustedes construyeron bombas atómicas,

Ustedes hicieron la guerra,

Ustedes asesinaron, engañaron y nos mintieron

Y trataron de hacernos creer que era por nuestro bien,

Ahora nosotros somos lo criminales.

Si, soy un criminal.

Mi crimen es la curiosidad.

Mi crimen es el juzgar a personas por lo que dicen y piensan, no por lo que aparentan.

Mi crimen es ser más inteligente, algo por lo cual nunca me olvidarás.

Soy un Hacker, este es mi manifiesto.

Tu podrás detener este esfuerzo individual, pero nunca podrás detenernos a todos..... después de todo, todos somos iguales.
------The Mentor[371]------

El manifiesto mostrado arriba, no sólo habla de la conducta de un grupo social determinado, sino del sentir de los individuos que por algún motivo se consideran marginados de los valores comúnmente aceptados. Se manifiesta también el intento por mostrarse, sobresalir, a través de sus propias convicciones ante un mundo que le cuesta trabajo entender y que está decidido a no entender, por el contrario, dentro de su actitud narcisista y egocéntrica, se muestra convencido que sus valores son los únicos o más importantes.

En el caso específico del manifiesto hacker, el sujeto describe un descubrimiento que lo justifica en su actuar, donde mantiene todo el control y donde no es juzgado por lo que él mismo percibe como amenazante; lugar en el que puede manifestar toda su ambición, misma que se torna virtual en el momento en que no puede de manera tangible hacerse de bienes en su medio real. Incluso en la parte donde dice "... existimos sin color, sin nacionalidad, sin prejuicios religiosos..." el simbolismo está claramente dirigido a la pérdida de la identidad, el anonimato, necesario en quienes temen ser atacados o juzgados.

Uno de los rasgos principalmente manifiestos a lo largo del manifiesto es la gran megalomanía de quien lo escribió, incluso se hace llamar el mentor, persona que guía o aconseja. Parece que el significado global de este escrito es la lucha por imponer valores que aún no están bien acogidos por muchas sociedades, a través de la formación de una hermandad parasocial que en ocasiones muestra tintes revolucionarios. Si en efecto se trata de una revolución poco convencional, entonces podemos compararla con cualquier otra forma de lucha por un cambio o al menos un esfuerzo por hacerse escuchar en un mundo considerado como indiferente a los intereses que no le convienen.

[371] Ob. Cit. http://rene1. Cjb. Net. " Crimen y Castigo en el Ciberespacio. Pág. 18.

Lo cierto es que, mientras el mundo de los hackers no sea aceptado como un valor convencional, seguirá siendo visto como oscuro. Lo que implica que personas con sentimientos de marginación y gran narcisismo lo tomen como un lugar seguro para manifestarse sin ser condenados y quienes se consideran adaptados a los valores convencionales lo vean como conductas que agreden sus intereses.

d) Seudónimos.

Como ya se ha mencionado con anterioridad, toda conducta es simbólica del pensamiento, habla de las necesidades, los deseos, los valores, las aspiraciones, pero también de la forma en que se comporta en la realidad el sujeto. Cuando dentro de un ambiente social determinado, alguien utiliza un seudónimo o sobrenombre para llamar a otro, este sobrenombre está basado en la apariencia física o en características de personalidad, que a juicio del que nombra son cubiertas por el apodado.

Cuando la misma persona apodada es quien ha inventado el sobrenombre, la situación se torna más interesante para el análisis, ya que podemos deducir que se trata de la percepción de características que el sujeto mismo tiene de sí englobados en una o varias palabras, o bien, es la manifestación del deseo de cómo la persona quisiera ser.

Para comprobar esta teoría, se tuvo la oportunidad de leer algunos casos de hackers y crackers que han sido presentados a juicio y en este sentido pudimos conocer su forma de ser y el sobrenombre que utilizaron para sus actividades.

- **Mitnick, Kevin, "El Cóndor", "El Chacal de la red".**

Analicemos las características del cóndor: Ave de rapiña, que puede medir hasta tres metros de envergadura y alza el vuelo a gran altura.

Chacal: Mamífero carnicero nocturno, parecido al lobo.

Tratemos de dar significado simbólico a las características de ambos animales: ambos son carnívoros, lo que comúnmente podemos llamar carnicero y cuyo significado simbólico se relaciona con alguien voraz, agresivo e incluso destructivo; Rapiña y nocturno, se puede relacionar con las actividades subrepticias; y vuelo a gran altura, en relación con el tamaño del ave, lo interpretaremos como una característica narcisista, egocéntrica del sujeto.

A continuación se describen las actividades mostradas por el sujeto y el lector decidirá si las características descritas arriba se relacionan con las características de personalidad del sujeto.

- ***Actividades de* Mitnick *Kevin, "El Cóndor", "El Chacal de la red"***[372].

Como Hacker, la carrera de Mitnick tiene sus inicios en 1980 cuando apenas contaba 16 años y, obsesionado por las redes de computadoras, rompió la seguridad del sistema administrativo de su colegio, pero no para alterar sus notas, lo hizo "solo para mirar". Su bautizo como infractor de la ley fue en 1981. Junto a dos amigos entró físicamente a las oficinas de COSMOS de Pacific Bell. COSMOS (Computer System for Mainframe Operations) era una base de datos utilizada por la mayor parte de las compañías telefónicas norteamericanas para controlar el registro de llamadas. Una vez dentro de las oficinas obtuvieron la lista de claves de seguridad, la combinación de las puertas de acceso de varias sucursales y manuales del sistema COSMOS. La información robada tenía un valor equivalente a los 200 mil dólares. Fueron delatados por la novia de uno de los amigos y debido a su minoría de edad una Corte Juvenil lo sentenció a tres meses de cárcel y a un año bajo libertad condicional.

Luego de cumplido el período de tres meses el oficial custodio encargado de su caso encontró que su teléfono fue desconectado y que en la compañía telefónica no había

[372] Ob. Cit. http://rene1. Cjb. Net. " Crimen y Castigo en el Ciberespacio. Págs. 21 al 25.

ningún registro de él. Sus objetivos iban creciendo a cada paso y en 1982 entró ilegalmente, vía módem, a la computadora del North American Air Defense Command en Colorado. Antes de entrar alteró el programa encargado de rastrear la procedencia de las llamadas y desvió el rastro de su llamada a otro lugar. El FBI, creyendo que había hallado a Mitnick, allanó la casa de unos inmigrantes que estaban viendo televisión.

Un año más tarde fue arrestado de nuevo cuando era estudiante de la Universidad del Sur de California. En esta ocasión entró ilegalmente a ARPAnet (la predecesora de Internet) y trató de accesar a la computadora del Pentágono. Lo sentenciaron a seis meses de cárcel en una prisión juvenil en California.

En 1987, luego de tratar de poner su vida en orden, cayó ante la tentación y fue acusado, en Santa Cruz California, de invadir el sistema de la compañía Microcorp Systems. Lo sentenciaron a tres años de libertad condicional y luego de la sentencia su expediente desapareció de la computadora de la policía local.

Luego buscó trabajo en lo que mejor sabía hacer y solicitó empleo en el Security Pacific Bank como encargado de la seguridad de la red del banco. El banco lo rechazó por sus antecedentes penales y Mitnick falsificó un balance general del banco donde se mostraban pérdidas por 400 millones de dólares y trató de enviarlo por la red. Afortunadamente el administrador de la red detuvo el balance antes de que viera la luz.

Ese mismo año inició el escándalo que lo lanzó a la fama. Durante meses observó secretamente el correo electrónico de los miembros del departamento de seguridad de MCI Communications y Digital Equipment Corporation para conocer cómo estaban protegidos las computadoras y el sistema telefónico de ambas compañías.

Luego de recoger suficiente información se apoderó de 16 códigos de seguridad de MCI y junto aun amigo, Lenny DiCicco, entraron a la red del laboratorio de investigaciones de Digital Corporation, conocida como Easynet. Ambos Hackers querían obtener una copia del prototipo del nuevo sistema operativo de seguridad de Digital llamado VMS. El

personal de seguridad de Digital se dio cuenta inmediatamente del ataque y dieron aviso al FBI, y comenzaron a rastrear a los hackers.....

Mitnick fue un mal cómplice y, a pesar de que habían trabajado juntos, trató de echarle toda la culpa a DiCicco haciendo llamadas anónimas al jefe de éste que trabajaba en una compañía de software como técnico de soporte. Lleno de rabia y frustración DiCicco le confesó todo a su jefe que los denunció a Digital y al FBI.

Mitnick fue arrestado en 1988 por invadir el sistema de Digital Equipment. La empresa acusó a Mitnick y a DiCicco ante un juez federal de causarles daños por 4 millones de dólares en el robo de su sistema operativo. Fue declarado culpable de un cargo de fraude en computadoras y de uno por posesión ilegal de códigos de acceso de larga distancia.

Adicional a la sentencia el fiscal obtuvo una orden de la Corte que prohibía a Mitnick el uso del teléfono en la prisión alegando que el prisionero podría obtener acceso a las computadoras a través de cualquier teléfono. A petición de Mitnick el juez lo autorizó a llamar únicamente a su abogado, a su esposa, a su madre y a su abuela y sólo bajo supervisión de un oficial de la prisión.

Este caso produjo revuelo en los Estados Unidos, no sólo por el hecho delictivo sino por la táctica que utilizó la defensa. Su abogado convenció al juez que Mitnick sufría de una adicción por las computadoras equivalente a la de un drogadicto, un alcohólico o un apostador. Gracias a esta maniobra de la defensa Mitnick fue sentenciado a sólo un año de prisión y al salir de allí debía seguir un programa de seis meses para tratar su "adicción a las computadoras". Durante su tratamiento le fue prohibido tocar una computadora o un módem y llegó a perder más de 45 kilos.

Para 1991 ya era el Hacker que había ocupado la primera plana del New York Times y uno de sus reporteros, John Markoff, decidió escribir un libro de estilo Cyberpunk narrando las aventuras de Mitnick. Al parecer a Mitnick no le gustó el libro ya que luego

de salir a la venta, la cuenta en Internet de Markoff fue invadida, cambiando su nivel de acceso, de manera de que cualquier persona en el mundo conectada a Internet podía ver su correo electrónico.

En 1992, y luego de concluir su programa, Mitnick comenzó a trabajar en una agencia de detectives. Pronto se descubrió un manejo ilegal en el uso de la base de datos y fue objeto de una investigación por parte del FBI quien determinó que había violado los términos de su libertad condicional. Allanaron su casa pero había desaparecido sin dejar rastro alguno. Ahora Mitnick se había convertido en un Hacker prófugo.

El fiscal no estaba tan equivocado cuando pidió la restricción del uso del teléfono. También en 1992, el Departamento de Vehículos de California ofreció una recompensa de 1 millón de dólares a quien arrestara a Mitnick por haber tratado de obtener una licencia de conducir de manera fraudulenta, utilizando un código de acceso y enviando sus datos vía fax.

Luego de convertirse en prófugo de la justicia cambió de táctica y concluyó que la mejor manera de no ser rastreado era utilizando teléfonos celulares. De esta manera podría cometer sus fechorías y no estar atado a ningún lugar fijo. Para ello necesitaba obtener programas que le permitieran moverse con la misma facilidad con que lo hacía en la red telefónica.

Luego de varios intentos infructuosos, en cuanto a calidad de información, se encontró con la computadora de Tsutomu Shimomura la cual invadió en la Navidad de 1994. Shimomura, físico computista y experto en sistemas de seguridad del San Diego Supercomputer Center, era además un muy buen Hacker, pero era de los "chicos buenos", ya que cuando hallaba una falla de seguridad en algún sistema lo reportaba a las autoridades, no a otros Hackers.

Shimomura notó que alguien había invadido su computadora en su ausencia, utilizando un método de intrusión muy sofisticado y que él nunca antes había visto. El intruso le había robado su correo electrónico, software para el control de teléfonos celulares y varias herramientas de seguridad en Internet. Allí comenzó la cuenta regresiva para Mitnick. Shimomura se propuso como orgullo personal atrapar al Hacker que había invadido su privacidad.

Hacia finales de enero de 1995, el software de Shimomura fue hallado en una cuenta en The Well, un proveedor de Internet en California. Mitnick había creado una cuenta fantasma en ese proveedor y desde allí utilizaba las herramientas de Shimomura para lanzar ataques hacia una docena de corporaciones de computadoras, entre ellas Motorola, Apple y Qualcomm.

Shimomura se reunió con el gerente de The Well y con un técnico de Sprint (proveedor de servicios telefónicos celulares) y descubrieron que Mitnick había creado un número celular fantasma para accesar el sistema. Luego de dos semanas de rastreos determinaron que las llamadas provenían de Raleigh, California.

Al llegar Shimomura a Raleigh recibió una llamada del experto en seguridad de InterNex, otro proveedor de Internet en California. Mitnick había invadido otra vez el sistema de InterNex, había creado una cuenta de nombre Nancy, borrado una con el nombre Bob y había cambiado varias claves de seguridad incluyendo la del experto y la del gerente del sistema que posee los privilegios más altos. De igual manera Shimomura tenía información sobre la invasión de Mitcnick a Netcom, una red de base de datos de noticias.. . .

Este persistente hacker actualmente está siendo juzgado y enfrenta dos cargos federales, uso ilegal de equipos de acceso telefónico y fraude por computadoras. Puede ser condenado por hasta 35 años y a pagar una multa de hasta medio millón de dólares. Mitnick también es sospechoso de robar el software que las compañías telefónicas piensan usar para todo tipo de procesos, desde la facturación hasta el seguimiento del

origen de una llamada pasando por la decodificación de las señales de los teléfonos celulares para preservar su privacidad.

Según el Departamento de Justicia de los Estados Unidos, este "terrorista electrónico", conocido como "el Cóndor", fue capaz de crear números telefónicos imposibles de facturar, de apropiarse de 20.000 números de tarjetas de crédito de habitantes de California y de burlarse del FBI por varios años

Kevin Mitnick. Este sencillo nombre, oculta la verdadera identidad de uno de los mayores hackers de la historia. Fue una de las mayores pesadillas del Departamento de justicia de los Estados Unidos. Entró virtualmente en una base de misiles y llegó a falsificar 20.000 números de tarjetas de crédito.

Al igual que el chico de la película "Juegos de Guerra", Mitnik se introdujo en el ordenador de la Comandancia para la Defensa de Norte América, en Colorado Springs.

Pero a diferencia del muchacho de Juegos de Guerra, Mitnik se dedicó a destruir y alterar datos, incluyendo las fichas del encargado de vigilar su libertad condicional y las de otros enemigos. La compañía Digital Equipment afirmó que las incursiones de Mitnik le costaron más de cuatro millones de dólares que se fueron en la reconstrucción de los archivos y las pérdidas ocasionada por el tiempo que los ordenadores estuvieron fuera de servicio.

Lunes, 22 de marzo de 1999. REDACCIÓN. El hacker más famoso del mundo, Kevin Mitnick, que dio lugar al guión de la película "Juegos de Guerra" y lleva en prisión desde 1995, ha conseguido un acuerdo con jueces y fiscales en vísperas del inicio de la vista, fijada para el 29 de marzo. Los términos concretos del acuerdo se desconocen, pues ninguna de las partes ha efectuado declaraciones, pero según informó, el jueves 18, "Los Angeles Times", Mitnick, de 35 años, podría quedar en libertad dentro de un año, aunque tendría prohibido durante tres años más el acceso a ordenadores y, además, se le

vetaría que obtuviera rendimiento económico contando su historia en medios de comunicación.

Sobre él pesaba una condena de 25 años por fraude informático y posesión ilegal de archivos sustraídos de compañías como Motorola y Sun Microsystems. La popularidad de Mitnick, que tiene su pagina en http://www.kevinmitnick.com/home.html, estalló ya en los años 80, cuando fue detenido cuatro veces. Estando en libertad provisional, en 1992, realizó diversas acciones de "hacking", y permaneció como fugitivo hasta su captura, en Carolina del Norte, en 1995.

A partir de ese momento, un buen número de hackers de todo el mundo, deseosos de que se produjera la excarcelación de su mentor, llevaron a cabo diversas acciones de intrusión en sistemas informáticos, el más notorio de los cuales fue el asalto, en septiembre de 1998, de la pagina del "New York Times", que quedó inoperativo durante un par de días. Encarcelado por el Gobierno norteamericano sin juicio, Kevin Mitnick había sido considerado por el FBI como el hacker más peligroso y escurridizo del mundo.

- **Zinn, Herbert, "Shadowhawk".**

El sentido de la palabra compuesta en inglés nos hace pensar en "sombra de halcón" o "halcón sombra", analíticamente podemos interpretarla como "ave de rapiña virtual". Es decir, el halcón es un ave rapaz relativamente pequeña y, sin embargo, el hecho de mostrarlo como sombra implica la subrepción, existe pero no de manera tangible, o como si no estuviera decidido a existir.

Otro significado de rapaz se refiere a usurero, ávido de ganancia, usurero e incluso inclinado al robo.

Por lo que el análisis simbólico como auto descripción sería: sujeto ávido de ganancia o usura, pero no a gran escala o poco convencido de ello.

- ***Actividades de "Shadowhawk"***[373]:

Fue el primer sentenciado bajo el cargo de fraude computacional y abuso en 1986. Zinn tenía 16 y 17 años cuando violó el acceso a AT&T y los sistemas del departamento de defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a $174,000 dls. estadounidenses en archivos y copias de programas. Publicó contraseñas e instrucciones de cómo violar la seguridad de los sistemas computacionales.

Aunque estos dos ejemplos muestran de manera gráfica la relación entre las manifestaciones conductuales y el contenido del pensamiento, es importante mencionar que cada caso en particular merece su exclusivo análisis. Sin embargo, las guías mostradas en este escrito pueden servir de manera amplia en la investigación y localización de un delincuente, no sólo informático sino de cualquier otro tipo.

3.5. ASPECTOS VÍCTIMOLOGICOS DE LOS DELITOS INFORMÁTICOS.

Cuando hablamos del sujeto pasivo ó víctima del delito, es evidente que referimos a la persona física o moral sobre la cual recae la conducta del sujeto activo, y en el caso las víctimas pueden ser individuos, empresas, instituciones bancarias, escuelas y un enorme etcétera.

La víctima del delito que nos ocupa, es sumamente importante para el estudio de los "*delitos informáticos*", ya que mediante él podemos conocer los diversos ilícitos que cometen los delincuentes informáticos, y muchos de ellos son descubiertos casualmente, y todo ello, por el desconocimiento del modus operandi de los sujetos activos.

Enfatizando que ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que muchos de estos no son descubiertos y por lo tanto no son denunciados a las autoridades competentes, y si a esto le sumamos el desconocimiento

[373] Ob. Cit. http://rene1. Cjb. Net. " Crimen y Castigo en el Ciberespacio. Pág. 27.

informático; la falta de leyes que protejan a las víctimas; la preparación por parte de las autoridades para comprender, investigar y aplicar la ley, así como el temor por parte de las empresas para denunciar este tipo de ilícitos, que muchas veces llegan al desprestigio de su propia empresa, sin olvidar las consecuencias económicas.

La Profesora Esther Morón, no señala que en cuanto a la etiología de esta desmesurada (zona oscura), se pueden advertir motivos específicos o inherentes a las nuevas tecnologías.[374] Así, en primer término, estas conductas son, en la mayoría de los casos, desconocida por las víctimas por dificultades de orden técnico. La posibilidad de trabajar en tiempo real, a distancia (el delincuente informático puede hallarse en el mismo despacho o en su domicilio, a kilómetros de distancia y en otro país), así como la habilidad y facilidad para no dejar huellas, contribuyen a que la víctima detecte la conducta ilícita debido a causas tan aleatorias como un error, una traición o la casualidad.[375]

En segundo, lugar, la víctima que acostumbra a ser una persona jurídica,[376] actúa como (colaboradora), en la medida que suele ocultar las conductas en las que se ve involucrada. La actitud poco favorable a la denuncia se debe al temor de que la trascendencia del hecho se traduzca en una suerte de descrédito de la fiabilidad de la gestión de la propia empresa (que, en este ámbito, se ciñe a una pérdida de confianza en los sistemas de seguridad de las redes informáticas) y de su prestigio. Así pues, a fin de evitar mayores pérdidas, prefieren resolver el problema internamente.[377]

Siendo evidente que en este tipo de delitos, el mejor cómplice del delincuente es su propia víctima.

---

[374] Existe acuerdo entre la doctrina a la hora de enunciar las causas del desconocimiento de este tipo de criminalidad. Ob. Cit. Morón Lerma Esther. Internet y Derecho Penal. Pág. 37.
[375] Idem. Pág. 37
[376] Afirma Gonzalez Rus, J.J. que los sectores más afectados por la criminalidad mediante computadora son la banca, la enseñanza, instituciones públicas, industrias de trasnformación y seguros. Ob. Cit. Morón Lerma Esther. Pa´g. 37.
[377] Camacho Losa, L. El Delito Informático. Madrid. 1987. Págs 11 y 69. Idem. Morón Lerma. Pág. 38.

Hoy día, existe la tendencia a evaluar el aumento o la disminución de los delitos a través de las víctimas del mismo.

El aprovechamiento –por parte del delincuente- del potencial de una persona para convertirse en víctima, es muy acentuado. Todo sujeto que se propone a cometer un delito, debe encontrar una víctima accesible.[378]

Siendo necesario, saber en que nos auxilia la victimología para este tipo de delitos.

Por lo que el estudio de la victimología revela el "comportamiento culpable de la víctima, estimulando, facilitando o agravando la lesión" al bien Jurídico.[379]

Ya que la Victimología puede definirse como el estudio científico de las víctimas. Es este aspecto amplio, la Victimología no se agota con el estudio del sujeto pasivo del delito, sino que atiende a otras personas afectadas, y a otros campos no delictivos como puede ser el de accidentes.[380]

Es indudable que la ciencia que más se ha enriquecido con la Victimología es la Criminología, áreas que no pueden estar separadas.

De acuerdo a las investigaciones sobre víctimas, los estudiosos se llevaron la sorpresa al descubrir que en una notable cantidad de hechos la víctima tenía una participación y, en ocasiones, era la verdadera causante del delito. Por lo que al clasificar a las víctimas podemos ver que hay:

[378] Barrita López Fernando A. Manual de Criminología. Edt. Porrúa. México. 1996. Pág. 158
[379] Idem. Pág. 159.
[380] Ob. Cit. Rodríguez Manzanera Luis. Criminología. Pág. 72

1.- Víctimas totalmente inocente. Es aquella que no tiene ninguna responsabilidad ni intervención con el delito.

2.- Víctima menos culpable que el criminal (víctima por ignorancia, víctima por imprudencia).

3.- Víctima tan culpable como el criminal. Es la víctima voluntaria (riña o duelo).

4.- Víctima más culpable que el criminal (víctima provocadora).

5.- Víctima totalmente culpable (víctima agresora, simuladora, imaginaria, etc.).

Para Mendelsohn víctima " Es la personalidad del individuo o de la colectividad en la medida en que está afectada por las consecuencias sociales de su sufrimiento determinado por factores de origen muy diversos- físicos, psíquicos, económicos, políticos o sociales, así como el ambiente natural o técnico".[381]

Así víctima sería la persona sobre quien recae la acción criminal o sufre en sí misma, en sus bienes o en sus derechos, las consecuencias nocivas de dicha acción.[382]

Mendelsohn[383] ha señalado que un delincuente tiene un solo camino que se le abre, el de infringir la ley. Sin embargo una víctima tiene por lo menos cinco posibilidades.

---

[381] Mendelsohn, Beniamin. La Victimología y las Tendencias de la Sociedad Contemporánea, Messis, Año 4, núm 7, págs 75 y ss, México, 1974. Citado por Rodríguez Manzanera Luis. Victimología " Estudio de la Víctima" Edt. Porrúa México 1996. Pág.57.

[382] Pratt farchild, henry, Diccionario de Sociología, Fondo de Cultura Económica, México, 1980. Pág. 311. Ob. Cit. Rodríguez Manzanera Luis. Victimología. Pág. 57.

[383] Mendelsohn, Beniamin, La Victimología y las Tendencias de la Sociedad Contemporánea, Ilanud al día, año 4, núm 10, San José Costa Rica, 1981, págs. 55 y ss. Ob. Cit. Rodríguez Manzanera Luis. Victimología . Pág. 59.

Se puede ser víctima de:

1. Un Criminal.
2. De sí mismo, por deficiencias o inclinación instintiva, impulso, psíquico o decisión consciente.
3. Del comportamiento antisocial, individual o colectivo.
4. De la tecnología.
5. De energía no controlada.

Por lo que no debemos de olvidar que " Quizá lo más importante del problema de la Victimología sea la deducción de que no solamente debemos hacer prevención criminal, sino también prevención victimal".[384]

Siendo de suma importancia este tipo de prevención victimal en los delitos informáticos, ya que en la mayoría de estos son causa de desconocimiento de la víctima por no contar con una cultura informática mínima.

Por todo lo anterior y descrito en este trabajo de investigación, se tuvo a bien llegar a las siguientes.

[384] Afirmación del criminólogo Luis Rodríguez Manzanera. Ob. Cit. Reyes Calderón José Alfredo. Criminología Pág. 124.

CONCLUSIONES.

1) En la actualidad, es un gran reto el potencial que trae consigo la tecnología informática, ya que sus consecuencias y sus características de dominio, plantean diversos desafíos a nuestro país, que aspira alcanzar una autonomía tecnológica, para consolidar su identidad cultural, y su firmeza económica, equilibrando su política, sin olvidar sus diversas alternativas legales, que tendrá que plantear el Poder Ejecutivo, Legislativo y Judicial, con la finalidad de adecuar la normatividad acorde a la evolución tecnológica y a las conductas que de ella se desprendan.

2) Ya que la humanidad ha progresado mucho más en los últimos cincuenta años que en cualquier otro periodo de la historia. Siendo una de estas razones, el avance tecnológico " la computadora". Efectivamente, el mundo está viviendo una segunda Revolución Industrial. Hoy conocida como la Revolución de la Información .

3) Ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en sus 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.

4) Siendo incuestionable el esfuerzo que tenemos que hacer en nuestro país, como una sociedad conciente, y adaptada a los combios de una era electrónica, que ayude al mejoramiento del bien común, sin perder de vista el compromiso que asumen nustras autoridades en salvaguardar la tutela jurídica a través de una adecuada protección jurídico -penal.

5) A través del presente estudio se ha podido establecer que en la actualidad es muy importante la relación que debe existir entre el derecho con la tecnología informática, como avance de toda regulación jurídica, la cual debe ser acorde a las actuales circunstancias y perspectivas sociales, económicas y políticas del país.

6) Debemos entender que el Derecho como la tecnología suponen cambios acelerados en un mundo informático, siendo imprescindible que el Derecho, aproveche convenientemente las ventajas de esas nuevas tecnologías, poniéndose a la vanguardia en sus ordenamientos legales, con la finalidad de proporcionar un orden y control, en base a una adecuada procuración e impartición de justicia, que la sociedad requiere acorde a una reestructuración legal, en beneficio de la misma.

7) Es de gran importancia destacar los avances que a tenido el derecho a nivel nacional e internacional, respecto a la informática jurídica y el derecho informático como ramas del derecho, reconociendo a la tecnología como un punto de partida que obliga a una nueva renovación del derecho, el cual tiene la necesidad de regular todos los fenómenos relacionados con la informática, los bienes y derechos fundamentales del hombre, así como las sanciones, civiles y administrativas a que pueden hacerse acreedores, además de las penales que son de mayor importancia, por la comisión de un delito.

8) Por lo tanto, no debe de haber excusa, por parte de nuestras autoridades, representantes, especialistas y profesionales del derecho en conocer la problemática jurídica derivada del uso y aplicación de las tecnologías informáticas y de comunicación, obligados siempre ha adquirir una formación y actualización básica, para el mejor desempeño de nuestra profesión en la solución de estos problemas.

9) No podemos quitar del renglón, la importancia que tiene la integración de estas materias al campo de estudio del derecho, así como la obligación de la debida difusión y enseñanza a todos los niveles de nuestra sociedad, como consecuencia de una cultura informática. Buscando siempre todo los medios necesarios para el logro de estos fines, llegando a todos un beneficio de acuerdo a una formación jurídica- informática.

10) También es compromiso de nuestros legisladores, el cumplir con los retos que deben enfrentar y superar del uso de las tecnologías, al cumplir con los objetivos de todo ordenamiento legal, que se vea reflejado en nuestras leyes aplicables a una realidad social.

11) Ya que el Derecho debe tener las respuestas, para facilitar la transición del medio físico al mundo virtual, hecho que debe regular a través de los ordenamientos jurídicos, para una convivencia social, flexibilizando a las instituciones en sus funciones e incorporando normas jurídicas aplicables a todos aquellos actos u omisiones que dentro del mundo informático, tengan consecuencias en el mundo real, castigando aquellos que cometan delitos.

12) Los delitos informáticos hoy en día, son una realidad latente, como riesgo que trae toda tecnología. Del cual sabemos y confirmamos que no tienen fronteras y que trae como consecuencias una variedad de problemas económicos, sociales y políticos, por lo que es necesario partir de una conciencia nacional e internacional ligada por su cooperación, a llevar el desarrollo adecuado de sus legislaciones e instituciones que combatan el creciente uso y abuso de los sujetos activos que utilizan una computadora. Pues no podemos hablar de la verdadera existencia de un derecho si no se ha reconocido previamente el mismo y se ha garantizado su ejercicio eficaz a través de la formulación en una norma jurídica.

13) Sin olvidar, entonces que no podemos dejar a un lado a la Ciencia del Derecho Penal, la cual nos ha aportado estudios y conocimientos del delito, el delincuente y la pena o medida de seguridad, aplicables a la realidad de un país, con el fin de salvaguardar los intereses jurídicos en favor de una persona o sociedad, como pago de su cultura, educación y religión, reflejo de un avance o retroceso de sus instituciones y leyes.

14) Reconocemos la gran importancia que tiene el conocer todo lo referente al delincuente informático, ya que al analizar su conducta en los aspectos bio-psico-social, nos aportara un panorama general de las causas que originaron a que el

sujeto cometiera el delito, sin olvidar claro, que la forma de actuar de cada persona se refleja en su forma de pensar y en ese sentido, todo acto es simbólico y representativo del pensamiento, por lo tanto tendremos elementos que nos ayudaran a investigar y perseguir a estos delincuentes.

15) Es indudable que nos enfrentamos con individuos, que tienen niveles de destreza y conocimiento relacionado a una computadora, algunos de ellos se destacan por ser brillantes, ambiciosos, motivados y dispuestos a aceptar nuevos retos tecnológicos, pero existe una linea divisoria entre la persona que se deja llevar por sus inquietudes de conocer y aprender, a la persona que es motivada para obtener un lucro, causar un daño u obtener un beneficio personal, llegando a ser un sujeto activo en potencia.

16) Es real que la conducta delictiva que estamos estudiando, puede tener diversas variables, como edades en que se cometen estos delitos que van desde los 15 hasta los 60 años, los niveles económicos, sociales, educativos y culturales, con los que cuenta una persona que entra a un sistema informático por curiosidad, por investigar o con la intención de violar un sistema de seguridad para llegar a un fin, que es diferente al empleado de una institución o empresa que tiene todos los conocimiento técnicos e informáticos y que maneja información sensible la cual tiene un valor.

17) Sabemos que las computadoras vienen a formar parte de un factor que auxilia a la conducta criminal, en ocasiones como objeto o como instrumento, ofreciendo un inmenso abanico de técnicas y estrategias que pueden disponer los delincuentes en la consumación de un delito, aportando con esto nuevas formas para su cometido. También sabemos que la información tiene un valor, la cual se ve refleja en el conocimiento, poder y dinero. Cuando la información se convierte en objeto de apropiación y en el blanco lucrativo del delincuente, se ven afectados diversos bienes jurídicos como son la intimidad, el orden socioeconómico, la fe pública y la seguridad social o del estado, entre otros muchos.

18) Por lo tanto no podemos dejar a un lado, la gran importancia que tiene la criminología, dentro del área jurídica, como ciencia que estudia todas las causas y fenómenos de la comisión de un delito, y de la cual se ocupa de la personalidad del delincuente, su desarrollo, sus características físicas y psíquicas en relación al delito, con el fin de aportar todos los elementos de prevención y tratamiento del delincuente.

19) Es cierto que el perfil criminológico de un delincuente informático apunta hacia el estudio de las causas, fenómenos, factores y características que lo rigen en su forma de actuar o cometer una conducta delictiva. Ya que el delincuente tecnológico asume una actitud de reto con los sistemas informáticos y con esto se encuentra al margen de que su conducta traspase o no al ámbito delictivo o criminal.

20) Ahora bien, sabemos que las ciencias auxiliares como la Sociología, la Antropología, la Biología y Psicología Criminal, nos ayudan a estudiar los problemas que acarrea un delincuente informático, explicando las causas de su conducta, cuando esta traspasa la legalidad de su actuar, aportando nuevos modelos o hipótesis, que servirán a la investigación de estos delitos. Pero aun más dará los elementos para tomar medidas preventivas y no represivas.

21) Por lo tanto no podemos dejar al olvido a la víctima o víctimas del delito informático, ya que mediante estos hemos podido conocer las diversas formas en que operan los delincuentes informáticos, siendo preocupante que la mayoría de estos son descubiertos casualmente, evidenciándose que el mejor cómplice del delincuente es su propia víctima. Toda vez que hemos olvidado o no queremos reconocer que somos parte de una revolución informática, que nos obliga a estudiar y prepararnos a los cambios que se avecinan, retomando entonces una prevención victimal.

PROPUESTAS.

Una vez valorada y analizada nuestra investigación, consideró importante establecer las siguientes propuestas, que en forma positiva, podría aportar este trabajo:

PRIMERO.- Requerimos urgentemente adelantos en nuestros ordenamientos jurídicos, en los que se contemplen los riesgos de una sociedad creciente en sus tecnologías, atravesando la barrera del tiempo en favor de una protección penal, tipificando conductas que por su resultado pueden dañar algún bien jurídico tutelado o ponerlo en peligro, por el simple acceso a un sistema informático, que muchas de las veces se puede convertir en acciones de otros delitos. Considerando necesario la incriminación autónoma, de estos comportamientos como objeto de estudio de esta investigación, haciendo las siguientes ***propuestas:***

1.- Reformar y adicionar el Código Penal para el Distrito Federal,[1] como consecuencia de una criminalidad informática, en el cual se debe aplicar una sanción en atención al delito. Y de acuerdo a mis consideraciones propondría para efectos de estos delitos:

El artículo 399 Cuater.- Que a la letra diga "Se sancionara con pena de prisión de uno a tres años y de ciento cincuenta a trescientos días multa al que utilice de cualquier forma una sistema informático o telemático, como instrumento u objeto, en la comisión de otro delito, de los señalados por este Código Penal, independientemente de la sanción que le correspondiere al mismo delito".

[1] Propuestas que también fueron plateadas, por el Diputado Francisco Suarez Tanorio del Grupo Parlamentario del Partido Acción Nacional, en fecha 22 de marzo del 2000, "Iniciativa de Reformas y Adiciones sobre diversas disposiciones del Código Penal para el Distrito Federal en materia de Fuero Común, y para toda la República en materia de Fuero Federal Artículo Unico: Se reforma del Título quinto, el capítulo I, artículo 167 párrafo VI; y del capítulo II del mismo título, se reforman los artículos 173 y 174, y se adiciona el artículo 174 bis. Se adiciona al Título Vigesimosegundo, capítulo III, con el artículo 389 ter, se adiciona el capítulo VII del mismo título con el artículo 399 ter, párrafos I al VIII, así como una reforma al título Vigésimo sexto, artículo 424".

2.- Por lo tanto, y como consecuencia de este nuevo catalogo de delitos, es importante adecuar nuevas reformas y adiciones a la Ley Orgánica de la Procuraduría General de Justicia del Distrito Federal, en donde se contemple la creación de un Fiscalía Especializada en Delitos Informáticos, la cual estará facultada para investigar y perseguir estos delitos, aportando los elementos necesarias que acrediten un delito y la responsabilidad penal ante el Órgano Jurisdiccional.

Sin olvidar la colaboración que debe haber entre las Procuradurías locales y la Procuraduría General de la República, en la investigación y persecución de delitos informáticos, como base de una cooperación nacional e internacional cuando se trate de otros países, con el fin de obtener frutos que garanticen y salvaguarden los intereses individuales, colectivos, nacionales e internacionales en favor de un bien común.

Respuesta que debe plantearse, en atención al creciente uso de la tecnología transnacional, que se ha vuelto hoy, un peligro eminente en la vulneración de redes, como el internet, creando problemas jurídicos relacionados a la competencia y jurisdicción de los países, cuando se ven afectados por una conducta criminal que se inicio en un país y se consumo en otro.

Siendo importante señalar, que se deberá revisar y actualizar, de nuestros ordenamientos jurídicos, los temas relativos a la jurisdicción, extradición y cooperación nacional e internacional, en base a los Acuerdos de Colaboración de los Estados y los Tratados Internacionales con otros Países, en atención al combate de los delitos informáticos.

Proponiendo los siguientes puntos:

Cooperación Nacional e Internacional, en la que se represente una entidad de 24 horas los 360 días, a través de una Fiscalía, Unidad o Agencia Especializada, para la investigación y persecución de los delitos informáticos, atendiendo los siguientes fines.

I. Asistencia Mutua, en el combate de estas actividades ilícitas.
II. La colaboración para la capacitación del personal que investiga estos delitos, en función de una ayuda bilateral, regional o internacional.
III. Intercambio de información en la investigación de los delitos informáticos.
IV. Ayuda Mutua entre Autoridades Ministeriales y Policiales en la investigación de los delitos.
V. Apoyo Jurídico en las circunstancias de emergencia.
VI. Asistencia Mutua, en los mecanismos de cooperación e intercambio de información, a fin de iniciar o recibir denuncia o querella por estos delitos.
VII. Colaboración, para la realización de tramites y diligencias Judiciales, en los casos de detención de personas, preservación de lugares y aseguramiento de objetos, documentos o instrumentos informáticos relacionados con un delito.
VIII. Colaboración de los Estados para la extradición de los delincuentes informáticos.
IX. Cooperación Internacional, respecto a las extradiciones relacionadas con los delincuentes informáticos.

SEGUNDO.- La prevención del delito informático, será por lo tanto, otro de los puntos a desarrollar, ya que la peculiaridad de estos ilícitos ha sido el problema para detectarlos, como un evidente reflejo de la falta de conocimientos de sus víctimas.

Debiendo entonces quedar muy claro, que las medidas preventivas del delito, serán el día de mañana la forma mas adecuada de atacarlo. Partiendo de una cultura informática, en donde el papel de la *educación juegue el rol más importante,* por lo que se deberá:

1.- Replantear los planes de estudio en favor de la educación informática, llegando a todos los niveles de conocimiento, interactuando con las instituciones educativas, asociaciones, empresas e industrias, con el fin prevenir estos delitos, evitando ser víctimas potenciales de estas conductas.

2.- Proponer nuevos proyectos, que den la base al mejoramiento de la educación ético-legal, sobre el uso y abuso de las tecnologías.

3.- Por lo que será necesario proponer reformas y adiciones a nuestra Constitución Política Federal. En su artículo 3o.- Respecto a que " Todo individuo tiene derecho a recibir educación..... "

Proponiendo se Agregue en sus fracciones lo siguiente.

II.- El criterio que orientará a esa educación se basará en los resultados del progreso científico, **tecnológico e informático, luchando contra la ignorancia y sus efectos**, las servidumbres, los fanatismos y los perjuicios.

V.- Además de impartir la educación preescolar, primaria y secundaria, señaladas en el primer párrafo, el Estado promoverá y atenderá todos los tipos y modalidades educativos- incluyendo la educación superior- necesarios para el desarrollo de la Nación, apoyará la investigación **científica, tecnológica e informática,** y alentará el fortalecimiento y difusión de nuestra cultura **por medio de la información**;

3.- De igual forma, deberá iniciarse la postura de reglamentar los ordenamientos internos, como obligación de las empresas, industrias, fabricas, instituciones y demás entidades jurídicas, con la finalidad de tomar medidas preventivas, como la vía más eficaz para combatir la criminalidad informática, llevando a cabo auditorías preventivas como medidas disuasorias, con el fin de evitar irregularidades, fiscalizando más a sus empleados.

Reconociendo plenamente, que no hay medida preventiva mas eficaz que el combate contra la ignorancia informática, que dará como resultado las bases a una sociedad consciente de su tecnología.

BIBLIOGRAFIA.

Obras.

Amuchategui Requena Irma. Derecho Penal. Edit. Harla México 1993.

Bacigalupo, Enrique. Lineamientos de la Teoría del Delito, Hammurabi SLR. Buenos Aires, Argentina 1989.

Barrita López Fernando A. Manual de Criminología. Edit. Porrúa. México. 1996.

Bartolini Esparza Marcelo en su Tesis para obtener el tituto de Licenciado en Derecho. El "Dinero Electrónico " a la luz del Derecho Positivo Mexicano. Universidad la Salle, A.C., Facultad de Derecho. México, D. F., 1999.

Basile Alejandro, A. Fundamentos de Medicina Legal: deontología y bioética ·3ª Ed. Buenos Aires: El ateneo 1999.

Castellanos Tena Fernando. Lineamientos Elementales de Derecho Penal. Edit. Porrúa. México. 1989.

Davara Rodríguez, Miguel Ángel. "Manual de Derecho Informático", Edit. Aranzadi, Pamplona, España 1997.

Davara Rodríguez, Miguel Angel. Derecho Informático. Edit. Aranzadi. Pamplona. España. 1993.

Daza Gomez Carlos Juan Manuel. Teoría General del Delito. Edit. Cardenas Editores Distribuidor.

Eberhard Struensee. Temas sobre Teoría del Delito. Instituto Nacional de Ciencias Penales. México. 1999.

Ferreira Delgado Franciso. Teoría General del Delito.Edit. Temis, S.A. Bogotá-Colombia, 1988.

Flores Olea, Víctor. Internet y la Revolución Cibernética. Editorial Océano de México, 1997.

Gisbert Calabuig Juan Antonio. Medicina Legal y Toxicología. 5ª Ed. Messon, S. A. Barcelona España. 1999.

Gómez Benitez José Manuel. Teoría Jurídica del Delito. Derecho Penal. Parte General. Edt. Civitas, Madrid, 1988.

Gookin Dan y Rathbone Andy, PCs para Inexpertos, Edit. Limusa, S.A. de C.V. México, D. F. 1998.

Halliday Caroline M. Secretos de los Sistemas de PC, Edit Limusa, S.A. de C.V., México 1994.

Jascheck Hans Heinrich. Tratado de Derecho Penal, Parte General. Vol I 3ra. Edición Edit. Bosch Barcelona 1989.

Lima de la Luz, María. Delitos Electrónicos en Criminalia. México. Academia Mexicana de Ciencias Penales. Edt. Porrúa. No. 1-6 AñoL. Enero- Junio 1984.

López Ayllón Sergio, Derecho a la información, México, Edt. Porrúa 1984.

López Batancourt Eduardo. Teoría del Delito, Edit. Porrúa, México, 1998.

Maggiore Giuseppe. Derecho Penal, Vol I 2da edición Edit. Tamis Bogota 1989.

Maguire Mike, Morgan Rod y Reiner Robert. Manual de Criminología Volumen 4. Oxford University Press. 1999.

Marcó del Pont, Luis, Nadelsticher Mitrani, Abraham. "Delitos de Cuello Blanco y Reacción Social", Instituto Nacional de Ciencias Penales, México 1981. Cuademo no.8 o págs. 17/23.

Marchiori, Hilda. Psicología Criminal. Edit. Porrúa, México, 1975.

Maurach, Reinhart, Tratado de Derecho Penal, tomo I, Edit. Ediciones Ariel, Barcelona 1962.

Méjan C. Luis Manuel. El Derecho a la Intimidad y la Informática, Segunda Edición, Edit. Porrúa México, 1996.

Morón Lerma Esther, Internet y Derecho: (hacking) y Otras Conductas Ilícitas en la Red. Edit. Arazandi, S.A. 1999. Pamplona España.

Muñoz Conde Francisco. Teoría General del Delito, Temis, Bogotá 1990.

Muñoz de Alba, Marcia., Manejo de la Información Vs. Vida Privada., en Núcleo de Estudios Interdisciplinarios en Salud y Derechos Humanos, reunión 16-I-95, Instituto de Investigaciones Jurídicas, Universidad Autónoma de México, México, 1995.

Novoa Monreal Eduardo. Derecho a la Vida Provada y Libertad de Información, un conflicto de Derecho. Edit. XXI Siglo Veintiuno Editores, S.A. México, Espeña, Argentina, colombia. 1981.

Orellana Wiarco Octavio Alberto. Teoría del Delito. Sistema Causalista y Finalista. 3ª Edic., Edit. Porrúa México 1996.

Pavón Vasconcelos Francisco. Derecho Penal Mexicano. Decimasegunda Edic., Edit Porrúa S.A. México. 1995.

Pierre Gratton. Protección Informática. Edit. Trillas. México 1998.

Plascencia Villanueva Raúl. Teoría del Delito. Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México. México 1998.

Reyes Calderón José Alfredo, Criminología, 2ª Ed. Cardenas Editor Distribuidor. México 1998.

Reynoso Dávila Roberto en su obra Teoría General del Delito. Edit. Porrúa. México, 1997.

Rodríguez Manzanera Luis. Criminología. Edit. Porrúa. México, 1998.

Rodríguez Manzanera Luis. Victimología " Estudio de la Víctima" Edit. Porrúa México 1996.

Romero Coloma Aurelía María. Derecho a la Información y Libertad de Expresión, Especial consideración al Proceso Penal. Edit. Bosh, Casa Editorial, S.A. 1984. Barcelo España.

Sánchez Goyanes Enrique "Constitución Española Comentada". " 21ª Edición . Edt. Pararninfo. Madrid, España, 1998.

Sander, Donald. Informática. Presente y Futuro, McGraw- Hill, México, 1985.

Téllez Valdés Julio, Derecho Informático, Segunda Edición, McGraw-Hill México 1996.

Toffer, Alvin. El Shock del Futuro.

Zaffaroni, Eugenio Raúl, Manuel de Derecho Penal. Parte General, 2ª Ed., Edit. Cárdenas Editores y Distribuidores, México 1991.

Análisis de Invesitgación.

Abizaid Peréz Mauricio Rafael. Estudio sobre la "Descripción de Rasgos Psicológicos Notorios en Hackers" Licenciado en Psicología Encargado del Programa de Psicología Forense en el Instituto de Formación Profesional de la Procuraduría General de Justicia del Distrito Federal. Septiembre del 2000.

Seminarios.

Alan Brock, Dr. De la Universidad Estatal de Pennsylvania. Penalistas. Lic. Eduardo Ibarrola y Mtro. José Trinidad Larrieta de la Procuraduría General de la República, Dr. Jorge Chabat del Centro de Investigación y Docencia Económica, Dra. Celia Toro, Colegio de México, Ernesto López Portillo, Instituto Nacional de Ciencias Penales y Lic. Raúl Roldan, Agregado Jurídico de la Embajada de los Estados Unidos de América. Apuntes "Seminario México-EUA sobre Crimen Organizado Trasnacional", celebrado en el auditorio Alfonso Quiroz Cuarón del Instituto Nacional de Ciencias Penales el día 11 de Agosto del 2000.

Miraut Martín Laura. Apuntes "La Experiencia Española". Curso Introducción a los Delitos Informáticos, impartido en el Instituto Nacional de Ciencias Penales. Julio del 2000.

Ojales, Rodolfo. Abogado del Ministerio de Justicia de los Estados Unidos. CCIPS (Computer Crime and Intellectual Proporty Section) U. S. Departmen of Justice.

Apuntes de "La expericencia Estadounidense" Curso Introducción a los Delitos Informácticos, Instituto Nacional de Ciencias Penales, Julio del 2000.

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.

Revista Electrónica en Internet.

Almeida, Carlos Sánchez. Bufete Almeida "El Hacking ante el Derecho Penal. Una visión Libertaria". http://www.bufetalmeida.com (España).

Bauzá Reilly Marcelo. Abogado. Asesor en temas de Derecho & Informática. Doctor en Derecho y Ciencias Sociales, Profesor de Informatica Jurídica de la Universidad de la República, Director de CINADE (Centro de Investigación de Informática Aplicada al Derecho, Facultad de Derecho de la UR), DEA en Informática Jurídica y Derecho de la Informática en la Universidad de Montpellier, Vicepresidente de FIADI (Federación Iberoamericana de Derecho e Informática). (Uruguay). "Informática Jurídica en la Facultad de Derecho. Roles y Perpectivas". 1999. Derecho Og. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www. Yahoo.com).

Calderón Rodriguez Cristian L. Abogado. Miembro del Cibertribunal Peruano.Especialista en Comercio Exterior. Miembro del Instituto Peruano de Comerio Electrónico. Conciliador del Centro de Conciliación de la Pontificia Universidad Católica del Perú. "El Impacto de la Era Digital en el Derecho". Perú 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www.yahoo.com).

Cantú Aguillén Ricardo. Miembro del Comité Académico del Instituto de la Judicatura del Estado de Nuevo León. Miembro adscrito del Instituto de Investigaciones Jurídicas de la facultad de Derecho y Ciencias Sociales de la U.A.N.L. (México) en su artículo "Tendencias actuales de la Informática y el Derecho a Nivel Internacinal". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www.yahoo.com).

Cuervo Alvarez José. Abogado, especializado en temas de Derecho Informático. (España) " Los delitos informáticos: protección penal de la intimidad". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. (www.yahoo.com).

De Paladella Salord Carlos. Abogado por la Universidad deBarcelona (España), Master en Derecho de Empresas por la Universidad Austral (Argentina) y posgrado de especialización sobre Revolución Digital CENIT. (España). "El Derecho en la Era Digital. Aspectos Jurídicos de las nuevas tecnologías de la información y de las comunicaciones (Parte I)". 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, (www.yahoo.com).

De Paladella Salord Carlos. "Derecho en la era digital. Aspectos jurídicos de las nuevas tecnologías dela información y de las comunidades (Parte II) Web. http// comunidad. Derecho. Org. /carlospaladella/ Director de Derecho Org. Argentina (España).

Fígoli Pacheco Andrés J. Apuntes "El Acceso No Autorizado a Sistemas Informáticos". (internet InfoJur.ccj. ufsc.br).

García Aguilar, Nicolás Licenciado en Informática. Diplomado en Derecho. Titulado Superior de Telefónica de España. Miembro de la Asociación de Licenciados en Informática (ALI) y de la Federación Iberoamericana de Asociaciones de Derecho

e Informática (FIADI). (España) "La cuestión de la responsabilidad en el Derecho Informático". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. (www.yahoo.com).

Gómez Pérez, Mariana. Organización Nacional de Bufetes Colectivos, CUBA. Editora en jefe de Revista Electrónica de Estudios Jurídicos (CubaLex) (Cuba) "Criminalidad informática: un fenomeno de fin de siglo". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), (www.yahoo.com).

Jiménez Dan, Rafael Ricardo Gerente de Tecnologías del Proyecto de Modernización de la Corte Suprema de Venezuela. (Venezuela) "Crimen Silencioso". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), (www.yahoo.com).

Lara Márquez Jaime. Abogado. Profesor de Informática Jurídica de la Pontificia Universidad Católica del Perú (Perú). "Derecho y Técnologia." "Una visión prospectiva del Derecho". 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www.yahoo.com).

Líbano Manzur Claudio. Abogado Profesor. Director Secretario Ejecutivo de la Asociación de Derecho Informático de Chile (ADI-CHILE) "Los Delitos de Hacking en sus Diversas Manifestaciones". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. (www.yahoo.com).

Nuñez Ponce Julio. Catedratico de Derecho Informático en la Universidad de Lima.(Perú) " Los delitos informáticos". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. (www.yahoo.com).

Pelaéz Hemández Eduardo, Memorias del Foro de Consulta sobre Derecho e Informática, Ponencia "Algunas consideraciones sobre la reglamentación del Derecho a la Información mencionado en el artículo 6ª Constitucional", Monterrey, Nuevo León, Septiembre de 1996. Aviso Legal 1999. Cámara de Diputados del H. Congreso de la Unión (www. Yahoo.com).

Peña Helen, Palazuelos Silvia, Alarcón Rosalía. "Delitos Informáticos". División de Estudios de Posgrado, Facultad de Derecho. UNAM 21 de mayo de 1997. Servidor de la Universisad Autonoma de Sinaloa. México 1997. (Web. http// www. Yahoo.com).

Peñaranda Hector. Doctor en Derecho Magister en Gerencia Tributaria, Profesor y Jefe de Cátedra de la materia: Seminario de Informática Jurídica de la Universidad Rafael Belloso Cacín, Maracaibo. Venezuela. " La informática jurídica y el Derecho informático com ciencias. El derecho informático como rama autónoma del Derecho". 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www.yahoo.com).

Perez Marayo Guillermo Augusto. Abogado y Notario, Universidad Complutense de Madrid. Asesor Parlamentario, especialista en Investigación de Información en el Internet, "Instrumentos de Pago Internacional, Tecnología Informática y Comercio Electronico". (Costa Rica) Derecho, Tecnología y Cambio. 1999. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), (www.yahoo.com).

Raymond, Eric. The New Hackers Dictionary. The MIT Press, 1991. (La versión electrónica "Jargon File Resources" está disponible en: http:// www.ccit.orgliargonl). recopilación de información hecha por http://rene1. Cjb. Net. " Crimen y Castigo en el Ciberespacio. Hermosillo Sonora, México. Diciembre de 1999.

Rodríguez da Costa, Marco Aurélio. Abogado de Uruguaiana. (Brasil) "El Derecho Penal informático vigente en Brasil" El presente trabajo corresponde a una parte del ensayo publicado por el autor en Jus Navigandi ("Crimes de Informática"), traducción de Luis Miguel Reyna Alfaro, bajo autorización del autor. Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), (www.yahoo.com).

Rodríguez Hernández Victor, Director de la Revista Electrónica de Derecho Mexicano. "La Informática Jurídica y su Papel en el Derecho Méxicano".1999 Derecho Org.(México) R.E.D.I. (Revista Electrónica de Derecho informático, Edita. Derecho Org: Portal Jurídico en Internet. Dorigen: Erick Iriarte y Luis Faus (www. yahoo.com.).

Viega Rodríguez María José. Doctora en Derecho y Ciencias Sociales. Escribana Pública. Integrante del CINADE (Centro de Investigaciones de Informática aplicada al Derecho), Facultad de Derecho de la Universidad de la República. (Uruguay). " Delitos Informáticos". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático, Edita. Derecho Org: Portal Jurídico en Internet. (www.yahoo.com).

Villalba Díaz, Federico Andrés. Abogado y Secretario Judicial de la Fiscalía de Primera Instancia en lo Contravencional N° 10. Titular de Derecho de Autor y Marca de la Facultad de Ciencias Jurídicas de la Universidad Abierta Interamericana. "Argentina: Los delitos y contravenciones informáticas. Los Hackers y el Código Contravencional de la Ciudad de Buenos Aires". Derecho Org. R.E.D.I. (Revista Electrónica de Derecho Informático), (www.yahoo.com).

Legislación.

Anexo Agenda Civil 2000. Decreto por el que reforma y adiciona diversas disposiciones del Código Civil para el Distrito Federal en Materia Comun y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles. Ediciones Fiscales ISEF.

Código Civil para el Distrito Federal. Agenda Civil 98, Edit. ISEF. S.A.

Código Penal Federal. Edit. Sista. México 1999.

Código Penal. Agenda Penal 98, Compendio de Leyes Penales. Edt. ISEF.

Código Penal para el Distrito Federal, con las disposiciones legales conocidas hasta octubre de 1999, Edit. Sista.

Código Penal y Procedimientos Penales de Sinaloa. Edt. Anaya Editores, S.A. México 1998.

Código Penal. Edición 2000, Edt. Biblioteca Nueva, Madrid. España.

Cuadernos de Derecho, Compilación y Actualización Legislativa, Constitución Política de los Estados Unidos Mexicanos, Vol. 67, enero de 2000, Director Lic. Jorge Orozco Flores, Publicación de ABZ Editores S.A. de C.V.

Convenio núm. 108 del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; BOE de 15 de noviembre de 1985.

El sistema UNAM-JURE un banco de datos legislativos, Dirección General de Publicaciones, Universidad Nacional Autónoma de México, México, 1985.

Legislación básica de informática. Edición preparada por Alvarez Rico Manuel, Catedrático de la Universidad Pontificia de Salamanca, Heredero Higueras Manuel, Doctor en Derecho, Abogado; Alvarez Rico Isabel, Universidad Poncificia de Salamanca, Facultad de Informática, Abogada. Madrid, Edit. Tecnos, S.A., Madrid. España 1999.

Ley 16/1993, de 23 de diciembre, de incorporación al Derecho español de la Directiva 91/250/CEE, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador; BOE de 24 de diciembre de 1993.
Ley 22/1987, de 11 de noviembre, de Propiedad Intelectual; BOE de 17 de noviembre de 1987.

Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común; BOE de 27 de noviembre de 1992.

Ley Federal del Derecho de Autor. Secretaria de Educación Pública. México, 1997.

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal; BOE de 31 de octubre de 1992.

Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la LORTAD; BOE de 21 de junio de 1994.

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos; BOE de 4 de mayo de 1993.

Manuales.

Autor Anonimo "Manual de Referencias Didacticas de Informática", realizado por la Subdirección de Control Interno y Desarrollo del Instituto de Formación Profesional de la Procuraduría General de Justicia del Distrito Federal.

Manual de Fundamentos Técnicos y Científicos para la Investigación Policial, Instituto de Formación Profesional, Procuraduría General de Justicia del Distrito Federal. Mayo del 2000.

Manual de Informática y las Telecomunicaciones, eleborado por la Dirección General de Tecnología y Sistemas Informaticos de la Procuraduría General de Justicia del Distrito Federal, (Curso Basico de Computación "La informática como herramienta para el personal sustantivo de la PFJDF) 1998.

Manuel de Naciones Unidas sobre la Prevención y control de delitos relacionados con la computadora. Revisión internacional de política criminal. 9 de mayo de 1996. Area de Traducción e Idiomas del Instituto de Formación Profesional de la Procuraduría General de Justicia del Distrito Federal. Coordinadora Beatriz Macin Lara. Julio del 2000.

Revistas.

Castro Fernández Diego, "El delito informático" Revista Jurídica número 41 en San Jose, Costa Rica.

Rojas Alberto en su artículo "¿Ya vacunó a su PC?" Artículo - Revista PCMPS.

Selecciones. Se equivoco George Owell. Kinsley, Michael. Editorial Reader's Digest. D.F. octubre de 1997.

Periodicos.

Business WeeK, The Microchip Revolution: Preciding New Society, 10 Nov. 1980.

El Universal. Internet hoy, mañana y a futuro. Guerra, Víctor. Universo de la Computación. Lunes 3 marzo, 1997.

El Universal. Internet/Intranet: ¿realidad o espejismo?. Pérez Fajardo, Judith. Universo de la Computación. Lunes 27 de octubre de 1997.

La Jornada. La Jornada Virtual. Yehya, Naief. Domingo 27 de abril de 1997. Cultural.

Reforma. Genera Oportunidades Comercio Electrónico. Chavez, Miguel Angel. Interfese. Lunes 28 de abril de 1997.

Reforma. Hay tecnología, falta confianza. Kanell. E. Michael. Interfase. Lunes 28 de abril, 1997.

Diccionarios e Enciclopedias.

Cabanellas de las Cuevas Guillermo y Hoague Eleanor C. Diccionario Jurídico, Inglés- Español. Edit. Heliasta S.R.L. Buenos Aires, Argentina 1996.

Dan Gookin, Wally Wang y Chris Van Buren. Diccionario Ilustrado de Computación para Inexpertos, Edit. Limuna, S.A. de C. V. 1995.

Enciclopedia Microsoft® Encarta® 2000. © 1993-1999 "Informática," Microsoft Corporation.