UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE DERECHO

"MODIFICACION DEL ARTICULO 211 BIS 1 PARTE PRIMERA DEL CODIGO PENAL FEDERAL POR RELACIONARSE CON EL DELITO DE DAÑO EN PROPIEDAD AJENA"

T E S I S

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN DERECHO

PRESENTA:

MARINA JIMENEZ LUCIANO

ASESOR:

LIC. CARLOS BARRAGAN SALVATIERRA

MEXICO, D. F. **2005**

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO
SEMINARIO DE DERECHO PENAL
OFICIO INTERNO FDER/099/SP/05/05
ASUNTO: APROBACION DE TESIS

DIRECTOR GENERAL DE LA ADMINISTRACION
ESCOLAR DE LA U.N.A. M.
P R E S E N T E.

La alumna **JIMÉNEZ LUCIANO MARINA,** ha elaborado en este Seminario a mi cargo y bajo la dirección del **LIC. CARLOS BARRAGÁN SALVATIERRA,** la tesis profesional titulada **"MODIFICACIÓN DEL ARTÍCULO 211 BIS 1 PARTE PRIMERA DEL CÓDIGO PENAL FEDERAL POR RELACIONARSE CON EL DELITO DE DAÑO EN PROPIEDAD AJENA"** que presentará como trabajo recepcional para obtener el título de Licenciado en Derecho.

El profesor **LIC. CARLOS BARRAGÁN SALVATIERRA** en su calidad de asesor, nos informa que el trabajo ha sido concluido satisfactoriamente, que reúne los requisitos reglamentarios y académicos, y que lo aprueba para su presentación en examen profesional.

Por lo anterior, comunico a usted que la tesis **"MODIFICACIÓN DEL ARTÍCULO 211 BIS 1 PARTE PRIMERA DEL CÓDIGO PENAL FEDERAL POR RELACIONARSE CON EL DELITO DE DAÑO EN PROPIEDAD AJENA"**, puede imprimirse para ser sometida a la consideración del H. Jurado que ha de examinar a la alumna **JIMÉNEZ LUCIANO MARINA.**

En la sesión del día 3 de febrero de 1998, el Consejo de Directores de Seminario acordó incluir en el oficio de aprobación la siguiente leyenda:

"El interesado deberá iniciar el trámite para su titulación dentro de los seis meses siguientes (contados de día a día) a aquél en que le sea entregado el presente oficio, en el entendido de que transcurrido dicho lapso sin haberlo hecho, caducará la autorización que ahora se le concede para someter su tesis a examen profesional, misma autorización que no podrá otorgarse nuevamente sino en el caso de que el trabajo recepcional conserve su actualidad y siempre que la oportuna iniciación del trámite para la celebración del examen haya sido impedida por circunstancia grave, todo lo cual calificará la Secretaría General de la Facultad"

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cd. Universitaria, D. F., a 9 de mayo de 2005

LIC. JOSE PABLO PATIÑO Y SOUZA.
DIRECTOR DEL SEMINARIO DE DERECHO PENAL

JPPYS/*lpg.

A Dios por estar cerca de mí, por escucharme,
por enseñarme que la vida siempre tiene un sonrisa
para los momentos más difíciles.

A mi madre por darme la vida, por su cariño,
comprensión apoyo y sobre todo por su inmenso amor.

A mi padre por su esfuerzo, por su apoyo incondicional
en mi educación y en cada etapa de mi vida.

A mis hijos Erick Yael y Alexis por ser la más bella
razón de mi existir, por la dicha de tenerlos a mi lado y
a quienes siempre tengo presentes en mi mente y corazón.

A mi hermana Rocio por cada palabra de aliento, por su cariño y
por estar cerca de mi cada vez que la necesito.

A mi hermano Daniel por los momentos en que ha estado a mi lado,
por su gran corazón, por su sensibilidad para comprenderme y
por su capacidad para disfrutar lo hermoso de la vida

A mi esposo Francisco por estar a mi lado, por ser mi mejor amigo,
por sus consejos , por su ternura, por ser mi compañero con él que he recorrido
y quiero recorrer todo el camino de mi vida.

A Angelina por su sinceridad, sencillez, buen humor, por ser una
persona muy especial, y en quien encontré un gran apoyo .

A mi asesor por su comprensión, por sus consejos
sin los cuales no hubiera podido llegar a la culminación de este trabajo.

Al Lic. José Francisco Morales Ríos por su paciencia
por su tiempo y por sus conocimientos
compartidos en la elaboración de este trabajo.

A todos mis amigos por su compañía y por sus consejos.

Y a todas esas personas que de alguna manera me han ayudado
en la terminación de mi carrera profesional.

A todos Gracias.

"MODIFICACIÓN DEL ARTÍCULO 211 BIS 1 PARTE PRIMERA DEL CÓDIGO PENAL FEDERAL POR RELACIONARSE CON EL DELITO DE DAÑO EN PROPIEDAD AJENA"

ÍNDICE

INTRODUCCIÓN

La tesis que a continuación se presenta tiene como uno de sus objetivos el hacer el estudio de un delito innovador, ya que la humanidad ha evolucionado en varios de sus factores tales como culturales, sociales, jurídicos, y siendo este último el que nos ocupa pues necesario tener una norma que regule la conducta antijurídica de las personas que utilizan medios informativos en su actuar ya sea laboral, particular o cualquier otro medio en el que se desenvuelve, por ello el Estado debe garantizar el derecho que tiene la persona a su tranquilidad desde el punto de vista normativo para mantener un equilibrio del hombre moderno frente a los posibles atentados en la utilización de la informática, tales como los daños que puede sufrir la información o a los sistemas de informática.

Con la creación del tipo penal de Acceso Ilícito a Sistemas de Informática se trata de regular la conducta antijurídica sobre el manejo de los sistemas de informática, dándosele un enfoque autónomo, pero como veremos durante el desarrollo de esta tesis su naturaleza es propiamente de un delito de daño en propiedad ajena pero con una nueva modalidad, necesaria para el mundo informático en el que vivimos, pues éste esta en constante cambio.

Con la incursión de este tipo penal contenido en el articulo 211- bis 1 párrafo primero del Código Penal Federal se pretende dar una protección a todos aquellos propietarios y usuarios de los sistemas de computo, pues como se ha visto existen no solo en México sino en todo el mundo entero, sujetos que están íntimamente ligados a la informática, capaces de destruir, modificar o provocar la perdida de información e incluso utilizar la información contenida en los sistemas informáticos para beneficio propio, ejemplo de ello es la transacción de cuentas bancarias, la utilización de bancos de datos de una empresa o entidad estatal, destruir sistemas de computo ya sea de un particular o de alguna entidad del gobierno o empresa privada.

En el presente trabajo se hace un estudio jurídico comparativo, para lo cual es necesario, y con fines didácticos, describir las características del delito de Acceso Ilícito a Sistemas de Computo contenido en el articulo 211-bis, párrafo primero, posteriormente la descripción del delito de daño en propiedad ajena para así concluir con el estudio jurídico comparativo en donde señalaremos las semejanzas y diferencias de ambos delitos.

Para poder lograr el objetivo del presente trabajo de investigación se ha utilizado diferentes métodos y técnicas para recabar, estudiar, analizar, comparar y ordenar la información contenida en esta Tesis, teniendo la necesidad de auxiliarnos de otras ciencias y materias diferentes a la jurídica como la teleológica, lingüística, informática, entre otras siendo una tesis multidisciplinaria.

Iniciamos esta investigación siguiendo un orden esquemático empezando con los antecedentes históricos pues éstos son necesarios en esta investigación en virtud de que se debe tener una noción de la evolución de la humanidad así como de las conductas ilícitas y como se origino en otros países hasta presentarse en el nuestro, ya que con el INTERNET todos los países o la gran mayoría de ellos están comunicados entre si y es mas fácil poder entrar a los diferentes sistemas particulares o gubernamentales, todos los sujetos que operen un computadora y que tengan conocimientos suficientes para acceder a aquellas pues esto facilita que accedan a los sistemas de computo para modificar, destruir o provocar la perdida de sistemas informáticos.

CAPÍTULO 1 GENERALIDADES DE LA INFORMÁTICA

1.1. HISTORIA DE LA INFORMÁTICA

La informática como ciencia y tecnología es muy joven por ello debemos de conocer como ha evolucionando a través del tiempo, ya que en la actualidad el hombre utiliza la informática en varios aspectos de su vida como lo es en lo social, educativo, tecnológico, entre otros, siendo una disciplina muy practica para las labores del hombre. Para conocer mas de ella debemos de saber como surgió y como ha ido progresando hasta nuestros días.

El concepto historia proviene del "latín historiam; griego historia, búsqueda; derecho de hister, sabio, estudio de los acontecimientos del pasado relativo al hombre y las sociedades humanas. Relato de suceso del pasado, especialmente cuando se trata de una narración ordenada cronológicamente y verificada con los métodos de la crítica histórica."[1]

Como puede observarse la historia tiene un orden conforme fueron sucediendo los hechos en el mundo, por lo que empezaremos a analizar lo que es la historia de la informática desde su inicio hasta la actualidad.

Desde tiempos muy remotos el hombre tuvo que buscar la forma de sobrevivir ante los acontecimientos de la naturaleza, es decir, la forma en como iba alimentarse, a vestirse, es por ello que poco a poco trato de mejorar su calidad de vida, teniendo la necesidad de cuantificar sus pertenencias, y de registrar ciertos hechos comenzando a buscar algunos procedimientos que le simplificaran el desarrollo de operaciones complejas. En un principio utilizaba sus dedos, posteriormente encontró otros medios para dicha tarea como palos, granos, piedras, etcétera, hasta llegar a inventar la computadora y con su invención trae una nueva ciencia la informática, este término fue "creado en Francia aproximadamente en 1695 con el objeto de designar las ciencias y técnicas de la comunicación que intervienen en la recopilación y utilización de datos a fin de

[1] Gran Enciclopedia Larousse Tomo 12, Ed. Planeta, España 1993, 1° edición pp 5467.

elaborar decisiones".[2] La palabra informática esta compuesta por dos términos "información y automática, y hace referencia al conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático y racional por medio de ordenadores"[3], es decir, es aquella disciplina que tiene relación a la manipulación de la información a través de un una computadora, también conocida como ordenador.

La primera herramienta construida por el hombre que le ayudaban a cuantificar fue el ábaco, instrumento que utilizó para realizar operaciones matemáticas, la cual "se originó entre 600 y 500 a.C., en China o Egipto".[4] Sin embargo Gonzalo Ferreyra Cortés señala que el ábaco fue creado en "Babilonia o tal vez en China".[5]

Toda vez que con el ábaco era difícil dividir y multiplicar Jonh Napier inventó en "1617 una máquina de contar para resolver problemas de multiplicación usando funciones logarítmicas".[6] Posteriormente en "1642 Blas Pascal diseñó una máquina de calcular basada en ruedas dentadas que sumaba y restaba".[7]

Gonzalo Ferreyra Cortés señala que: en 1673, el matemático alemán Gottfried von Leibnitz trato de mejorar la máquina de Pascal sin éxito, por lo que decidió diseñar una calculadora mecánica propia. Esta ya permitía multiplicar, dividir y extraer raíz cuadrada mediante sumas y restas sucesivas, usando una serie de cilindros con dientes graduados".[8]

Julio Téllez Valdez señala que "Joseph Marie Jacquard en 1804, construyó una máquina para tejer complicados diseños de telas, la cual funcionaba con

---

[2] M. FALCÓN, ENRIQUE, ¿QUÉ ES LA INFORMÁTICA JURÍDICA? Ed. Abeledo Perrot, Buenos Aires 1992, primera edición, pp. 11

[3] UREÑA LOPEZ, L. ALFONSO, "FUNDAMENTOS DE LA INFORMÁTICA", Ed, Alfaomega, México 1999, primera edición, pp 2.

[4] http://www.monografias.com/trabajos/marcohistocomp/marcohistocomp.shtml

[5] FERREYRA CORTÉS, GONZALO, "INFORMATICA, PASO A PASO", Ed. Alfaomega, México 2000, primera edición, pp 21.

[6] http//:www.coqui.metro.inter.edu

[7] M. FALCÓN, ENRIQUE; pp. 26.

[8] FERREYRA CORTÉS, GONZALO, pp 23.

"tarjetas perforadas que contenían información del camino que debían seguir los hilos de la tela para lograr un diseño determinado".[9]

Después del invento de la tarjeta perforada, Herman Hollerit se dio cuenta de las grandes posibilidades que tenían dichas tarjetas en el procesamiento de datos y en los cálculos matemáticos, por lo que al ser "agente del censo de los Estados Unidos de América, aplico el criterio a una cinta perforada para realizar el censo de dicha nación correspondiente a 1890".[10]

"En Inglaterra, Charles Babbage profesor de matemáticas de la Universidad de Cambridge, trabajaba hacia 1822 en un proyecto financiado por la Royal Society al cual llamó la "máquina diferencial", con la intención de producir tablas logarítmicas de hasta 6 cifras. La máquina nunca fue terminada debido a que, mientras avanzaba en la construcción, constantemente se le ocurrían mejoras par perfeccionar el aparato".[11]

Posteriormente Herman Hollerit en la universidad de Harvard, en la empresa IBM, llevo a cabo "en 1937 una gigantesca calculadora llamada Mark I, por Howard Aiken".[12]

No paso mucho tiempo cuando fue inventado el "ENIAC (Integrado Electrónico Numérico y Calculadora) constuido por J. Presper Eckert hijo y John Mauchly"[13], por su parte Enrique M. Falcón señala que dicha máquina fue creada además por "Eckert, Mauchly y Goldstine en 1946".[14]

A partir de la década de los cincuenta, las computadoras han sido clasificadas por generaciones, éste término "se refiere a la moderna tecnología y a los componentes con la que se construían y se siguen construyendo computadoras"[15].

---

[9] TÉLLEZ VALDEZ, JULIO, "DERECHO INFORMÁTICO", Ed. Universidad Nacional Autónoma de México; México 1987, primera edición, pp. 13
[10] M. FALCÓN, ENRIQUE; pp. 26.
[11] FERREYRA CORTÉS, GONZALO; "INFORMÁTICA, CURSOS PARA BACHILLERATO", Ed. Alfaomega, México 2000, primera edición pp. 25.
[12] M. FALCÓN, ENRIQUE; pp. 26.
[13] http://www. monogrfias.com/tabajos/marcohistocomp/marcohistocomp.shtml
[14] M. FALCÓN, ENRIQUE; pp. 26
[15] Idem

Las generaciones duran hasta que se produce un nuevo cambio, los autores manejan diferentes generaciones, algunos manejan cuatro, otros cinco y en particular Gonzalo Ferreyra Cortés maneja hasta seis generaciones y no todos concuerdan en las fechas en que comienzan y terminan cada una de ellas.

1.1.1. PRIMERA GENERACIÓN

"La primera generación la constituyen las computadoras que se construyeron en los años 1950 y 1959"[16]. A ésta generación le corresponde las máquinas que funcionaban a través de la "válvula de vado (dispositivo electrónico formado por dos electrodos encerrados en una ampolla en la que se ha practicado el vacío). Estas máquinas se programaban directamente en lenguaje máquina y eran capaces de realizar hasta 1.000 instrucciones por segundo; disponían asimismo de una capacidad de memoria que podía llegar hasta las 20.000 posiciones"[17]. Por otra parte el autor Enrique M. Falcón menciona que ésta generación abarca de "1950 a 1959"[18].

1.1.2. SEGUNDA GENERACIÓN

El periodo de esta generación la abarca de "(1959-1964). Aquí aparece la aplicación del transistor, los sistemas operativos, los lenguajes de alto nivel y los discos magnéticos"[19] La ventaja de éstas computadoras con la aparición del transistor es que se hicieron "más rápidas, más pequeñas y con menos necesidades de ventilación eran sustancialmente más pequeñas y rápidas que las de bulbos"[20].

---

[16] http://www.cyberlatino.com.mx/info/pc/main.htm#COMPUTADORA
[17] Idem
[18] M. FALCÓN, ENRIQUE; pp. 27.
[19] Idem; pp. 28.
[20] http://www.monografias.com/trabajos/refercomp/refercomp.shtml

1.1.3. TERCERA GENERACIÓN

Enrique M. Falcón manifiesta. que esta generación comprende de "1964-1975 la marca la aparición de los circuitos integrados"[21].

Por su parte Gonzalo Ferreyra Cortés menciona como las principales características de ésta generación las siguientes:

- "Se sigue utilizando la memoria de núcleos magnéticos.
- Los tiempos de operación son del orden de nanosegundos
- Aparece el disco magnético
- Compatibilidad de información para diferentes tipos de computadoras" [22].

1.1.4. CUARTA GENERACIÓN

Comienza un avance tecnológico con mayor rapidez surgiendo una gran cantidad de fabricantes de micro computadoras o también llamadas personales.

"Inicia en 1971 con la aparición del microprocesador o chip de 4 bits los cuales con dispositivos del estado sólido que efectúan las funciones de acceso operación y mando del computador"[23].

1.1.5. QUINTA GENERACIÓN

Esta generación, se ubican entre los años 80's a partir de la "creación de la primera supercomputadora con capacidad de proceso paralelo,las computadoras de esta generación pueden reconocer voz e imágenes. También tienen la capacidad de comunicarse con un lenguaje natural, el almacenamiento de información se realiza en dispositivos que pueden almacenar decenas de Gigabytes; se establece el DVD (Digital Video Disk O Digital Versatile Disk) como estándar para el almacenamiento de video y sonido"[24].

---

[21] M. FALCÓN, ENRIQUE; pp. 28
[22] FERREYRA CORTÉS; GONZALO, pp. 35.
[23] ARECHIGA GALLEGOS, RAFAEL, "INTRODUCCIÓN A LA INFORMATICA" Ed Limusa, México 1990, Séptima Reimpresión pp. 19.
[24] http://www.cyberlatino.com.mx/info/pc/main.htm#COMPUTADORA

1.1.6. SEXTA GENERACIÓN

Gonzalo Ferreyra Cortés, señala que nos encontramos en la sexta generación de las computadoras caracterizándose dichas computadoras "por realizar más de un millón de millones de operaciones aritméticas por segundo"[25].

1.2 PARTES INTEGRALES DE UNA COMPUTADORA

Como se puede observar la informática ha evolucionado y ha cambiado la vida del hombre, ya que es una disciplina que manipula la información a través de una computadora. La computadora es: "una máquina compuesta de elementos físicos en su mayoría de origen electrónico capaz de aceptar unos datos de entrada, realizar con ellos operaciones lógicas y aritméticas con gran velocidad y precisión, y proporcionar los resultados a través de algún medio de salida; todo ello es llevado a cabo sin la intervención de un operador humano y bajo el control de un programa de instrucciones previamente almacenado en la propia computadora"[26]. La computadora es el instrumento que utiliza el hombre y por medio del cual se ha facilitado diferentes tareas desde un trabajo escolar hasta llegar al funcionamiento de una empresa obteniendo la información necesaria para dicho funcionamiento y poder recuperar dicha información en un tiempo determinado. Motivo por el cual a continuación estudiaremos las partes que forman una computadora.

1.2.1. HARDWARE

"La palabra hardware está compuesta por dos palabras de origen anglosajón hard (duro) y ware (mercadería) "[27], es decir, es la parte física de una computadora dividiéndose comúnmente por tres categorías principales: entrada, salida y almacenamiento.

---

[25] GONZALO FERREYRA, CORTÉS; pp. 40
[26] UREÑA LOPEZ, L. ALFONSO, Op. Cit pp 2
[27] M. FALCÓN, ENRIQUE Op cit pp.35.

Los componentes de dichas categorías están conectados a través de un conjunto de cables o circuitos a los que se les denomina comúnmente bus, los bus se conectan con la unidad central de proceso (CPU) del ordenador. Para que el hardware funcione necesita de conexiones materiales que permitan a los componentes comunicarse entre sí e interaccionar. Un bus constituye un sistema común interconectado, compuesto por un grupo de cables o circuitos que coordina y transporta información entre las partes internas de la computadora. Un bus tiene dos propiedades una es la cantidad de información que puede manipular simultáneamente y la otra es la rapidez con que puede transferir dichos datos"[28].

Los buses se interconectan entre las distintas unidades de un ordenador y son: bus de datos, bus de direcciones y bus de control.

El bus de datos, este trasporta los datos que se transfieren entre unidades, es decir los mismos hilos se utilizan para transmitir información hacia adentro o hacia fuera de una unidad, pero siempre en instantes diferentes. Dentro del bus de datos esta el interno y el externo, el primero transfiere datos entre los elementos de la computadora central, es decir entre la unidad central de procesamiento y la memoria principal, por su parte el bus de datos externo pone en comunicación el procesador con las unidades de entrada y de salida.

El bus de direcciones: transporta la dirección de la posición de memoria o del periférico que interviene en el tráfico de información, es decir permite la comunicación entre el procesador y las celdas de la memoria RAM.

Por último del bus de control contiene hilos que transportan las señales de control y las señales de estado, indicando la dirección de la transferencia de datos.

1.2.2. ENCENDIDO DE LA COMPUTADORA

La computadora es un aparato inerte, por lo que necesita una orden para poder realizar su tarea, motivo por el cual el hardware a través del "RESET (puesta a nivel lógico CERO o inicialización). Los dispositivos internos esperan que

[28] Telecomunicación, Enciclopedia Microsoft Encarta 2004. © 1993-2004 Microsoft Corporation.

la señal de RESET ponga en nivel lógico de cero a uno, a partir del cual comienzan las tareas, las que llevan a fijar un resultado binario determinado"[29].

Es necesario destacar que la información contenida dentro de una computadora es representada por el código binario, es decir, esta representada por 0 y 1, el 0 para la máquina quiere decir apagada, no pasa corriente eléctrica o luz, por lo contrario el 1 significa encendido, pasa corriente eléctrica o luz.. La información que proviene del exterior debe ser transformada a este código para que pueda ser procesada por la computadora y la información resultante del procesamiento debe transformarse a otros códigos que puedan ser entendidos por los usuarios.

Cada 0 y 1 es lo que conocemos como un bit.

"Un byte es el número de bits necesarios para almacenar un carácter (generalmente son 8bits, por lo que se habla también de octeto). Al igual que ocurre con otras unidades, es muy usual utilizar múltiplos de byte:

1 Kilobyte (1KB) = 2_{10} byte= 1.024

1 Megabyte (1MB) = 1.024 KB

1 Gigabyte (1GB) = 1.024 MB

1 Terabyte (1TB) = 1.024 GB

1 Petabyte (1PB) = 1.024 TB"[30]

1.2.2.1. DISPOSITIVOS DE ENTRADA

Son dispositivos físicos a través de los cuales se introduce datos a una computadora, las unidades de entrada transforman los datos introducidos en códigos binarios que pueden ser entendidos y procesados por la computadora, estos dispositivos pueden ser:

a) Lápiz óptico es un puntero con un extremo fotosensible que se emplea para dibujar directamente sobre la pantalla, o para seleccionar información en la

[29] M. FALCÓN, Enrique Op. Cit p.48 y 49
[30] UREÑA LOPEZ, L. ALFONSO, Op. Cit pp 5

pantalla pulsando un botón en el lápiz óptico o presionando el lápiz contra la superficie de la pantalla.

b) Mouse, o ratón, es un dispositivo apuntador diseñado para ser agarrado con una mano. Cuenta en su parte inferior con un dispositivo detector generalmente es una bola que permite al usuario controlar el movimiento de un cursor en la pantalla deslizando el mouse por una superficie plana. Para seleccionar objetos o elegir instrucciones en la pantalla, el usuario pulsa un botón del mouse. También cuenta generalmente con dos botones, estos botones permiten simular que se oprime la tecla. De esta manera, si en la pantalla se está preguntando que acción seguir y se dispone de un ratón, se podrá ubicar el apuntador o puntero, casi siempre representado por una flecha, sobre la opción deseada y a continuación, oprimir cualquiera de sus botones.

c) Joystick es un dispositivo formado por una palanca que se mueve en varias direcciones y dirige un cursor u otro objeto gráfico por la pantalla de la computadora;

d) Teclado es un dispositivo parecido a una máquina de escribir, que permite al usuario introducir textos e instrucciones.

e) Digitalizador óptico es un dispositivo que puede convertir imágenes por ejemplo, una fotografía o un texto en señales electrónicas que puedan ser manipuladas por la máquina. Por ejemplo, es posible digitalizar una fotografía, introducirla en una computadora e integrarla en un documento de texto creado en dicha computadora.

f) Micrófono es un dispositivo para convertir sonidos en señales que puedan ser almacenadas, manipuladas y reproducidas por el ordenador

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

h) Scanner su función consiste en rastrear una imagen para que sea introducida en la computadora y poder modificarla.

i) Cámara digital. es un dispositivo de entrada de alta precisión utilizando como herramienta el diseño.

j) Módem es un dispositivo que conecta una computadora con una línea telefónica y permite intercambiar información con otro ordenador a través de dicha línea. Todos los ordenadores que envían o reciben información deben estar conectados a un módem.

1.2.2.2. DISPOSITIVOS DE SALIDA

Son dispositivos que muestran los resultados emitidos por la computadora; es decir; a través de los dispositivos de salida la información generada por la computadora es transferida al usuario.

Entre estos dispositivos están:

a) La pantalla, a través de la cual la información generada por el ordenador se convierte en información visual.

Las pantallas suelen adoptar una de las siguientes formas: un monitor de rayos catódicos o una pantalla de cristal líquido. Los primeros son semejantes a un televisor, la información procedente de la CPU se representa empleando un haz de electrones que barre una superficie fosforescente que emite luz y genera imágenes. En cambio las pantallas de cristal liquido son más planas y más pequeñas que los monitores de rayos catódicos, y se emplean frecuentemente en ordenadores portátiles.

b) Las impresoras reciben textos e imágenes de la computadora y los imprimen en papel. Dentro de las cuales podemos mencionar las impresoras matriciales que emplean minúsculos alambres que golpean una cinta entintada formando caracteres. Las impresoras de chorro de tinta lanzan

gotitas de tinta sobre el papel para formar caracteres e imágenes. Las impresoras láser emplean haces de luz para trazar imágenes en un tambor que posteriormente recoge pequeñas partículas de un pigmento negro denominado tóner. El tóner se aplica sobre la hoja de papel para producir una imagen"[31].

c) Los discos flexibles

d) Los CD-ROM

En la actualidad algunos dispositivos pueden ser de entrada y de salida, entre estos están el modem, los discos flexibles.

También entre los dispositivos de entrada y de salida se encuentran: la pantalla sensible al tacto, las terminales de punto de venta y las terminales de operaciones financieras.

La pantalla sensible al tacto en la que se incluye un dispositivo capaz de reconocer la zona donde se aplica un presión, ejemplo de esto es el contacto con el dedo. Se utiliza para representar información realizando operaciones mediante un grupo de opciones las cuales se localizan a lo largo de la pantalla, de forma que una de ellas puede ser reconocida por el contacto. Estas pantallas se pueden localizar en lugares públicos para suministrar información de cualquier índole como son precios de artículos, horarios de transportes.

Las terminales de punto de venta son unidades de tipo comercial, las cuales constan de un teclado, una impresora y una caja de monedas y billetes controlada por el teclado.

Las terminales de operaciones financleras también denominados cajeros automáticos, son unidades conectadas a una computadora central de una entidad financiera para la realización de operaciones de los clientes con la mencionada entidad

[31] "Computadora" Enciclopedia Microsoft Encarta 2004. © 1993-2004 Microsoft Corporation

1.2.3. CPU

La unidad central de proceso o UCP, conocida en inglés por sus siglas CPU, "es un circuito microscópico que interpreta y ejecuta instrucciones, la cual se ocupa del control y el proceso de datos en las computadoras".[32] Podemos decir que es el verdadero cerebro de la computadora, es quien controla y coordina todas las operaciones del sistema. Para que pueda realizar su función poco a poco va ejecutando una por una de las instrucciones del programa ubicado en memoria principal, las analiza y emite las órdenes para su completa realización.

Físicamente está formada por circuitos electrónicos los cuales se encuentran integrados en un chip denominado procesador.

La unidad de procesamiento central está formado por una unidad aritmético-lógica y por la unidad de control.

La unidad aritmético-lógica es la encargada de realizar cálculos y comparaciones, y toma decisiones lógicas, es decir, determina si una afirmación es cierta o falsa, mediante las reglas del álgebra de Boole; por una serie de registros donde se almacena información temporalmente, y la una unidad de control que interpreta y ejecuta las instrucciones. Para aceptar órdenes del usuario, acceder a los datos y presentar los resultados.

Al ejecutarse un programa, el registro de la CPU, denominado contador de programa, lleva la cuenta de la instrucción posterior, garantizando que las instrucciones se lleven a cabo en la secuencia adecuada. La unidad de control de la CPU coordina y administra las funciones de la CPU, recuperando la siguiente instrucción desde la memoria. En una secuencia propia, la CPU localiza la instrucción en el dispositivo de almacenamiento correspondiente. Posteriormente, la CPU ejecuta la instrucción, y los resultados se almacenan en otro registro o se copian en una dirección de memoria determinada.

[32] "CPU" Enciclopedia Microsoft Encarta 2004. © 1993-2004 Microsoft Corporation

1.2.4. MEMORIAS

"La memoria es todo dispositivo electrónico que puede almacenar información y programas que el ordenador deba recuperar en algún momento, se dividen en dos: a) la memoria principal, central o primaria y b) la memoria auxiliar, periférica o secundaria"[33].

1.2.4.1. CENTRALES

Esta memoria actúa a mayor velocidad ya que esta ligada directamente a las unidades más rápidas de la computara. Para que un programa pueda ser utilizado debe estar almacenado en la memoria central.

La memora central esta formada por "multitud de celdas o posiciones (palabras de memoria) de un determinado número de bits y numeradas de forma consecutiva. A la numeración de las celdas se le denomina dirección de memoria mediante esta dirección se puede acceder de forma directa a cualquiera de ellas, independientemente de su posición; por ello se dice que la memoria principal es una memoria de acceso directo o memoria accesible por dirección".[34]

Este tipo de memoria esta dividida en:

a) Las memoria ROM "(Read Only Memory- Memoria de sólo lectura)" [35]es aquella en la que sólo se permite leer y es permanente, es decir al apagar la computadora la información no se pierde, ya que contiene información y software indispensable que debe estar disponible para el funcionamiento de la computadora.

Las variantes de la memoria ROM es la memoria PROM y la EPROM, la memoria PROM es la memoria programable de solo lectura en virtud de que una vez que esta memoria ha sido programada los datos permanecen fijos y no

---

[33] M. FALCON, ENRIQUE, Op. Cit pp 46
[34] UREÑA LOPEZ, L. ALFONSO, Op. Cit pp 41
[35] Idem pp 41

pueden reprogramarse, en cambio la memoria programable de solo lectura la EPROM puede borrarse.

b) La memoria RAM "(Random Access Memory- Memoria de acceso aleatorio)"[36] es la memoria viva o volátil, se denomina así por que la información contenida en ésta se pierde cuando se desconecta el ordenador, permite leer y escribir información de modo indistinto.

1.2.4.1. AUXILIARES

La información obtenida por la memoria RAM puede ser almacenada permanentemente de tal forma que puede ser recuperada automática y eficientemente en unidades de disco, como son:

a) discos duros son parte permanente de la computadora pueden almacenar grandes cantidades de información y recuperarla rápidamente;

b) discos flexibles también almacena información y son de 5 1/2 pulgadas o de 3.5 pulgadas; la lectura y grabación se efectúa introduciendo el disquete en una unidad de disco de su mismo tipo.

c) discos magneto-óptico almacena información como un disco duro pero la velocidad para recuperarla es menor y

d) discos compactos o CD-ROM, también guarda información solo que la desventaja de este tipo de disco es que no se puede borrar la información ni sustituirse por otra.

1.2.5. SOFTWARE

"La palabra software significa partes blandas, siendo lo contrario de la palabra hardware que son las partes duras. Por lo que el software son las instrucciones necesarias para que el hardware realice sus funciones, es decir, son los programas cargados en el ordenador para que éste funcione". [37]

---

[36] Idem pp 42

[37] "SOFTWARE " Enciclopedia Microsoft Encarta 2004. © 1993-2004 Microsoft Corporation

El software se puede dividir según el tipo de trabajo que realice en distintas categorías. Las dos categorías primarias de software son: "los sistemas operativos (software del sistema o de base), es el software incorporado al ROM que controlan los trabajos del ordenador o computadora, y el software de aplicación, que dirige las distintas tareas para las que se utilizan las computadoras. Por lo tanto, el software del sistema procesa tareas tan esenciales, aunque a menudo invisibles, como el mantenimiento de los archivos del disco y la administración de la pantalla, mientras que el software de aplicación lleva a cabo tareas de tratamiento de textos, gestión de bases de datos y similares. Constituyen dos categorías separadas el software de red, que permite comunicarse a grupos de usuarios, y el software de lenguaje utilizado para escribir programas".[38]

Dentro del software de aplicación esta el software estándar o herramientas informáticas y el software a medida.

"El software estándar o herramientas informáticas hacen referencia a aquellas aplicaciones de uso general especialmente diseñadas para su lanzamiento al mercado. Estas aplicaciones pueden ser utilizadas por gran número de usuarios y sobre diferentes sistemas. Algunas de estas aplicaciones de uso común son el tratamiento de textos, las hojas de cálculo, comunicaciones, gráficos, etc. El software a medida está constituido por aquellas aplicaciones específicas que se refieren a actividades más especializadas. En este caso, una aplicación de este tipo es desarrollada para un/unos usuario/s concreto/s y para un sistema específico"[39].

Además de estas categorías basadas en tareas, existen varios tipos de software los cuales se basan en su distribución. Entre estos se encuentra, el software desarrollado por compañías y vendido principalmente por distribuidores, el cual se le denomina freeware o dominio público, este tipo de software se ofrecen sin costo alguno y se ofrece a menudo en boletines electrónicos a través de grupos de usuarios. Los programadores independientes pueden ofrecer sus productos como freeware, ya sea por satisfacción personal o para asegurarse de

[38] Idem
[39] UREÑA LOPEZ, L. ALFONSO, Op. Cit pp 81

que llega a los usuarios interesados. Los programadores de freeware conservan a menudo todos los derechos sobre su software. Los usuarios no siempre tienen libertad para copiar o redistribuir el producto. Por otro lado, encontramos el shareware, este software es parecido al freeware, sin embargo conlleva una pequeña tasa a pagar por los usuarios que lo utilizan profesionalmente y por último encontramos el software denominado vapourware, es el que no llega a presentarse o aparece mucho después de lo prometido.

Por otro lado existen los software de esparcimiento e instrucción. Este tipo de software esta constituido especialmente por los juegos electrónicos y los sistemas de enseñanza electrónicos, entre los cuales se encuentran los de enseñanza de la computadora.

1.2.6. PROGRAMAS

"El programa informático es conjunto de ordenes o instrucciones que se le dan a una computadora para realizar un proceso determinado. Las ordenes que integran un programa indican a la computadora las tareas que han de ser realizadas par llevar a cabo el proceso requerido".[40]

Un programa es una secuencia de instrucciones que indican al hardware del 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.

Programa de aplicación es el programa informático diseñado para facilitar al usuario la realización de un determinado tipo de trabajo. Posee ciertas características que le diferencia de un sistema operativo (que hace funcionar al ordenador), de una utilidad (que realiza tareas de mantenimiento o de uso general) y de un lenguaje (con el cual se crean los programas informáticos). Suele

---

[40]" UREÑA LOPEZ, L. ALFONSO, Op. Cit pp 2

resultar una solución informática para la automatización de ciertas tareas complicadas como puede ser la contabilidad o la gestión de un almacén.

1.2.7. SISTEMA

En informática la palabra sistema es: "cualquier conjunto de dispositivos que colaboran en la realización de una tarea. En informática, la palabra sistema se utiliza en varios contextos. Una computadora es el sistema formado por su hardware y su sistema operativo. Sistema se refiere también a cualquier colección o combinación de programas, procedimientos, datos y equipamiento utilizado en el procesamiento de información: un sistema de contabilidad, un sistema de facturación y un sistema de gestión de base de datos".[41]

El sistema operativo "es el software básico que controla una computadora. El sistema operativo tiene tres grandes funciones: coordina y manipula el hardware de la computadora, como la memoria, las impresoras, las unidades de disco, el teclado o el mouse; organiza los archivos en diversos dispositivos de almacenamiento, como discos flexibles, discos duros, discos compactos o cintas magnéticas, y gestiona los errores de hardware y la pérdida de datos".[42] Es decir el sistema operativo es el conjunto de programas y funciones que controlan y gestionan el funcionamiento del hardware, teniendo como objetivos principales: alcanzar un eficaz rendimiento de los recursos hardware y facilita al usuario un acceso flexible y sencillo a dichos recursos.

Los sistemas operativos controlan diferentes procesos de la computadora. Un proceso importante es la interpretación de los comandos que permiten al usuario comunicarse con el ordenador. Algunos intérpretes de instrucciones están basados en texto y exigen que las instrucciones sean tecleadas. Otros

---

[41]"Sistema (informática)," *Enciclopedia Microsoft® Encarta® 2004.* © 1993-2004 Microsoft Corporation. Reservados todos los derechos.

[42]"Sistema operativo," *Enciclopedia Microsoft® Encarta® 2004.* © 1993-2004 Microsoft Corporation. Reservados todos los derechos.

están basados en gráficos, y permiten al usuario comunicarse señalando y haciendo clic en un icono. Por lo general, los intérpretes basados en gráficos son más sencillos de utilizar.

Los sistemas operativos pueden ser de tarea única o multitarea. Los sistemas operativos de tarea única, sólo pueden manejar un proceso en cada momento. Por ejemplo, cuando la computadora está imprimiendo un documento, no puede iniciar otro proceso ni responder a nuevas instrucciones hasta que se termine la impresión.

Los sistemas operativos modernos son multitarea es decir pueden ejecutar varios procesos simultáneamente.

En la mayoría de los ordenadores sólo hay una unidad central de procesamiento; un sistema operativo multitarea crea la ilusión de que varios procesos se ejecutan simultáneamente en la unidad central de procesamiento. El mecanismo que se emplea más a menudo para lograr esta ilusión es la multitarea por segmentación de tiempos, en la que cada proceso se ejecuta individualmente durante un periodo de tiempo determinado. Si el proceso no finaliza en el tiempo asignado, se suspende y se ejecuta otro proceso. Este intercambio de procesos se denomina conmutación de contexto. El sistema operativo se encarga de controlar el estado de los procesos suspendidos. También cuenta con un mecanismo llamado planificador que determina el siguiente proceso que debe ejecutarse. El planificador ejecuta los procesos basándose en su prioridad para minimizar el retraso percibido por el usuario. Los procesos parecen efectuarse simultáneamente por la alta velocidad del cambio de contexto. Los sistemas operativos pueden emplear memoria virtual para ejecutar procesos que exigen más memoria principal de la realmente disponible. Con esta técnica se emplea espacio en el disco duro para simular la memoria adicional necesaria. Sin embargo, el acceso al disco duro requiere más tiempo que el acceso a la memoria principal, por lo que el funcionamiento del ordenador resulta más lento.

Los sistemas operativos empleados normalmente son UNIX, Macintosh OS, MS-DOS, OS/2 y Windows-NT. El UNIX y sus clones permiten múltiples tareas y múltiples usuarios. Su sistema de archivos proporciona un método sencillo de organizar archivos y permite la protección de archivos. Sin embargo, las instrucciones del UNIX no son intuitivas. Otros sistemas operativos multiusuario y multitarea son OS/2, desarrollado inicialmente por Microsoft Corporation e International Business Machines (IBM) y Windows-NT, desarrollado por Microsoft. El sistema operativo multitarea de las computadoras Apple se denomina Macintosh OS. El DOS y su sucesor, el MS-DOS, son sistemas operativos populares entre los usuarios de computadoras personales. Sólo permiten un usuario y una tarea.

Los sistemas operativos siguen evolucionando. Los sistemas operativos distribuidos están diseñados para su uso en un grupo de ordenadores conectados pero independientes que comparten recursos.

MS-DOS, "acrónimo de *Microsoft Disk Operating System* (sistema operativo de disco de Microsoft)".[43]

El sistema MS-DOS supervisa las operaciones de entrada y salida del disco y controla el adaptador de vídeo, el teclado y muchas funciones internas relacionadas con la ejecución de programas y el mantenimiento de archivos. El MS-DOS es un sistema operativo monotarea y monousuario con una interfaz de línea de comandos.

OS/2, "es un sistema operativo multitarea para ordenadores o computadoras personales. El OS/2 puede ejecutar aplicaciones para Windows y MS-DOS y leer discos de MS-DOS". [44]

---

[43] "MS-DOS," *Enciclopedia Microsoft® Encarta® 2004.* © 1993-2004 Microsoft Corporation.

[44]"OS/2," *Enciclopedia Microsoft® Encarta® 2004.* © 1993-2004 Microsoft Corporation. Reservados todos los derechos.

UNIX, es un sistema operativo multiusuario que incorpora multitarea. El sistema operativo UNIX tiene diversas variantes y se considera potente, más transportable e independiente de equipos concretos que otros sistemas operativos.

El UNIX está disponible en varias formas, entre las que se cuenta: "AIX, una versión de UNIX adaptada por IBM (para su uso en estaciones de trabajo basadas en RISC), A/UX (versión gráfica para equipos Apple Macintosh) y Mach (un sistema operativo reescrito, pero esencialmente compatible con UNIX, para las computadoras NeXT).[45]

Sistema operativo de disco o DOS, conocido como DOS (acrónimo de *Disk Operating System*), en sus orígenes el término diferenciaba entre los sistemas basados en disco y los sistemas operativos de los microordenadores más antiguos, basados en memoria o que sólo soportaban cinta magnética o de papel.[46]

1.2.8. LENGUAJE INFORMÁTICO

En informática también es llamado lenguaje de programación y es: "cualquier lenguaje artificial que puede utilizarse para definir una secuencia de instrucciones para su procesamiento por un ordenador o computadora".[47] Es decir es la traducción de las instrucciones a un código que comprende la computadora.

---

[45]"UNIX," *Enciclopedia Microsoft® Encarta® 2004.* © 1993-2004 Microsoft Corporation. Reservados todos los derechos.

[46]"Sistema operativo de disco," *Enciclopedia Microsoft® Encarta® 2004.* © 1993-2004 Microsoft Corporation. Reservados todos los derechos.

[47] "Lenguaje de programación," *Enciclopedia Microsoft® Encarta® 2004.* © 1993-2004 Microsoft Corporation. Reservados todos los derechos.

1.2.8.1. LENGUAJE EN CÓDIGO MÁQUINA

"Es el más cercano al lenguaje de la máquina, que se comunica con otros lenguajes o con intermediarios o traductores".[48] Ya que la manera en que el ser humano comprende el significado de alguna indicación que se le de, difiere de la forma en que la computadora lo puede entender, para poder activar la unidad de control, la memoria, los dispositivos de entrada y de salida se necesita un lenguaje especial, y el único lenguaje que el ordenador, entiende es el de ceros y unos, pues bien, todas las órdenes, acciones, etc., que el ordenador ejecuta, se realizan por las diferentes secuencias de ceros y unos que el ordenador puede entender. El lenguaje binario es el lenguaje máquina y a éste lenguaje se le denomina de bajo nivel.

1.2.8.2. LENGUAJE ENSAMBLADOR

Es un lenguaje intermedio entre el lenguaje máquina y el de alto nivel.

"En el lenguaje ensamblador existe un cierto nivel de simbolismos, es decir, donde una instrucción simboliza o abrevia un pequeño número de operaciones básicas, representaciones típicas son ADD (sumar), Sub (sustraer), Load (cargar), el programador debe escribir todas las instrucciones que tiene que realizar la computadora, pero se evita tener que describir todos los pasos imprescindibles para dar una orden, tal como sumar o restar, pues el lenguaje ensamblador se ocupa de hacerlo, bastando entonces con indicar el nombre del código (ADD, etc), y no hay que expresar una a una como el lenguaje máquina".[49]

1.2.8.3. LENGUAJE DE ALTO NIVEL

"Los lenguajes de alto nivel son normalmente fáciles de aprender porque están formados por elementos de lenguajes naturales, como el inglés".[50]

---

[48] M. FALCON, ENRIQUE. Op. Cit pp 75

[49] CLEMENTE DE BLAS, "GUÍA DEL USUARIOS", Ed, Ra-Ma, primera edición, Madrid España 1990. primera edición, pp 108

[50] "LENGUAJES" Enciclopedia Microsoft Encarta 2004. © 1993-2004 Microsoft Corporation

"Los lenguajes de alto nivel, contiene instrucciones directas y sencillas de interpretar y manejar por el usuario, operan como traductores entre el usuario y la máquina, de allí que los lenguajes suelan denominarse intérpretes. En rigor, lo que hacen es reducir a una única instrucción un conjunto de ellas. De este modo, al usuario le basta con decir sume o imprima, y el programa se ocupa luego de generar todas las instrucciones indispensables para que el computador cumpla aquel pedido".[51] Por ello es el lenguaje que actualmente se utiliza en todas las computadoras por ser el más fácil para el usuario. Ya que con este tipo de lenguaje se puede establecer una comunicación más sencilla entre el hombre y la máquina.

Las ventajas que ofrecen los lenguajes de alto nivel son las siguientes:

- Facilidad de comunicación, ya que es sencillo establecer comunicación entre el hombre y la máquina a la vez que las instrucciones son comprendidas por cualquier persona que tenga un poco de conocimiento de programación.
- Compatibilidad. Debido a convenios establecidos en el diseño de las máquinas, las indicaciones son comprendidas por diversos tipos de ordenadores. Por ejemplo existen ciertos dispositivos o programas que pueden ser utilizados en diferentes computadoras.
- Facilidad de entendimiento. Se puede contar con símbolos que utilizamos en la vida diaria y así poder realizar mas fácilmente el trabajo a desarrollar en la computadora.
- Rapidez de programación. Lo sencillo de los lenguajes, permite al programador desarrollar los programas con mayor rapidez en la codificación de las instrucciones.

Dentro de los lenguajes de alto nivel encontramos los siguientes:

---

[51] ANTONIO PRADO, PEDRO, "LA INFORMÁTICA Y EL ABOGADO", Ed. Abeledo-Perrot,, Buenos Aires, Argentina 1988, primera edición, pp 44.

1.2.8.3.1. C1 BASIC

"Beginner's All-purpose symbolic Instruction Code, (código de instrucciones simbólicas de propósito general para principiantes), es de usos masivos en los ordenadores personales".[52]

1.2.8.3.2. C2 FORTRAN

"Formula traslation (traducción de fórmulas)"[53] Diseñado para lenguaje matemático, tiene numerosas funciones en el área de las matemáticas.

1.2.8.3.3. C3 COBOL

"Common Business Oriented Languge (lenguaje orientado al tratamiento y uso común del comercio), para el tratamiento de cuestiones de gestión, ficheros y una enorme potencia para el tratamiento de datos".[54]

1.2.8.3.4. PL/1

"Programming Language que pretende reunir las virtudes del FORTRAN y del COBOL".[55]

1.2.8.3.5. ALGOL

"Algorithmic Language"[56] Ve sobre las cuestiones científicas.

1.2.8.3.6. PASCAL

Es el primer lenguaje inspirado en los principios de la programación estructurada moderna.

---

[52] M. FALCON, ENRIQUE. Op, cit. pp 76
[53] Idem
[54] Idem
[55] Idem
[56] Idem

1.2.8.3.7. PROLOG

"Programming in logic"[57], Fue creado para la aplicación de la inteligencia artificial.

1.2.8.3.8. LOGO

Es especialmente para los niños por ser apto para ellos.

Tomando en cuenta que una computadora solo entiende el lenguaje máquina, es necesario contar con programas que sean capaces de traducir el lenguaje de alto nivel al lenguaje máquina, existen dos tipos de traductores esto depende de cómo sea el proceso de traducción.

"Los compiladores traducen globalmente el programa inicial (programa fuente), obteniendo un programa semánticamente equivalente en lenguaje máquina (programa objeto) que será ejecutado después de la traducción. Los intérpretes analizan, traducen y ejecutan las instrucciones del programa fuente secuencialmente, de tal forma que la traducción y la ejecución del programa fuente se entrelazan en el tiempo. En este último caso, no se genera un programa objeto como salida, sino que los resultados de la ejecución del programa son generados directamente".[58]

1.2.10 ACCESO

La palabra acceso en informática significa "localizar, cargar en la memoria o preparar para su ejecución alguna operación. El término acceso se utiliza también para expresar el permiso que tiene un usuario en relación con discos, archivos, registros y procedimientos de entrada en una red". [59]

---

[57] Idem

[58] URENA LOPEZ, L. ALFONSO. Op. Cit pp 9

[59] "Acceso," *Enciclopedia Microsoft® Encarta® 2004.* © 1993-2004 Microsoft Corporation. Reservados todos los derechos.

El tiempo de acceso, en informática, es: "en general el tiempo que transcurre desde que se solicita cierta información de un origen remoto (de la memoria o del disco duro) hasta que estos datos están disponibles. En referencia a la administración de la memoria, el tiempo de acceso es el tiempo que le lleva a la memoria del sistema presentar la información en el microprocesador después de haberse elegido una dirección". [60]

En cuanto al almacenamiento en disco, es el tiempo necesario para que una unidad de disco responda a una solicitud de una operación de lectura o de escritura de datos. Por lo general, el tiempo de acceso se mide en milisegundos (milésimas de segundo) y cubre el intervalo desde el momento en que se emitió el comando de lectura/escritura hasta el momento en que se recibe la información que indica el éxito (o fracaso) de la operación. El tiempo de acceso se establece en los discos duros para indicar a qué velocidad funcionan. Esta información puede referirse al tiempo de acceso más corto posible, o bien al tiempo de acceso promedio. En la actualidad un tiempo de acceso inferior a los 10 milisegundos comienza a considerarse rápido. Por encima de ese tiempo se estima lento.

1.2.11 EQUIPO

Son "componentes mecánicos eléctricos magnéticos y electrónicos de una computadora o sistema de computo. Los componentes físicos de un sistema de cómputo de contrapartida con el software, que es intangible"

En informática se le denomina equipo en línea al "conjunto de dispositivos que realizan un proceso de datos, totalmente comentados bajo el control programado de un ordenador central"[61]

---

[60] "Tiempo de acceso," *Enciclopedia Microsoft® Encarta® 2004.* © 1993-2004 Microsoft Corporation. Reservados todos los derechos.

[61] "DICCCIONARIO ENCICLOPEDICO EPSASA", Tomo VIII, Ed. Espasa Calpe, Madrid, España 1992, segunda edición, pp 4507

1.3. PROGRESOS DE LA INFORMÁTICA EN LA ACTUALIDAD.

El uso de la tecnología no se ha restringido únicamente al campo de la actividad económica. Las computadoras se encuentran prácticamente en todas las áreas de gobierno, están presentes en los institutos científicos y empiezan a tomar un lugar importante en los hogares y actualmente una de las áreas de mayor crecimiento en la industria del software está en la producción de juegos para computadoras.

El uso de una computadora ha sido tan radical, que hoy sería impensable en el funcionamiento de la sociedad sin la tecnología de la información, ya que todas las actividades humanas involucran el uso de información extendiéndose al resto de la sociedad. Sin embargo si comparamos con los millones de seres humanos que existen en el planeta nos daríamos cuenta que es mínima la gente que utiliza una computadora ya sea por falta de recursos económicos o bien por ser gente adulta que no es capaz de poderse involucrar con un ordenador.

Actualmente el ser humano digitaliza su entorno, esto quiere decir que traduce información como textos, imágenes o sonidos, a un formato que puedan entender las computadoras, ya que éstas sólo entienden la información a través del código binario, es decir, a través de unos y ceros. Por medio de la digitalización, la sociedad transmite la información que manejan las computadoras.

Anteriormente si se quería consultar un libro se tenia que ir a la biblioteca, sin embargo hoy en día se puede consultar sin salir de casa, solo teniendo una computadora y un modem para poderse consultar por Internet.

En un futuro cercano, a través de la digitalización de programas de radio y televisión, se podrá tener acceso a los archivos de las televisoras y radiodifusoras en Internet con el fin de rentar algún programa de interés, sin importar si fue transmitido hace un mes o 10 años.

Una de las ventajas de la digitalización, es que se puede buscar datos específicos en volúmenes muy grandes de información: también permite procesar la información de una base de datos para ofrecer productos acordes a los interéses de cada uno de los clientes.

En Internet es mucho más rápido, barato y fácil publicar información que imprimirla en forma de libro: no hay necesidad de contar con una casa editorial, no es necesario hacer revisiones a las pruebas de impresión, no hay que comprar papel, solo basta con escribir el texto en un procesador de palabras, guardarlo en un formato de archivos compatible con Internet.

La digitalización tiene un gran impacto gracias a las redes. A través de éstas la información digitalizada se trasmite a muchas personas. Éstos son los cimientos sobre los que se construye el espacio virtual de la sociedad. Conformado por servidores, discos duros, cables, centrales telefónicas y un sin fin de aditamentos de alta tecnología destinados a dirigir y hacer eficiente la búsqueda y transmisión de datos. Las herramientas para construir este espacio, son las aplicaciones de software con las que se desarrollan las páginas para Internet.

A diferencia de los libros, en donde una vez impreso el contenido no hay forma de cambiarlo, la información digitalizada es versátil y gracias a los diferentes programas para explotarla, podemos interactuar con ella modificándola de infinitas maneras o emplearla como vehículo de comunicación e interacción con otros usuarios en la red.

En el espacio de las redes y en especial en la Internet, podemos transmitir archivos o comunicarnos con otras personas, empleando el correo electrónico, consultar información sobre empresas e instituciones visitando su sitio en Internet, o jugar solo o en grupo conectándonos a sitios de entretenimiento, sin importar las distancias físicas que nos separan, comprar un automóvil o gran variedad de cosas. De hecho, lo que hacemos en la red es en gran medida equivalente a lo que hacemos en el mundo real dentro de la sociedad. Lo que varía es el medio a través del cual lo hacemos.

Hoy cada día es más común que las empresas tengan computadoras para operar sus procesos; también es más cotidiano que en las ciudades las personas lleven una computadora portátil en su portafolio. Las cajas registradoras del supermercado se sustituyen por equipos más sofisticados que incluyen un lector

óptico y una terminal de computadora. Los manuales de organización y procedimiento, que antes se registraban en papel, ahora se tiene en bits.

Las cámaras digitales registran las imágenes y el audio en formato digital; también se observa que los empleados que surten de bebidas embotelladas a una tienda, en muchas ocasiones registran sus pedidos en un aparato informático de mano llamado hands hell.

Herramientas como el correo electrónico, los fotos en línea, los manejadores de base de datos, teléfonos portátiles, la transmisión digital de archivos o el servicio de acceso a los servidores de la empresa desde cualquier parte del mundo, son la base para que una empresa en red se desarrolle.

El uso del correo electrónico en algunas empresas ha permitido una reducción del papeleo y una comunicación directa entre las personas que ahí laboran. Por ejemplo anteriormente en una empresa, cuando un trabajador del departamento de gerencia quería ponerse en contacto con un trabajador del departamento de producción era necesario que la mecanógrafa tecleara un oficio, que éste fuera aprobado por el jefe de gerencia y enviado al departamento de producción, en donde la correspondencia era revisada por la secretaria del departamento de producción y turnada al destinatario final. Hoy, es el mismo trabajador del departamento de gerencia el que teclea un mensaje de correo electrónico en su computadora y lo manda al buzón electrónico del trabajador del departamento de producción quien lo recibe en pocos segundos. De esta forma, se han simplificado las estructuras de las organizaciones y han desaparecido algunos tipos de trabajo como el de mecanógrafa, archivista o mensajero. Sin embargo, al mismo tiempo han surgido puestos nuevos como los de capturista, soporte técnico y administración de redes.

Las grandes tiendas de autoservicio al momento en que se paga el producto adquirido el sistema lo descarga del inventario de la tienda y cuado se llega a un cierto nivel en las existencias del producto, el sistema genera un nuevo pedido al proveedor de manera automática. Como respuesta a ese pedido, en la entrega semanal de productos del fabricante a la sucursal de la tienda de autoservicio se

incluirá la restitución requerida del producto para mantener en el anaquel el volumen que se haya establecido. Es decir la manera de operar es la siguiente son empresas que tienen en el centro al fabricante del producto, rodeado de varias compañías que lo proveen de los materiales necesarios para su producción, por una parte, y de las empresas que venden los productos terminados al usuario final por la otra. Todas éstas enlazadas por sistemas de comunicación digital como el correo electrónico o las redes privadas. En el momento en que se vende un producto la información se envía del vendedor al fabricante, quien de inmediato pone las órdenes de compra de las partes necesarias a los proveedores para fabricar un nuevo producto que reemplace al producto vendido. Los proveedores producen las partes solicitadas y las entregan a la fábrica en el momento justo que se requieren en la línea de producción; una vez terminado, el nuevo producto es enviado a la empresa vendedora para que sea ofrecido al público.

Un elemento importante que ayuda en este proceso es el código de barras, el cual permite efectuar un control de las mercancías a lo largo de su venta, distribución y control de inventarios.

Por otra parte contar con medios electrónicos de acceso a la información tan potentes como los actuales, ha abierto la posibilidad para que los empleados puedan participar en los procesos de trabajo de manera más flexible, sin importar su ubicación o su horario. Por ejemplo, la gente puede laborar en su casa sin presentarse en la oficina; esto ha proliferado en muchos lugares del mundo y su auge no sería posible sin los avances tecnológicos registrados en los últimos años. Prácticamente cualquier persona podría trabajar desde cualquier punto de la ciudad, siempre y cuando cuente con una computadora, acceso a Internet y a la Intranet (es decir a la red local de la empresa donde labora), una impresora, el software apropiado, un fax y una línea telefónica.

El aprovechamiento de la información propicia el mejoramiento de los niveles de bienestar y permite aumentar la productividad y competitividad de las naciones. El aporte de la información se ha visto enriquecido por la posibilidad que ha traído

consigo la informática para producir información en grandes volúmenes, para consultarla y trasmitirla a una gran distancia.

La informática ha producido un importante cambio en la economía. Asimismo, la informática ha impulsado nuevos mecanismos de producción, así como el uso del tiempo y la forma de vida.

La informática prácticamente a afectado todas las actividades humanas, modificando las estructuras de producción y comercialización, la organización de instituciones, la generación de nuevas tecnologías y la difusión de conocimientos, así como la prestación de servicios.

Las consecuencias de la informática serán múltiples y algunas ya son claramente perceptibles. En el ámbito económico, en particular los avances tecnológicos han permitido reducir, en formar antes inimaginables, el tiempo requerido para producir bienes de toda índole. Así con el apoyo de la informática se han alcanzado niveles muy superiores de productividad y competitividad.

Los servicios que exigen un manejo masivo de información, como los del sector financiero, los seguros y el comercio, pueden prestarse en forma casi instantánea, aumentando su eficiencia, al poder enlazarse oficinas, clientes y proveedores en cualquier parte del mundo a través de redes de computadoras, también la informática ha hecho posible un mercado mundial capaz de reaccionar prácticamente al instante a los eventos que se suscitan en cualquier parte de nuestro planeta y que permite amplias transacciones de productos y servicios.

La informática esta modificando también a las organizaciones, se redefinen las responsabilidades de los directivos y de los trabajadores. Aparecen nuevos enfoques administrativos que buscan mejorar la productividad y la competitividad, como es la administración mediante la calidad total y la reingeniería, que para su exitosa aplicación se apoyan de manera fundamental en la tecnología informática.

En los ámbitos sociales y culturales, los efectos de la informática son muy importantes porque están cambiando las formas tradicionales de organización y comunicación, transformando las actividades y las condiciones de vida. El trabajo a distancia es ya una realidad en algunos países.

Con el apoyo de la informática, los gobiernos y las instituciones educativas están en posibilidades de mejorar sustancialmente los mecanismos tradicionales de gestión de servicio, lo cual se traduce en beneficios reales y tangibles para la población.

Los avances de la informática harán posible la transformación de los servicios para acercarnos a las necesidades particulares de las personas. Por ejemplo para los estudiantes y maestros estará disponible la información contenida en acervos anteriores fuera de su alcance; el médico podrá consultar información sobre la historia clínica de un paciente, sobre padecimientos y nuevos tratamientos, y aun comunicar e intercambiar información y opiniones con otros especialistas.

La informática, ha transformado la materia financiera actualmente se creo el sistema de tarjetas de crédito, el cual desarrollo el comercio tradicional, la transferencia electrónica de fondos, posteriormente se introducen los cajeros automáticos que actualmente han creado su propia red internacional de transferencia de dinero en efectivo.

La informática motivará ver fotografías en forma digital, y los videos. El escáner puede facilitar tener las fotos archivadas en la PC en forma digital y poderlas enviar a otras personas, incluso si se encuentran en otro país por medio del Internet.

Como se puede observar la informática esta modificando y modificara aún mas nuestra vida cotidiana, nuestra forma de ver el mundo y de relacionarnos con él.

CAPÍTULO 2 DELITOS INFORMÁTICOS

La informática esta hoy presente en casi todos los campos de la vida moderna permitiendo procesar y poner a disposición de la sociedad una gran cantidad de información de toda naturaleza, al alcance de millones de usuarios. Todas las esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporados a sistemas informáticos que, en la práctica cotidiana, entrega a quien lo desee, los datos que hasta hace unos años sólo podían ubicarse después de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, esa gran cantidad de conocimiento puede obtenerse, en segundos o minutos y transmitirse hasta llegar al receptor mediante sistemas sencillos de operar, confiables. Por lo que podemos decir que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan con el paso del tiempo.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, tiene un lado ventajoso también plantea problemas de importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad. Por lo que el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en varios países, representa una amenaza para la economía de un país y también para la socledad en su conjunto.

En la actualidad la informatización se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que

presenta comienzan a surgir algunas facetas negativas, como son los delitos informáticos.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

Si se toma en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas. Y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían llegar a estarlo de modo dramático,

algunos valores colectivos y por consiguiente los bienes jurídicos que el ordenamiento jurídico debe proteger.

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

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

2.1 CONCEPTO DE DELITO INFÓRMATICO

Los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto típico), o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)".[62]

El autor Julio Téllez Valdés también menciona la características de los delitos informáticos, y señala las siguientes:

a) Son conductas criminógenas de cuello blanco toda vez que solo determinado numero de personas con ciertos conocimientos en informática.

b) Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.

c) Son acciones de oportunidad en cuando que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico

d) Provocan serias pérdidas económicas ya que casi siempre producen beneficios de mas de cinco cifras a aquellos que los realiza

[62] TÉLLEZ VALDÉS, JULIO; Op. Cit; pp. 104

e) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a cometerse

f) Son muchos los casos y pocas las denuncia y todo ello debido a la misma falta de contemplación por parte del derecho

g) Son sumamente sofisticados y relativamente frecuentes en el ámbito militar

h) Presentan grandes dificultades para su comprobación, esto, por su mismo carácter técnico

i) En su mayoría son imprudenciales y no necesariamente intencionales

j) Ofrecen facilidades para su comisión a los menores de edad

k) Tienden a proliferar cada vez mas, por lo que requieren una urgente regulación

l) Por el momento siguen siendo ilícitos manifiestamente impunes ante la ley.

Asimismo, este autor clasifica a estos delitos, de acuerdo a dos criterios:

1. Como instrumento o medio.

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

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

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

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

d. Lectura, sustracción o copiado de información confidencial.

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

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

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

h. Uso no autorizado de programas de computo.

i. Introducción de instrucciones que provocan `interrupciones` en la lógica interna de los programas.

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

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

l. Acceso a áreas informatizadas en forma no autorizada.

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

1. Como fin u objetivo.

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

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

b. Destrucción de programas por cualquier método.

c. Daño a la memoria.

d. Atentado físico contra la máquina o sus accesorios.

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

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

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

Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.

Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

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

Estafas electrónicas: A través de compras realizadas haciendo uso de la red.

Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Por otro lado, Internet permite dar soporte para la comisión de otro tipo de delitos:

Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

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

2.2 DERECHO COMPARADO

La informática ha venido a cambiar varias áreas en la vida del hombre como lo son la social, la laboral, la escolar, la profesional, en la investigación, en lo jurídico, entre otras, sin embargo en esta evolución pocos son los países que han legislado en dicha materia, tratando de prevenir algunas conductas ilícitas que pudieran realizarse a través de una computadora, los países que ha legislado al respecto son principalmente los del continente Europeo, sin embargo no hay que dejar pasar por inadvertido que en América también se ha legislado sobre la materia, es por ello que a continuación, se mencionan algunas legislaciones que contemplan lo que llaman delitos informáticos y en particular como protegen dichos ordenamientos la perdida de información por su modificación o destrucción,

misma que ésta contenida en sistemas o equipos de informática tema del presente trabajo.

Por lo anterior iniciaremos con las legislaciones de los países de acuerdo a como fueron surgiendo en el tiempo.

2.2.1. ALEMANIA

Es el primer país que conforme a nuestra investigación, comenzó a legislar sobre los delitos informáticos.

"En Alemania, a partir del 1 de agosto de 1986, con el objeto de hacer frente a la delincuencia relacionada con la informática se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986"[63].

Dicha ley contempla los siguientes delitos:

* Espionaje de datos
* Estafa informática
* Falsificación de datos probatorios
* Alteración de datos
* Sabotaje informático
* Utilización abusiva de cheques o tarjetas de crédito

En Alemania, se protegen los datos en cuanto a su alteración o inutilización así como la destrucción de elaboración de datos en un sistema a través del acceso ilícito también podemos ver que protege documentos e información; además contempla un artículo en donde regula a las personas que utilizan tarjetas de crédito o cheques a través de un sistema de computo.

"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"[64]. Como se puede observar en este tipo penal se observa algo importante ya que a una máquina no se le puede engañar o caer en un error como lo seria en un ser humano, por lo que la conducta consiste en influir en el resultado de los datos.

2.2.2. AUSTRIA

En este país se reformo el Código Penal "el 22 de diciembre de 1987"[65]. Contemplando los siguientes delitos de destrucción de datos y estafa informática.

En el tipo penal de destrucción de datos se contempla los datos personales, los no personales y los programas.

La estafa informática sanciona a los que dolosamente causen un perjuicio patrimonial a un tercero interviniendo en el resultado de datos obtenidos de manera automática por medio de la elaboración del programa, la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos; agravando la pena para aquellas personas que tengan conocimientos profesionales en sistemas.

2.2.3. FRANCIA

En Francia la "Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático"[66] contempla los siguientes delitos:

* Acceso fraudulento a un sistema de elaboración de datos
* Sabotaje informático
* Destrucción de datos
* Falsificación de documentos informatizados

---

[63] www.tny.vasnet.mx/prof/cln/der/silvia/leyint.htm.
[64] www.tny.vasnet.mx/prof/cln/der/silvia/leyint.htm.
[65] www.tny.vasnet.mx/prof/cln/der/silvia/leyint.htm.
[66] www.tny.vasnet.mx/prof/cln/der/silvia/leyint.htm.

* Uso de documentos informatizados falsos

En el tipo penal de acceso fraudulento a un sistema de elaboración de datos sanciona a los que accesen y se permanezcan en el sistema; agravando la pena si de ese acceso se modifica o suprime los datos del sistema o bien afecte el funcionamiento del sistema.

Sabotaje informático en esta figura delictiva se sanciona a quien impida, falsee o altere el funcionamiento de un sistema de tratamiento automático de datos.

Por lo que resulta al tipo penal de destrucción de datos se sanciona a quien dolosamente y sin derecho de la persona autorizada para acceder al sistema, introduzca datos en un sistema, suprima o modifique los datos que este contiene o los modos de tratamiento de transmisión.

En el delito de falsificación de documentos informatizados sanciona a quien dolosamente falsifique por cualquier medio documentos informatizados causando un perjuicio a otro. Relacionándose este delito con el de uso de documentos informatizados, ya que este ultimo sanciona a los que con dolo utilicen documentos falsos.

2.2.4. GRAN BRETAÑA.

En 1991 sucedió un acontecimiento referente a un sabotaje informático por lo que comenzó a regir en este país la "Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas"[67].

La legislación de éste país sanciona la modificación de datos y el acceso con el fin de liberar un virus, agravando la pena dependiendo del daño que se ocasione por liberar un virus informático.

---

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

2.2.5. HOLANDA.

En este país a partir del "1 de marzo de 1993 entro en vigencia la Ley de Delitos Informáticos"[68] donde se tipifican diferentes conductas realizadas a través de las computadoras como son:

a) El hacking
b) El preacking, sujeto que evita pagar total o parcialmente el consumo de servicios de telecomunicación.
c) Ingeniería social aquí el sujeto activo convence a la gente de dar información

Distribución de virus si por algún error son deliberados la pena es muy corta, en virtud de que la misma no alcanza ni el mes, en cambio cuando es con intención la pena es mayor toda vez que puede llegar hasta los 4 años de prisión.

2.2.6. CHILE

Es importante destacar a éste país ya que, es el primero en Latinoamérica que legisló sobre los delitos informáticos en su "ley 19.223 promulgada con fecha 28 de mayo de 1993 y publicada en el Diario Oficial N°34.584, de fecha 7 de junio de 1993"[69].

Dicha ley es muy amplia y ambigua en el sentido de contemplar como delito informático el daño a los soportes físicos o hardware, asimismo protege cualquier tipo de información que este contenida en un equipo de computo.

Además contempla otras conductas delictivas tales como el fraude informático consistente en "las alteraciones tanto de los datos como de los programas de un sistema computacional"[70]. Así como el espionaje informático,

---

[68] Información enviada por, Katholiede Universit leuven. Centre for Low Information Technology Ducth

[69] DE LA CUADRA, ENRIQUE, "REGULACIÓN JURÍDICA DE LA INFORMÁTICA COMPUTACIONAL" Temas de Derecho Año II No. 3.1987, Universidad Gabriela Mistral. Santiago de Chile; primera edición pp.1-4

[70] www.viajuridica.com en exclusiva con el abogado especialista en Derecho Informático, Renato Jijena L

considerado como "la obtención ilícita, dolosa sin autorización de datos y de programas computacionales"[71].

2.2.7. ESTADOS UNIDOS DE NORTEAMÉRICA

Cabe hacer mención que Estados Unidos de Norteamérica adopto "en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986"[72].

El acta establece una pena de prisión mayor para aquellas personas que causan un daño intencionalmente por la transmisión de virus y para aquellas que lo realizan de manera intencional la pena es menor.

"En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen"[73].

Es importante mencionar que esta ley ve hacia el futuro ya que contempla varias conductas delictivas, no solo a los virus o gusanos sino que contempla otras instrucciones que tienen como efecto contaminar los programas o base de datos, lo modifiquen, destruyan, copien, transmitan datos o bien altere la operación normal de las computadores, de los sistemas o redes informáticas.

2.2.8. ARGENTINA

Es importante señalar que Argentina, aún no tiene una legislación sobre los llamados delitos informáticos. Pero fue promulgada "la Ley 11.723 de propiedad intelectual el 8 de febrero de 1994"[74].

---

[71] www.viajuridica.com en exclusiva con el abogado especialista en Derecho Informático, Renato Jijena L

[72] www.tny.vasnet.mx/prof/cln/der/silvia/leyint.htm

[73] www.tny.vasnet.mx/prof/cln/der/silvia/leyint.htm.

[74] http://tiny.uasnet.mx/prof/cln/der/silvia/leyint.htm

Esta ley solo define lo que son obras de software, los programas de computadoras protegiéndolas en cuanto a la forma de su divulgación o reproducción exclusivamente.

2.2.9. ESPAÑA

Existe un Nuevo Código Penal de España en donde su artículo 264-2) contempla penas para aquellas personas que "por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. El nuevo Código Penal de España sanciona en forma detallada la violación de secretos, espionaje y divulgación, aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa y cuando el hecho es cometido por parte funcionarios públicos se penaliza con inhabilitación. En materia de estafas electrónicas, el nuevo Código Penal de España, en su artículo 248, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito."[75]

Ambos artículos se localizan dentro del Capítulo IX, titulado de los daños, mismo que se encuentra en el Título XIII, denominado de los delitos contra el patrimonio y contra el orden socioeconómico. Asimismo, se puede observar que el artículo 264-2) del citado código es similar al articulo 211 bis 1 de nuestro Código Penal Federal, ya que ambos protegen la información, toda vez que ésta contiene datos y la misma se encuentra dentro de programas y documentos, sin embargo en nuestro país la información debe estar protegida con un sistema de seguridad en cambio la legislación española no solo protege la información sino también los programas, además no es necesario que dicha información se encuentre protegida basta que este contenida en redes, soportes o sistemas informáticos.

2.3. LEGISLACIÓN EN NUESTRO PAÍS

Nuestro país cuenta con una red mundial de información donde se manejan una gran cantidad de datos contenidos en sistemas informáticos, pero en la actualidad es poca la legislación con la que contamos para prevenir y sancionar las conductas ilícitas que lesionan bienes jurídicos relacionados con la informática.

Las reformas publicadas en el Diario Oficial de la Federación el 17 de mayo de 1999, al Código Penal Federal contempla en su Título Noveno, Capítulo II el acceso ilícito a sistemas y equipos de informática; señalando la modificación, destrucción, provocación de pérdida de información, acceso ilegal a sistemas de particulares (211 bis-1), gubernamentales (211 bis-2 y 211 bis-3) o de servicios financieros (211 bis-4 y 211 bis-5).

Por su parte, el Código Penal para el Distrito Federal en su artículo 231 fracción XIV contempla el delito de fraude informático.

La Ley Federal del Derecho de autor del 24 de diciembre de 1996 y vigente a partir del 24 de marzo de 1997 contempla lo relativo a la protección de los programas de computación, bases de datos y derechos de autor que se relacionan con los dos anteriores. Define al programa de computación, y señala los casos en donde un usuario podrá hacer copias de un programa con autorización del autor estableciendo las facultades y prohibiciones de la reproducción, el acceso a la información contenida en la base de datos con autorización entre los particulares para su publicación reproducción, divulgación, comunicación pública y transmisión, por lo que establece infracciones y sanciones de las conductas ilícitas relacionadas con los programas en cuestión y las bases de datos, entre otros.

Otras entidades federativas, como Sinaloa se ha visto en la necesidad de legislar en cuanto a lo que nombran delitos informáticos, contemplándolos en el Título Décimo denominado contra el patrimonio, siendo éste su bien jurídico tutelado en dicha entidad. Por lo que a la letra se transcribe el siguiente articulo.
"Artículo 217.- Comete delito informático, la persona que dolosamente y sin derecho:

---

[75] www.mir.es/policia/viti/legisla.htm

Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa"[76].

Como se puede observar en este articulo se contemplan varias conductas realizadas en un soporte lógico, en un programa de computadora, en la base, sistema o en una red, imponiéndose a quien incurra en una de ellas la misma pena sin agravarla o atenuarla.

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

CAPÍTULO 3 ELEMENTOS DEL DELITO DE ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA CONTENIDO EN EL ARTÍCULO 211 BIS 1 DEL CÓDIGO PENAL FEDERAL.

3.1. DERECHO A LA INFORMACIÓN

La palabra información significa "acción y efecto de informar. Conjunto de noticias o informes. En cibernética, un sistema y que eventualmente es transmitido por este sistema a otro."[77]. Sin embargo en relación con el procesamiento electrónico de datos significa "datos recopilados y presentados de modo que contengan un significado". [78]

"A la mitad del siglo XX con la Declaración Universal de los Derechos del Hombre 1948, apareció el concepto de derecho a la información". [79]; ya que en su articulo 19 señala que: todo individuo tiene derecho a la libertad de expresión y de opinión, este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. Por lo que el derecho a la información es el derecho que todo ser humano tiene a recibir, investigar y difundir hechos públicos a través de cualquier medio de comunicación social.

El derecho a la información comprende "tres facultades vinculadas entre si 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".[80]

El deber de informar "esta parte que 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"[81].

---

[77] DICCIONARIO ENCICLOPEDICO,"LAROUSSE" COLOMBIA 1999, 6 edición, pp. 102
[78] RODRÍGUEZ, LUIS ÁNGEL; "SEGURIDAD DE LA INFORMACIÓN EN SISTEMAS DE COMPUTO", Ed. Ventura pp. 17.
[79] TÉLLEZ VALDÉS; JULIO; Op. Cit, pp 64
[80] Idem pp 66
[81] Idem pp 66

México reconoce la libertad de expresión en el artículo 6° Constitucional Política señala: "la manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden público; el derecho a la información será garantizado por el Estado".[82]

Así mismo el artículo 7 de nuestra Carta Magna establece que: "Es inviolable la libertad de escribir y publicar escritos sobre cualquier materia. Ninguna ley ni autoridad pude establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública.

Las leyes orgánicas dictarán cuantas disposiciones sean necesarias par afeitar que so pretexto de las denuncias por delitos de prensa, sean encarcelados los expendedores, "papeleros", operarios y demás empleados del establecimiento de donde haya salido el escrito denunciado, a menos que se demuestre previamente la responsabilidad de aquéllos".[83]

El derecho a ser informado "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"[84].

"El derecho al *habeas data* o a la autodeterminación informativa consiste en la garantía que tiene toda persona para conocer todos los registros, archivos, registros, bases o bancos de datos personales, donde se contengan informaciones relativas a ella, así como el derecho que le asiste para corregir o actualizar, en su caso, los datos en cuestión."[85]

---

[82] CONSTITUCIÓN POLICA DE LOS ESTADOS UNIDOS MEXICANOS; ed. 129; Ed. Porrúa; México 2005; pp 12

[83] Idem pp. 12

[84] Op. Cit. TÉLLEZ VALDES; JULIO, pp 66

[85] VILLANUEVA, ERNESTO; "DERECHO COMPARADO DE LA INFORMACIÓN", 2° edición; Ed. Porrúa; México 2002, pp. 25

Dependiendo del tipo de datos o información que fluyan a través de los diferentes medios se encuentran: la información comercial, información empresarial y la información especial.

La información comercial "se manifiesta según una lógica mercantil de distribución".[86] Es decir aquí podemos encontrar información de carácter bancario, financiero, industrial, bursátil, entre otros.

La información empresarial es aquella sustentada "en un cuadro puramente privado en el seno de consorcios empresariales con notorias repercusiones a nivel de dirección, decisión, administración y operación de las mismas";[87] Es decir es aquella información acerca de control de producción, gestión del personal, pedidos, existencias.

La información especial es aquella que "se convierte en intercambio de conocimientos que permiten un mejor desarrollo de las actividades educativas o de investigación a nivel técnico o científico".[88]

El servicio que las redes de comunicación pueden prestar más fácilmente es la información, la mayoría de la información que existe en Internet está disponible gratuitamente; por ejemplo, las versiones en línea de diarios, revistas, informes e incluso programas informáticos está a disposición del publico.

Agrupar la información en archivos computacionales almacenados en sitios específicos aumenta la vulnerabilidad de los datos y la posibilidad de destrucciones, accesos o modificaciones no autorizadas.

El crecimiento de los bancos de datos donde está contenida la información estratégica ha multiplicado los riesgos de violación al carácter confidencial, motivo por el cual es importante en el caso de las empresas instalar dispositivos de seguridad para proteger la información almacenada en las computadoras.

El autor Julio Téllez Valdes manifiesta que "la importancia económica de la información no está puesta en duda, es un verdadero bien susceptible de

---

[86] TÉLLEZ VALDES; JULIO; Op. Cit pp. 80
[87] Idem pp 80
[88] Ibidem

apropiación con un innegable valor patrimonial inherente".[89] Por lo que podemos decir que la información puede ser susceptible de apropiación y la misma pertenece a su autor. Por ello cualquier persona que tenga algún tipo de información tiene derecho a protegerla de su destrucción o modificación con algún tipo de seguridad, tema del cual hablaremos en seguida.

3.2. DERECHO A LA PROTECCIÓN DE LA INFORMACIÓN

En años recientes, el uso de las computadoras ha crecido al punto que hoy está presente en casi cualquier aspecto del mundo de los negocios y en otros aspectos. Junto con este crecimiento ha sido la necesidad de compartir recurso, utilizar mejor equipo y utilizar el trabajo de otros. Motivos por el cual la necesidad de compartir y cooperar ha crecido en la gente involucrada y su necesidad de acceso rápido e intercambio de información. Tal crecimiento ha presentado nuevos problemas en la seguridad de la información.

La seguridad informática Jesús de Marcelo Rodao la define como: "el conjunto de procedimientos que nos permite que nuestros datos de hoy puedan ser utilizados mañana sin ninguna merma de calidad en los mismos".[90]

Las medidas de seguridad están orientadas a preservar la información, impidiendo cualquier intromisión que pudiera conducir a la destrucción o alteración de los archivos que forman la base de datos.

La seguridad se refiere al acceso ilegal a los archivos de la computadora en la red con el propósito de destruir, modificar o tener acceso a los datos sin permiso. La red es "un grupo de computadoras interconectadas capaces de compartir datos con las otras" [91].

En lo que respecta a redes de computadoras, "la definición de seguridad implica tres aspectos básicos de protección (1) proveer acceso controlado a los recursos

---

[89] Idem pp 65

[90] DE MARCELO RODAO, JESÚS; "PIRATAS CIBERNÉTICOS"; Ed. Alfaomega; primera edición México 2002; pp. 70

[91] RODRÍGUEZ, LUIS ÁNGEL; Op. Cit, pp 102

(identificación y autentificación), (2) proveer el uso controlado de esos recursos y (3) proveer la seguridad de que el nivel de protección deseado es alcanzado". [92]

El propósito de la seguridad en redes es la siguiente:

"Preservar la confidencialidad de los datos que pasan a través de cualquier canal de comunicación.

Asegurar que el mensaje permanezca inalterado durante su transmisión, reteniendo la integridad de los datos que están siendo enviados.

Asegurar también que realmente estamos conectados con quien creemos que estamos y ellos (los receptores) deben, a su vez estar seguros de que nosotros somos quienes dijimos que éramos.

Adicionalmente, deben existir formas de probar que un mensaje transmitido ha sido recibido exitosamente.

Asimismo, debemos asegurarnos que solamente los usuarios autorizados tengan acceso a la red, controlando el acceso a los componentes de la red y a los passwords"[93]

Toda información debe ser protegida para asegurar credibilidad junto con calidad y precisión al usuario.

"Las compañías sin posibilidades de producir o utilizar sistemas de información, pueden sufrir pérdidas importantes e incluso fatales. Por este motivo, es recomendable contar con medidas de prevención que limiten los peligros potenciales y métodos para hacer frente a las consecuencias. Dichos riesgos reúnen diversos aspectos que van desde catástrofes naturales (incendios, inundaciones, etc) hasta fallas de hardware o software, además de la destrucción accidental o intencionada de la información (descompostura de una máquina, destrucción de archivos, sabotaje, etc)."[94]

También existen otro tipos de riesgos que afectan la integridad de la información entre estos se encuentran los siguientes:

---

[92] Idem
[93] Idem pp 104
[94] GATTON PIERRE, "PROTECCIÓN INFORMÁTICA", Ed. Trillas, México 1998, pp 35

A) Equipos con errores mecánicos, ya que con el transcurso del tiempo las computadoras pueden tener fallas.

B) Estafas informáticas, es decir, muchas veces compramos el software o el hardware a un precio inferior lo que nos lleva a que posteriormente no funcione el equipo adecuadamente.

C) Error humano, muchas veces no leemos el manual lo que nos conlleva a cometer errores en la computadora creando fallas en ella.

D) Gamberrismo, esto es la destrucción de datos por venganza, ya sea por un empleado descontento o por el simple placer de hacerlo.

E) Virus cabe mencionar que la mayor amenaza para los usuarios y administradores de la red son los virus informáticos, ya que los virus a través su propagación destruye los datos e infecta los disquetes o incluso la misma red.

La palabra virus fue utilizada por "David Gerrold, que en 1972 escribió la novela When Harlie Was One. En ella una computadora emulaba al cerebro del hombre. Para conectarse con otras computados usaba un programa llamdo VIRUS. Era inevitable el uso de la palabra, dado que existían ciertas analogías entre los virus biológicos y los de ordenador. Hace unos años una comision internacional, decidieron mantener la palabra virus pero no como un nombre, sino como un acrónimo, más concretamente V.I.R.U.S. (Vital Information Resources Under Siege- Recursos De Información Vital Bajo Acoso)"[95]

Los virus tiene diferentes finalidades algunos solo infectan, otros alteran datos, otros los eliminan y algunos solo muestran mensajes.

"Existen ciertas similitudes entre virus biológicos y los informáticos: mientras los primeros son agentes externos que invaden células para alterar su información genética y reproducirse, los segundos son programas-rutinas, en un sentido más estricto, capaces de infectar archivos de computadoras y reproducirse una y otra vez cuando se accede a dichos archivos, por lo que dañan la

[95] DE MARCELO RODAO, JESÚS, Op. Cit, pp. 75

información existente en la memoria o en alguno de los dispositivos de almacenamiento de la computadora".[96] Por lo que podemos decir que los virus informáticos son programas generalmente destructivos ya que son capaces de modificar o dañar la información contenida en una computadora, el cual se instala sin el consentimiento o permiso del usuario.

Un virus informático presenta las siguientes características:

1. "Puede contaminar a un gran número de computadoras
2. Tiene efectos negativos y destructivos
3. Puede infectar otros programas
4. Suele pasar inadvertido hasta el momento de su propagación masiva
5. Puede activarse con un suceso particular (una fecha o una hora determinada."[97]

Los tipos de virus pueden ser:

"1. Virus latente: espera una fecha determinada o algún otro evento para activarse.

2. Virus activo: se activa desde el momento de introducirse en una computadora

3. Virus mutante: pude activarse así mismo y sufrir una transformación para adaptarse a las condiciones del ambiente 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."[98]

Las categorías de los virus son las siguientes:

1. Bug-ware: "Son programas totalmente legales que realizan una serie de tareas concretas, por ejemplo propagadores de hardware o incluso antivirus. Si no se conoce bien su manejo, o tienen una programación complicada, pueden producir daños al hardware de la computadora o al software"[99]. Es decir si el usuario no sabe manejar este tipo de programas puede ocasionar fallas a su computadora.

---

[96] HERNÁNDEZ HERNÁNDEZ, ARTURO; "GUÍAS Y TEXTOS DE COMPUTO; VIRUS INFORMÁTICO"; Ed. Dirección General de Servicios de Cómputo Académico, pp- 3

[97] GRATTON PIERRE; Op. Cit, pp 254

[98] Idem pp 256

[99] HERNÁNDEZ HERNÁNDEZ, ARTURO, Op. Cit, pp. 9

2. Caballo de Troya: "éste es un programa maligno que se oculta en un programa legítimo".[100] Es decir este programa se diseña para realizar una función maligna pero no lo parece.

3. Camaleón: Es parecido al caballo de Troya la diferencia es que reproduce fielmente al programa que imita.

4. Bombas lógicas: es un programa que "actúa según un determinado tipo de condiciones técnicas"[101]. Es decir, este virus se presenta después de un periodo determinado, en una fecha estipulada, después de cierto número de ejecuciones del programa, la ejecución de determinado programa..

5. Conejo: "Evita cualquier posible preferencia de otro usuario; la mayoría se autodestruyen una vez que han actuado".[102] Este tipo de programa se ve en la red ya que en la red existe lo que se denomina multitarea, esto es en que las tareas siguen un orden determinado, pero en la red puede haber preferencias para ciertos usuarios y que se pueden saltar las tareas de otros y ellos ser los primeros.

6. Gusanos: "Programa cuya única finalidad es ir consumiendo espacio en la memoria RAM, mediante copias sucesivas de si mismo residentes en la memoria, hasta desbordarla, en ese momento generalmente aborta todo lo que está en ejecución".[103]

7. Killer o retrovirus. "Son un tipo determinado de virus que entre sus instrucciones llevan la de borrar o infectar a una vacuna o a varias".[104]

8. Joke-program,: no es maligno, son virus " que solo resultan simpáticos. En un principio había muchos, como el come-come, el cookie, hoy en día se diseña alguno de tarde"[105]

---

[100] SEOANE, JOSÉ ALBERTO, "ACOSO DIGITAL; PREVENCIÓN Y ANTIDOTOS"; Ed. Macchi, México 2001, pp. 107

[101] HERNÁNDEZ HERNÁNDEZ, ARTURO, Op. Cit, pp. 10

[102] Idem pp. 10

[103] SEOANE, JOSÉ ALBERTO Op. Cit, pp 107

[104] DE MARCELO RODAO, JESÚS. Op. Cit, pp.19

[105] Idem; pp.19

9. Leopfrog o rana: "Es un programa parecido al gusano que a partir de una serie de datos conocidos, como la clave de acceso a una cuenta y el nombre de usuario, se dedica a recopilar información".[106]

10. Máscara: "Este programa asume la identidad de un usuario autorizado y realiza así las mismas labores de la anterior".[107]

11. Mockinbird: es un virus que: "se queda fuera del sistema en estado de espera, y cuando un usuario autorizado entra, se fija en el proceso de entrada aprendiendo la clave de acceso, nombre de usuario y cualquier otro dato interesante. Puede aprovechar el hueco para entrar y actuar. Normalmente no causa daños para no revelar su existencia".[108]

F) Ataques de piratas. Comúnmente es para robar información, dañarla destruirla o simplemente para retar los sistemas de seguridad, el autor de Jesús Marcelo Rodao [109] señala los siguientes:

Los hacker son usuarios con un alto nivel de conocimiento en informática. El término hacker se utiliza para nombrar a una cierta élite de caballeros del bit y a aquellos que se especializan en la intrusión en sistemas no autorizados.

El hacker es el término más general, otro término es el de Wracker son usuarios que se dedican a viajar por Internet buscando programas Shareware o Freewarey, este tipo de usuarios pueden producir daños sin querer.

Los lamber son individuo que no tiene los conocimientos en informática iguales a los de los hackers pero tiene un poco mas de conocimientos que el resto de los individuos. Sin embargo el termino lamber en informática es un termino despectivo ya que este tipo de usuarios presume de tener muchos conocimientos en informática sin embargo no es así, normalmente utilizan técnicas demasiado viejas pero para la mayoría de los usuarios son novedosas.

Un script kiddies se dedica a ocasionar diversas gamberradas, siendo estas molestas y no peligrosas, ejemplo de ello es en EE.UU una redada contra un grupo

---

[106] HERNÁNDEZ HERNÁNDEZ, ARTURO Op. Cit pp. 11
[107] Ibidem
[108] DE MARCELO RODAO, JESÚS; Op. Cit; pp 20
[109] Idem pp 23

de estos chicos que habían llenado de graffitis varias paginas web de organismos gubernamentales.

Newbie no son peligrosos porque refieren asesorarse y normalmente acaban siendo hackers. En cierto modo un newbie es el aprendiz de un hacker. Este tipo de personas prefieren aprender sin causar ningún tipo de daño.

Los phreaker, este término se utiliza en dos casos, el más doloroso es del pirata informático que busca realizar actividades ilegales para enriquecerse, o bien destruir por puro terrorismo.

Un craker es el que se especializa en reventar sistemas de protección de programas, o bien sistemas electrónicos de protección de video, en cuyo caso sería un videocraker.

Un sneaker es un espía informático, una variante de éste es el snuffer, se limita a averiguar claves de acceso a sistemas y sobre todo descubre errores y agujeros en programas.

Por último tenemos al rider, es alguien que anteriormente estuvo dentro de una categoría de las anteriores y que actualmente trabaja como especialistas de seguridad en algún tipo de empresa.

Asimismo podemos hablar de varias técnicas de ataque o destrucción de la información en una computadora.

Las técnicas que pueden ayudar a tener un acceso para atacar o destruir la información son:

1. Sniffer: son técnicas para averiguar principalmente claves de acceso. Con un sniffer un hacker podrá apoderarse de todas las contraseñas e identificaciones de la red. También podrá interceptar documentos, datos financieros y correos electrónicos.

Para no ser victima de un sniffer se deberia de encriptar la información, ya que el sniffer podrá interceptar la información pero tendrá que descifrarla, y si se quiere aumentar la seguridad dicha información se podrá codificar.

2. Back door: como su nombre lo dice son puertas traseras creadas por el diseñador del sistema para poder acceder a él sin que posteriormente lo detecten.

3. Spamming. Técnicas utilizadas para mandar de forma masiva correo. Se utiliza normalmente para mandar publicidad.

4. Cancelling: Técnicas para anular mensajes en una lista de correo.

Existen varios sistemas de seguridad ante el acceso no autorizado, en la Enciclopedia Encarta [110] se señalan las siguientes:

1. Las claves de acceso son secuencias confidenciales de caracteres que permiten que los usuarios autorizados puedan acceder a un ordenador. Para que las claves de acceso obtengan un buen resultado deben ser difíciles de adivinar. Por lo que suelen contener una mezcla de caracteres y símbolos que no corresponden a una palabra y la misma debe limitar el número de intentos de introducir la clave, es decir pueden ser alfanuméricos.

2. Las tarjetas de contraseña son tarjetas de plástico que no pueden ser manipuladas, dotadas de un microprocesador que almacena una clave de acceso que cambia frecuentemente de forma automática. Estas tarjetas contienen una clave y al introducir el usuario su clave las compara verificando que sea la clave que la tarjeta genera automáticamente.

Posiblemente con el paso del tiempo las claves y las tarjetas de acceso tengan mecanismos basados en características personales únicas como las huellas dactilares, los capilares de la retina, las secreciones de la piel, las variaciones de la voz, entre otros.

3. El contrafuegos es un ordenador situado entre las computadoras de una red corporativa e Internet. El cortafuegos impide a los usuarios no autorizados acceder a los ordenadores de una red, y garantiza que la información recibida de una fuente externa no contenga virus. Las redes corporativas u ordenadores en caso de estar conectadas a Internet utilizan los contrafuegos.

4. El cifrado es otra técnica para proteger la confidencialidad. A través de esta técnica "la información puede cifrarse y descifrarse empleando ecuaciones

---

[110] "Seguridad informática," *Enciclopedia Microsoft® Encarta® 2000.* © 1993-1999 Microsoft Corporation. Reservados todos los derechos.

matemáticas y un código secreto denominado clave. Es decir aquí se emplean dos claves, una para codificar la información y otra para descodificarla. La clave que codifica la información sólo es conocida por el emisor. La clave que descodifica los datos puede ser conocida por varios receptores. Estas claves se modifican periódicamente, lo que complica el acceso no autorizado y hace muy difícil descodificar o falsificar la información cifrada.

5. Las técnicas de firma electrónica permiten autentificar los datos enviados de forma que se pueda garantizar la procedencia de los mismos (imprescindible, por ejemplo, a la hora de enviar una orden de pago).

Para proteger la información de un ataque de virus: existen los programas antivirus. Los objetivos de este tipo de programas son "evitar la presencia de virus, diagnosticar el tipo de infección producida y vacunar los archivos contaminados".[111]

El programa antivirus se encarga de vigilar la presencia de virus y una vez que detecto el virus trata de destruirlo. Sin embargo ningún programa antivirus puede garantizar la protección absoluta contra las infecciones de los virus, ya que los diseñadores de los virus ven un desafío para desarrollar nuevos programas que superen las medidas preventivas y de seguridad.

Por otro lado también existen lo que se conoce como agujeros de seguridad, por aquí es donde un hacker suele entrar a un sistema, "pueden ser en la mayor parte de los casos un bug, un error de programación"[112].

Los agujeros de seguridad se pueden clasificar según lo que permiten hacer en:

- Los que niegan el uso de un servicio
- Los que permiten a un hacker acceder sin autorización,
- Los que permiten a un usuario con nivel bajo de permisos acceder a un nivel más alto.

---

[111] GRATTON PIERRE; Op. Cit, pp 260
[112] DE MARCELO RODAO, JESÚS; Op. Cit; pp 148

Por otro parte como se ha visto en los capítulos anteriores con la aparición de la computadora también han surgido nuevas formas de realizar conductas ilícitas, motivo por el cual como ya lo hemos visto diferentes países incluyendo el nuestro ha tratado de proteger la información, por lo que a continuación nos abocaremos al estudio del delito contemplado en el artículo 211 bis 1 párrafo primero del Código Penal Federal, el cual a la letra dice "al que sin autorización modifique, destruya o provoque pérdida de la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se les impondrá de seis meses a dos años de prisión y de cinco a trescientos días multa."[113]

3.3. CONCEPTO DE DELITO

La palabra delito "deriva del verbo latino delinquere, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley. El delito, está íntimamente ligado a la manera de ser de cada pueblo y a las necesidades de cada época, los hechos que en determinado momento han tenido ese carácter, lo han perdido en función de situaciones diversas y, al contrario, acciones no delictuosas, han sido erigidas en delitos".[114] En este orden de ideas podemos decir que las conductas tipificadas ayer como delito en la actualidad pueden no serlo y viceversa, ya que las necesidades en la vida de cada país va cambiando por lo que el derecho tiene que cambiar y adecuarse a ella.

Para Francisco Carrara, el delito "es la infracción de la ley del estado promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso".[115]

---

[113] AGENDA PENAL FEDERAL Y DEL DISTRITO FEDERAL; Ed. RAUL JUAREZ CARRO SOCIEDAD ANONIMA DE CAPITAL VARIABLE, México 2003, pp. 152

[114] CASTELLANOS TENA, FERNANDO, "LINEAMIENTOS ELEMENTALES DE DERECHO PENAL", Ed. Porrúa, México 2004, Cuadragésimo Quinta Edición pp. 125

[115] Ibidem, págs. 125 y 126

Por su parte, Rafael Garófalo, representante del positivismo, lo define de la siguiente manera: "Es la violación de los sentimientos altruistas de probidad y de piedad en la medida media indispensable para la adaptación del individuo a la colectividad".[116]

Para Jiménez de Asúa delito "es el acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal".[117] Para Cuello Calón delito "es la acción antijurídica, típica, culpable y sancionada con una pena."[118]

Sin embargo el Código Penal Federal en su artículo 7° párrafo primero establece que delito "es el acto u omisión que sancionan las leyes penales".[119]

3.4 CLASIFICACION DEL DELITO

Existen varias formas de clasificar los delitos, entre las más importantes se encuentran:

1. Por la conducta los delitos son de:

a) acción: "se cometen mediante un comportamiento positivo; en ellos se viola una ley prohibitiva.

b) Omisión: el objeto prohibido es una abstención del agente, consisten en la no ejecución de algo ordenado por la ley. Los delitos de omisión a su vez se subdividen en de simple omisión y de comisión por omisión:

Delitos de simple omisión: Consisten en la falta de una actividad jurídicamente ordenada, con independencia del resultado material que produzcan.

Delitos de comisión por omisión o impropios delitos de omisión: son aquellos en los que el agente decide no actuar y por esa inacción se produce el resultado material". [120]

---

[116] Ibidem, pág. 126

[117] JIMÉNEZ DE ASUA, LUIS; "PRINCIPIOS DEL DERECHO PENAL LA LEY Y EL DELITO", Argentina 1990, cuarta edición Ed. Abelardo –Perrot, pp. 207

[118] MARQUEZ PIÑERO, RAFAEL; "DERECHO PENAL PARTE GENERAL", Ed. Truillas, México 1999, quinta edición pp. 133

[119] AGENDA PENAL FEDERAL. Op. Cit pp. 123

[120] CASTELLANOS TENA, FERNANDO. Op. Cit. pp. 136

De lo anterior podemos decir que los delitos de acción son aquellos que se consuman a través de un comportamiento positivo, es decir, en una conducta de hacer o un actuar; y los delitos de omisión son aquellos que para que tenga lugar la consumación del delito se requiere una conducta de abstención, es decir un no hacer. Podemos agregar que en delitos de omisión o simple omisión no existe un cambio en el mundo exterior y en los delitos de comisión por omisión o impropios existe un cambio en el mundo exterior.

El delito materia del presente estudio, es un delito de acción toda vez que se requiere la realización de una conducta para que se pueda llevar a cabo a través de un hacer, es decir que se debe de realizar varias actividades para que se pueda consumar el delito, como lo es dar instrucciones a la computadora para que las vaya ejecutando y así llegar al resultado deseado que en este caso seria modificar, destruir o provocar la perdida de información.

2. Por el resultado los delitos son:

a) Delito formal: "es el que jurídicamente se consuma por el solo hecho de la acción o de la omisión del culpable sin que sea precisa la producción de un resultado externo .

b) Delito material: se entiende el que no puede consumarse si no se produce el resultado antijurídico que el delincuente se propuso obtener". [121]

Por lo que podemos decir que los delitos formales son cuando existe una acción o una omisión pero no se manifiesta un resultado externo, lo que se castiga es la conducta en si, y los delitos materiales son los que si provocan un resultado externo y se sanciona éste.

En cuanto al resultado el delito en estudio es un delito de resultado material, ya que para que se tipifique el delito es necesario un cambio en el mundo exterior como es la modificación, destrucción o bien la perdida de información.

3. Por el daño que producen:

---

[121] CUELLO CALÓN; EUGENIO "PARTE GENERAL TOMO I,"; Bosch Casa Editorial, Barcelona 1981, edición décimo octava, pp 318

a) Delitos de lesión: "producen un daño efectivo y directo en los intereses o bienes jurídicamente protegidos por la norma vulnerada.

b) Delitos de peligro: no causan un daño efectivo y directo en intereses o bienes jurídicamente protegidos, pero propician una situación de amenaza evidente de daño para ellos". [122]

Por lo que podemos afirmar que los delitos de lesión provocan un daño directo a los bienes jurídicamente tutelados y los delitos de peligro como su nombre lo dice son aquellos que solo ponen en peligro los bienes jurídicamente protegidos o tutelados por la ley penal, ya que no sufren un daño directo.

Por lo que el tipo penal en estudio por el daño que produce es un delito de lesión ya que altera, modifica, destruye o provoca la perdida de la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

4. Por su duración se clasifican en: delitos instantáneos, permanentes y continuados, contemplados en el articulo 7 del Código Penal Federal :

a) Delitos instantáneos: "cuando la consumación se agota en el mismo momento en que se han realizado todos sus elementos constitutivos.

c) Delitos continuados: cuando con unidad de propósito delictivo, pluralidad de conducta y unidad de sujeto pasivo, se viola el mismo precepto legal.

d) Delitos permanentes o continuo: cuando la consumación se prolonga en el tiempo". [123]

En otras palabras, los delitos instantáneos son aquellos que se produce en un solo momento o instante; delitos permanentes son aquellos que requieren una continuidad tanto en la conciencia del sujeto activo como en su ejecución y los delitos continuados son aquellos en el que se producen varias acciones y una sola lesión jurídica.

Por la duración del delito en estudio es un delito instantáneo ya que se realiza en un solo momento.

---

[122] MARQUEZ PIÑERO, RAFAEL. Op. Cit. pp. 140

[123] "AGENDA PENAL FEDERAL Y DEL DISTRITO FEDERAL" . Op. Cit. pp. 124

5. Su culpabilidad los delitos se clasifican en:

a) Delitos dolosos: "cuando se dirige la voluntad consciente a la realización del hecho típico y antijurídico.

b) Delitos culposos: no se quiere el resultado penalmente tipificado, mas surge por el obrar sin las cautelas y precauciones exigidas por el Estado para asegurar la vida en común". [124]

Es decir los delitos dolosos son aquellos en donde existe la voluntad del sujeto activo de realizar el resultado típico y antijurídico, en otras palabras el sujeto activo del delito quiere realizar la conducta; los delitos culposos son aquellos que se producen cuando el sujeto activo no desea el resultado típico y antijurídico, sin embargo este se presenta por la falta de atención y cuidado del mismo.

En atención a lo anterior, el delito que nos ocupa es un delito doloso, en virtud de que el sujeto activo quiere realizar la modificación, destrucción o pérdida de la información.

6. Forma de persecución delitos:

a) Delitos por querella: "perseguibles por iniciativa privada o por acción privada".[125]

b) Delitos de oficio: "son investigados y posteriormente sancionados por iniciativa de la autoridad".[126]

Por lo que los delitos de querella son aquellos delitos perseguibles a petición de la parte legitimada y los delitos de oficio son aquellos en que la autoridad esta obligada por mandato de ley a perseguir y castigar a los responsables del delito.

Por lo antes expuesto podemos decir que el tipo penal contemplado en el artículo 211 bis 1, es un delito perseguible de oficio, ya que la autoridad se encuentra obligada a perseguir la conducta ilícita.

7. Su gravedad: Existen dos clasificaciones la bipartita donde distinguen los delitos de las faltas y la tripartita habla de crímenes, delitos y faltas o contravenciones.

---

[124] CASTELLANOS TENA, FERNANDO. Op. Cit. pp. 141
[125] MARQUEZ PIÑERO, RAFAEL. Op. Cit. pp. 141
[126] Ibidem pp. 141

"En está división se consideran crímenes, los atentados contra la vida y los derechos naturales del hombre; delitos, las conductas contrarias a los derechos nacidos del contrato social, como el derecho de propiedad; por faltas o contravenciones, las infracciones a los reglamentos de policía y buen gobierno".[127]

En el caso en estudio por su gravedad es un delito.

8. Por los sujetos que intervienen:

a) Delitos unisubjetivos: son aquellos en que solo basta con un individuo para su ejecución

b) Delitos plurisubjetivos: son aquellos donde es necesaria la participación de dos o más individuos para que se pueda ejecutar el delito.

Por lo que hace a los sujetos que intervienen en el delito de estudio, puede ser un delito unisubjetivo: ya que solo basta con la participación de un sujeto para su ejecución.

3.5 ELEMENTOS POSITIVOS DEL DELITO

Los elementos positivos del delito son los requisitos que la ley establece para que una conducta sea considerada como delito.

Como se puede observar de las definiciones de delito que dan los doctrinarios de la materia penal no se ha llegado a un acuerdo sobre los elementos del delito, en virtud de que para algunos éste es indivisible, es decir, es un todo (corriente unitaria o totalizadora), y para otros, el delito está constituido por varios elementos (corriente atomizadora o analítica).

En cuanto a los elementos que integran el delito los autores varian en cuales son los elementos positivos y los negativos, encontrando dentro de las anteriores definiciones de delito los siguientes:

Aspectos positivos	Aspectos negativos
Conducta	Ausencia de conducta
Tipicidad	Atipicidad

[127] JIMÉNEZ DE ASUA, LUIS. Op. Cit. pp. 135

Antijuridicidad	Causas de justificación
Imputabilidad	Inimputabilidad
Culpabilidad	Inculpabilidad

3.5.1. **CONDUCTA**

"La conducta es el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito".[128]

Solo el ser humano tiene relevancia para el ámbito de aplicación del derecho penal. Por lo que respecta a las personas morales, éstas no se consideran sujetos activos de los delitos por carecer de voluntad propia; sin embargo, pueden considerarse sujetos pasivos, del delito especialmente cuando se presentan infracciones patrimoniales en su contra.

A) La acción.- "La acción consiste en la conducta positiva, expresada mediante un hacer, una actividad, un movimiento corporal voluntario con violación a una norma prohibitiva."[129]

Algunos autores consideran al acto como sinónimo de acción, de hecho o de conducta. Sin embargo para Jiménez de Asúa el acto abarca la acción y la omisión.

Definiendo al acto como "la manifestación de voluntad que, mediante acción, produce un cambio en el mundo exterior, o que por no hacer lo que se espera deja sin mudanza ese mundo externo cuya modificación se aguarda"[130].

Rafael Marquez Piñero en su obra cita a Bindig señalando éste último que la palabra hecho "designa todo acontecimiento, sea o no procedente del intelecto humano o de su actividad, o acaezca por simple caso fortuito, sin voluntariedad, nota fundamental del derecho penal".[131]

Por lo que podemos decir que la acción es un movimiento corporal a través del cual se produce un resultado material.

---

[128] CASTELLANOS TENA, FERNANDO. Op. Cit. pp. 149
[129] PAVON VASCONCELOS, FRANCISCO. "DERECHO PENAL MEXICANO"; Décima Edición, S.A, Ed. Porrúa; México 1991; pp. 186
[130] JIMÉNEZ DE ASUA, LUIS. Op. Cit. pp. 210
[131] MARQUEZ PIÑERO, RAFAEL. Op. Cit. pp. 157

Los elementos de la acción son:

a) La manifestación de voluntad. "Consiste en el peculiar comportamiento de un hombre que se traduce exteriormente en una actividad o inactividad voluntaria; es decir, la conducta consiste exclusivamente en una actividad o movimiento corporal, o bien una inactividad, una abstención, un no hacer."[132]

b) El resultado. Comprende "tanto las modificaciones de orden físico, como las del orden jurídico y ético, tanto las cosas materiales como los estados de ánimo del sujeto pasivo y de la sociedad, no sólo el cambio en el mundo material sino también mutación en el mundo psíquico y aún el riesgo o peligro.

c) El nexo de causalidad. Entre la acción y el resultado debe de haber una relación de causa a efecto; y es causa tanto la actividad que produce inmediatamente el resultado como la que lo origina inmediatamente, sea por elementos penalmente inoperantes persé, pero cuya eficacia dañosa es aprovechada." [133]

B) La omisión. Consiste en dejar de hacer lo que se debe de realizar, es decir, se deja de hacer algo que se encuentra ordenado por la ley; es una inactividad, una abstención. "La omisión es conducta negativa, es inactividad voluntaria de una norma preceptiva"[134]. Se clasifica en dos tipos:

a) Omisión simple. Es dejar de hacer en el que se viola una ley preceptiva y se produce un resultado jurídico no material.

b) Comisión por omisión. Consiste en una doble violación a una ley prohibitiva y a otra preceptiva, es decir, se presentan dos tipos de conducta, por un lado el hacer y por el otro un no hacer, produciendo

---

[132] GONZÁLEZ QUINTANILLA, JOSÉ ARTURO; "DERECHO PENAL MEXICANO, PARTE GENERAL", Ed. Porrúa, México 1991, primera edición, pp. 182

[133] CARRANCA Y TRUJILLO, RAÚL, "DERECHO PENAL MEXICANO", Mexico, Ed- Purrúa, vigésimo segunda edición, México 2004. pp 223

[134] ibidem pp.263

con esto un resultado jurídico y otro material, existiendo entre ambos una relación causal.

Por lo que podemos decir que el delito de acceso ilícito a sistemas y equipos de informática es un delito de acción toda vez que se requiere la realización de un hacer voluntario y así poder llegar al resultado deseado que en este caso sería modificar, destruir o provocar la pérdida de información contenida en un sistema y equipo de informática.

3.5.2 TIPICIDAD

Es importante señalar y analizar lo que dispone el artículo 14 de la Constitución Política de los Estados Unidos Mexicanos, que a la letra dice:

Art. 14 "En los juicios de orden criminal queda prohibido imponer por simple analogía y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trate."[135]

De lo anterior se puede deducir que si la conducta no esta contemplada en la ley, no puede considerar delito aún siendo ilícita; por lo tanto éste es uno de los elementos indispensables para configurar un delito. En este orden de ideas es necesario hacer una distinción de lo que conoce como tipicidad y tipo.

La tipicidad, Raúl Carranca y Trujillo la define como "la conformidad de una conducta con la hipótesis delictiva consignada en la ley penal".[136] Para el Doctor Jesús Martínez Garnelo, dice que la tipicidad "es el encuadramiento de una conducta con la descripción hecha en la ley, la adecuación de una conducta concreta con la descripción legal formulada en abstracto; y el tipo es la descripción legal de una conducta estimada como delito, que lesiona o hace peligrar bienes jurídicos protegidos por la norma penal; es una concepción legislativa, es la descripción de una conducta dentro de los preceptos penales".[137]

---

[135] CONSTITUCIÓN. Op. Cit. pp.4
[136] Op. Cit. pp. 171
[137] MARTÍNEZ GARNELO, JESÚS: "LA INVESTIGACIÓN MINISTERIAL PREVIA"; Ed. CGS Editores, pp. 15

En otras palabras, tipicidad es el encuadramiento de una conducta realizada por el sujeto activo en la descripción hecha por la ley y el tipo es la descripción de la conducta que el Estado por medio de sus órganos realiza y queda prohibida en la legislación penal.

Según Fernando Castellanos Tena clasifica a los tipos penales "atendiendo a su composición; (normales y anormales); ordenación metodológica (fundamentales o básicos, especiales y complementados), en función de su autonomía o independencia (autónomos o independientes y subordinados), por su formulación (casuísticos y amplios), y por el daño que causan (de daño o de lesión y de peligro)".[138]

Normales: Son aquellos que se limitan a hacer una descripción objetiva. (Como ejemplo encontramos el tipo penal de homicidio).

Anormales: Son aquellos que además de contener elementos objetivos, contienen elementos subjetivos o normativos. (Como ejemplo encontramos al estupro).

Fundamentales: Son aquellos que constituyen la esencia o fundamento de otros tipos. (Ejemplo: homicidio).

Especiales: Se forman agregando otros elementos al tipo fundamental, al cual subsumen. (Ejemplo: parricidio).

Complementados: Se constituyen al lado de un tipo básico y una circunstancia o peculiaridad distinta. (ejemplo: homicidio calificado).

Autónomos: Tienen vida por sí mismo. (Robo simple).

Subordinados: Dependen de otro tipo. (homicidio en riña).

Casuístico: Prevé varias hipótesis, y en algunas ocasiones el tipo se integra con una de ellas. (Usurpación de funciones).

Amplios: Es una sola hipótesis. (robo).

De daño o de lesión. Protegen al bien de la disminución o destrucción. (homicidio, fraude).

---

[138] CASTELLANOS TENA, FERNANDO. Op. Cit. pp. 174-175

De peligro. Protegen al bien de ser dañado.

Por lo que a continuación analizaremos los elementos del tipo penal en el delito de acceso ilícito a sistemas y equipos de informática.

a) Conducta: En cuanto hace al delito de acceso ilícito a sistemas y equipos de informática, la conducta es de acción para que se modifique, destruya se provoque la pérdida de la información contenida en un sistemas y equipos de informática.

b) Resultado: El delito en estudio hay un cambio en el mundo exterior.

c) Nexo Causal: Es la relación que existe entre la conducta realizada por el sujeto activo y el resultado en este caso es cuando el sujeto activo realiza un hacer voluntario para modificar, destruir o provocar la perdida de la información contenida en un sistema y equipos de informática realizando así un cambio en el mundo fáctico.

d) Sujeto activo: "sólo el hombre es sujeto activo del delito, porque únicamente el se encuentra provisto de capacidad y voluntad y puede, con su acción u omisión, infringir el ordenamiento jurídico penal. Se dice que una persona es sujeto activo cuando realiza la conducta o el hecho típico, antijurídico, culpable y punible, ya sea como autor intelectual, material, partícipe, cómplice o encubridor".[139]

Dentro de éste delito el sujeto activo es un especialista y el cual tiene conocimientos amplios de informática.

e) Sujeto pasivo: "Por tal se conoce al titular del derecho o interés lesionado o puesto en peligro por el delito"[140]. Es el titular del derecho violado en su contra y que jurídicamente ese derecho está protegido por la norma. Por lo tanto es importante señalar en primer lugar, que debemos hacer una distinción entre el sujeto pasivo y el ofendido, ya que el sujeto pasivo es la persona sobre la cual recae la conducta de acción u omisión que realiza el sujeto activo y ofendido es

---

[139] PAVÓN VASCONCELOS, FRANCISCO. Op. Cit. pp. 17

[140] CUELLO CALÓN, EUGENIO; "DERECHO PENAL I", Décimo octava edición; Barcelona 1981 pp. 315

la persona física o moral que reciente el daño causado por el sujeto activo. Sin embargo en algunas ocasiones el sujeto pasivo y el ofendido son la misma persona.

En este orden de ideas en el delito de acceso ilícito a sistemas y equipos de informática, es procedente afirmar que el sujeto pasivo puede ser las embajadas, empleados o servidores públicos federales, las dependencias de organismos descentralizados o empresas de participación estatal del Gobierno Federal.

f) Objeto material: El objeto material de un delito lo constituye la persona o cosa sobre quien recae el peligro o el daño, sobre la persona o cosa sobre quien recae de manera directa el acto o evento delictuoso. Dentro del delito en estudio se puede considerar como objeto material del delito la información contenida en sistemas o equipos de informática, protegida por algún mecanismo de seguridad.

g) Bien jurídico: "Sobre el patrimonio se han elaborado, fundamentalmente, dos conceptos, uno de carácter económico y el otro jurídico. Desde un punto de vista económico, patrimonio es, dice MAGGIORE, el conjunto de los bienes mediante los cuales el hombre satisface sus necesidades y, en sentido jurídico, agrega el mismo autor, es el conjunto de relaciones jurídicas económicamente valuables". [141]

Por otra parte en materia de derecho civil al patrimonio lo define como "el conjunto de bienes, derechos, obligaciones y cargas apreciables en dinero, que constituyen una universalidad jurídica y que pertenecen a una persona física o moral".[142]

"El patrimonio, penalísticamente concebido, está, pues, constituido con aquel plexo de cosas y derechos destinado a satisfacer las necesidades humanas y sujeto al servicio de su titular. Integran el patrimonio todas aquellas cosas que pueden ser objeto de apropiación. Cuando esta posibilidad deviene en realidad, se

---

[141] PAVÓN VASCONCELOS, FRANCISCO; "DELITO CONTRA EL PATRIMONIO"", Ed. Porrúa, México 2001; primera edición pp 13

[142] REYNOSO DAVILA; ROBERTO "DELITOS PATRIMONIALES"; Ed. Porrúa, Méx. 1999, primera edición pp 1

muta la cualidad del objeto, pues las cosas y los derechos se transforman en bienes patrimoniales. Jiménez Huerta".[143]

De lo anterior se puede afirmar que la información es un bien jurídico de carácter patrimonial en razón de que pueda ser utilizada por el titular de la misma en su diivulgación o explotación e incluso con carácter eminentemente económico, concepto de patrimonio que entendemos como "el conjunto de bienes, derechos y obligaciones de una persona, pecuniarios o morales, que forman una universalidad de derecho".[144]

El bien jurídico "es el interés jurídicamente tutelado por la ley",[145] en este orden de ideas podemos decir que el bien jurídico protegido es el bien salvaguardado por el Estado mediante la creación de la ley penal, con el propósito de resguardarlo y protegerlo de las conductas ilícitas, motivo por el cual se puede afirmar que el objeto jurídico protegido en el delito contemplado en el artículo 211 bis 1 párrafo primero del Código Penal Federal es el patrimonio.

h) Medios: En el delito de acceso ilícito a sistemas y equipos de informática, los medios utilizados para llevar a cabo la modificación, pérdida o destrucción de la información, son el sistema y equipo de informática. Por otra parte puede ser cualquier medio idóneo que pueda causar un mal funcionamiento o incluso la destrucción de una computadora ya que con ello se puede llevar a cabo la pérdida o destrucción de la información que se encuentre protegida por algún mecanismo de seguridad.

i) Circunstancias:.

- De tiempo: No exige ninguna circunstancia de tiempo.
- De lugar: No se requiere de algún lugar en especifico.
- De ocasión: No se requiere ningún tipo de ocasión especifica.

---

[143] JIMENEZ HUERTA; MARIANO "DERECHO PENAL MEXICANO", Ed. Porrúa, séptima edición, México 2003, pp. 10-117

[144] GUTIÉRREZ Y GONZÁLEZ, ERNESTO. "DERECHO SUCESORIO, INTER.-VIVOS Y MORTIS CAUSA", sexta edición . Porrúa, México 2002.pp. 55

[145] AMUCHATEGUI REQUENA, IRMA G; "DERECHO PENAL". Segunda edición. Colección de textos Jurídicos universitarios, Editorial Oxford. México 2002 pp. 37

Sin embargo dichas circunstancias deben ser idóneas

j) Elemento subjetivo específico: No requieren ningún elemento subjetivo.

k) Elemento normativo: Dentro de los elementos normativos del delito de acceso ilícito a sistemas y equipos de informática tenemos: autorización, modifique, destruya, sistema, equipos, informática, mecanismo.

3.5.3 ANTIJURIDICIDAD

Para el Maestro Pavón Vasconcelos la antijuridicidad "es un desvalor jurídico, una contradicción o desacuerdo entre el hecho del hombre y las normas del Derecho".[146] Por su parte Raúl Carranca y Trujillo nos define la antijuridicidad como: "la oposición a las normas de cultura, reconocidas por el Estado."[147]

En otras palabras, la antijuridicidad es la incompatibilidad de una conducta hacia el orden jurídico establecido. Atento a lo anterior, "una acción es antijurídica cuando constituye un ataque a un bien jurídico (menoscabándolo, poniéndolo en peligro) protegido por el mandato, no se adecua a una finalidad admitida o impuesta por el derecho; en otras palabras: es antijurídico el ataque a un bien jurídico protegido, no admitido por el derecho".[148]

Franz Von Lisz y Cuello Calón han manifestado que la antijuridicidad maneja dos aspectos el formal y el material.

Formal: "cuando implique transgresión a una norma establecida por el Estado (oposición a la ley).

Material: Se presenta cuando la conducta ilícita signifique contradicción a los interese colectivos"; [149]

En otras palabras la antijuridicidad formal es la rebeldía contra la norma y la antijuridicidad material se presenta cuando dicha conducta ha causado un daño o perjuicio social por esa rebeldía.

---

[146] PAVÓN VASCONSELOS, FRANCISCO. Op. Cit. pp. 295
[147] CARRANCÁ Y TRUJILLO, RAÚL. Op. Cit. pp. 337
[148] MARTÍNEZ GARNELO, JESÚS. Op. Cit.pp. 22
[149] CASTELLANOS TENA, FERNANDO. Op. Cit. pp. 181

La antijuridicidad en el delito de acceso ilícito a sistemas y equipos de informática se va a presentar cuando el sujeto activo sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad lesionando el bien jurídico protegido por el Estado, que en este caso es la propiedad, además no debe encontrarse permitido por un ordenamiento legal.

3.5.4. IMPUTABILIDAD

Jiménez de Asúa explica qué "Imputar un hecho a un individuo es atribuírselo para hacerle sufrir las consecuencias, es decir, para hacerle responsable de el, puesto que de tal hecho es culpable".[150]

El Maestro Castellanos Tena, define la imputabilidad como "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 otras palabras, podemos definir la imputabilidad como la capacidad de entender y de querer en el campo del Derecho Penal".[151]

Por lo que en el delito en estudio la noción de imputabilidad no solo requiere el querer del sujeto, sino además su capacidad de entendimiento, ya que solo quien por su desarrollo y salud mental es capaz de representar el hecho, conocer su significación y mover su voluntad a la violación de la norma, puede ser reprochado en el juicio de la culpabilidad.

3.5.5. CULPABILIDAD

Una conducta no solo será delictuosa cuando sea típica y antijurídica, sino además debe existir una reprochabilidad hacia un sujeto por haber cometido un delito o haberse conducido contrario a la norma penal previamente establecida.

---

[150] JIMÉNEZ DE ASÚA; LUIS. Op. Cit. pp. 325
[151] CASTELLANOS TENA, FERNANDO. Op. Cit. pp. 218

Para Francisco Pavón Vasconcelos, la culpabilidad es "el reproche hecho al autor sobre su conducta antijurídica".[152] Castellanos Tena nos señala que la culpabilidad es "el nexo intelectual y emocional que liga al sujeto con su acto".[153] Y para Jiménez de Asúa se puede definir la culpabilidad como "el conjunto de presupuestos que fundamentan la reprochabilidad personal de la conducta antijurídica".[154]

El elemento de la culpabilidad se manifiesta de las siguientes formas:

a) El dolo. Se presenta cuando el sujeto activo realiza una conducta voluntaria con el propósito de realizar un daño o cometer un delito, es decir: "el sujeto activo ha representado en su mente la conducta que va a realizar y el resultado de esa conducta y decide en su acto la voluntad de llevar a cabo lo que en su mente representa".[155] Sus elementos son:

Elemento emocional o ético: Esta constituido por la conciencia de que se quebranta el deber.

Elemento volitivo o psicológico: "Consiste en la voluntad de realizar el acto; en la volición del hecho típico.

El dolo se clasifica en:

1. Dolo directo: "Es aquel en el que el sujeto se representa el resultado penalmente tipificado y lo quiere. Hay voluntariedad en la conducta y querer del resultado. Según Cuello Calón el dolo directo se da cuando el resultado corresponde a la intención del agente;
2. Dolo eventual: Existe cuando el agente se representa como posible un resultado delictuoso, y a pesar de tal representación, no renuncia a la ejecución del hecho, aceptando sus consecuencias. Hay voluntariedad de la conducta y representación de la posibilidad del resultado; éste no se quiere directamente, pero tampoco se deja de

[152] PAVÓN VASCONSELOS; FRANCISCO. Op. Cit. pp. 359
[153] CASTELLANOS TENA; FERNANDO. Op. Cit. pp. 234
[154] JIMÉNEZ DE ASÚA; LUIS. Op. Cit 233
[155] MARTÍNEZ GARNELO, JESÚS. Op. Cit. pp. 31

querer, se menosprecia, que en última instancia equivale a aceptarlo". [156]

En el dolo directo el resultado es el mismo que hubiera previsto y deseado el sujeto activo de la conducta. y el dolo eventual se presenta cuando el sujeto desea cometer un delito, pero en caso de que presentarse la posibilidad de que aparecieran otros delitos, acepta que los mismos ocurran.

El dolo directo y el dolo eventual se encuentra regulado en el articulo 9 del Código Penal Federal.

b) La culpa. "Cuando el activo no desea realizar una conducta que lleve a un resultado delictivo, pero por un actuar impudente, negligente, carente de atención, cuidados y reflexión, verifica una conducta que produce un resultado previsible o no intencional".[157]

Los elementos de la culpa son los siguientes:

Una acción u omisión, consciente y voluntaria, pero no intencional.

"1. Cuando el agente está dominado por una fuerza, que lo obliga a hacer u omitir, falta la nota de voluntariedad, indispensable en toda imputación penal.

2. Que el agente realice el acto inicial, sin tomar aquellas cautelas o precauciones necesarias para evitar resultados lesivos. Si no ha previsto las consecuencias dañosas de su hecho, por que no ha querido preverlas como debía, ésta es la razón de su castigo.

3. El resultado dañoso debe ser previsible para el agente.

4. El resultado dañoso tiene que encajar en una figura legal delictiva, por muy grave que sea aquél; si no integra una infracción prevista en la ley, el agente no será penado, pues el hecho no es delictuoso.

5. Debe haber relación de causa a efecto entre el acto inicial y el resultado dañoso; esta relación ha de ser directa e inmediata."[158]

---

[156] CASTELLANOS TENA, FERNADO. Op. Cit. pp. 239
[157] MARTINEZ GARNELO; JESUS. Op. Cit. pp. 33
[158] MARQUEZ PIÑERO, RAFAEL. Op. Cit. pp. 299-300

Para Fernando Castellanos Tena los elementos de la culpa son: "por ser necesaria la conducta humana para la existencia del delito, ella constituirá el primer elemento; es decir un actuar voluntario (positivo o negativo), en segundo término que esa conducta voluntaria se realice sin las cautelas o precauciones exigidas por el Estado; tercero: los resultados del acto han de ser previsibles y evitables y tipificarse penalmente; por último, precisa una relación de causalidad entre el hacer o no hacer iniciales y el resultado no querido".[159]

Por lo que podemos decir que los elementos de la culpa son:

Acción u omisión

Incumplimiento o determinación de un deber de cuidado

Resultado típico, previsible y evitable,

Ausencia de voluntad de causar daño

Nexo causal entre la conducta y el resultado

La culpa se clasifica en:

a) Culpa consciente, con previsión o representación: "Existe cuando el agente ha previsto el resultado típico como posible, pero no solamente no lo quiere, sino que abriga la esperanza de que no ocurrirá.

b) Culpa inconsciente, sin previsión o sin representación: se presenta cuando no se prevé un resultado previsible. Existe voluntariedad de la conducta causal, pero no hay representación del resultado de naturaleza previsible". [160]

Es importante anotar lo que nos dice el Código Penal Federal en su artículo 9°, el cual a la letra dice:

"Artículo 9º. 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, y

Obra culposamente el que produce el resultado típico, que no previo siendo previsible o previó confiando en que no se produciría, en virtud de la violación a un

[159] CASTELLANOS TENA, FERNANDO. Op. Cit. pp. 249
[160] ibidem pp. 249

deber de cuidado, que debía podía observar según las circunstancias y condiciones personales." [161]

Por lo tanto una vez analizado el elemento de la culpabilidad, es pertinente señalar que en el delito que nos ocupa, para que exista una conducta culpable en el sujeto activo es necesaria la acción dolosa ya que debe de existir una voluntad por parte del infractor para cometer este tipo de delito, en otras palabras, debe de ser un dolo directo, toda vez que la persona que ejecuta el acto quiere realizar la conducta por lo que sabe exactamente que tipo de instrucciones le debe de dar a la computadora para obtener el resultado deseado, sin embargo también puede existir el dolo eventual cuando el sujeto activo modifique, dañe o provoque la perdida de la información que se encuentren protegida por algún mecanismo de seguridad, logrando violar ese mecanismo, solo con la inquietud de conocer la información contenida en ese sistema, aceptando ese resultado.

Por otra parte el delito en estudio no se encuentra contemplado dentro del articulo 60 del Código Penal Federal motivo por el cual no se puede sancionar de manera culposa .

3.6 ELEMENTOS NEGATIVOS DEL DELITO

Es la falta de alguno de los elementos positivos del delito

3.6.1 AUSENCIA DE CONDUCTA

Para la ejecución de un delito es necesaria la presencia de una conducta humana, y si ésta faltará; no se configuraría el delito.

"Es unánime el pensamiento, en el sentido de considerar como factores eliminatorios de la conducta a la vis maior (fuerza mayor) y a los movimientos reflejos. Entre nosotros estas causas adquieren carácter supra legal, por no estar expresamente detectadas en la ley, pero pueden operar, porque su presencia demuestra la falta del elemento volitivo, indispensable para la aparición de la conducta que, como hemos dicho, es siempre un comportamiento humano

[161] "CÓDIGO PENAL FEDERAL" . Op. Cit. pp. 3

voluntario. Solo resta añadir que la vis absoluta y la vis maior difieren por razón de su procedencia; la primera deriva del hombre y la segunda de la naturaleza, es decir, es energía no humana. Los actos reflejos son movimientos corporales involuntarios (si el sujeto puede controlarlos o por lo menos retardarlos, ya no funcionan como factores negativos del delito)"[162].

Ahora bien, una vez analizado lo anterior, en el delito en estudio la conducta siempre va a estar manifestada mediante una acción, y nunca por omisión, en razón de que forzosamente para el funcionamiento de una computadora, es indispensable que el hombre haga uso de ella (desde encenderla hasta apagarla), le señale una serie de instrucciones y ordenamientos técnicos y lógicos a través de los comandos, y una vez realizado esto, obtendrá el resultado físico, en el delito en estudio seria la destrucción modificación o la perdida de la información. Se puede observar que la relación de causalidad o el nexo causal si se presenta en los delitos informáticos, porque existe una conducta de hacer, y un resultado material.

En este orden de ideas, la ausencia de la conducta en el tipo penal del articulo 211 bis 1 del Código Penal Federal solo opera cuando existe vis absoluta, en razón de que para cometer esta conducta es necesario los conocimientos de informática, y por lo tanto puede presentarse la hipótesis en que un usuario tenga que realizar cierto tipo de conducta por causa de vis absoluta, y si somos extremistas, en el caso de que una persona en estado de hipnótico lleve a cabo una conducta delictiva, existe también una ausencia de conducta. Por lo tanto este elemento negativo si se presentan en éste delito.

3.6.2 ATIPICIDAD

La atipicidad se presenta cuando no se reúnen todos y cada uno de los elementos del tipo penal por lo que es el aspecto negativo del delito.

El Doctor Martínez Garnelo hace la distinción entre atipicidad y ausencia del tipo de la siguiente manera:

---

[162] CASTELLANO TENA, FERNANDO. Op. Cit. pp. 16

a) "Atipicidad: Supone una conducta que no llega a ser típica por falta de alguno o algunos de los elementos descriptivos del tipo, ya con referencia a calidades en los sujetos, de referencia temporales o espaciales, de elementos subjetivos, etc.

b) Ausencia de tipo: Esto presupone la ausencia total de la descripción. Se maneja cuando unánimemente se establece que no hay delito sin tipo legal, cuando el legislador no describe una conducta dentro de las leyes penales, tal conducta no es delito; hay ausencia del tipo, ya que no existe descripción legal de una conducta considerada como delictiva." [163]

En este orden de ideas podemos señalar que la atipicidad se va a presentar cuando aparezca algún elemento negativo del tipo penal como son:

a) Falta de conducta: Por lo que hace al delito de acceso ilícito a sistemas y equipos de informática la conducta no se va a presentar sino existe la acción para provocar la modificación, destrucción o la pérdida de la información contenida en sistemas o equipos de informática
b) Falta de resultado: se va a presentar cuando no exista un cambio en el mundo exterior.
c) Falta de nexo causal: No se va a presentar el nexo causal cuando no existe una relación entre la conducta por el sujeto activo y el resultado.
d) Falta de sujeto activo: Cuando no exista sujeto activo.
e) Falta de sujeto pasivo: Cuando no exista sujeto pasivo.
f) Falta de objeto material: Cuando no haya objeto material que en este caso es la información contenida en sistemas o equipos de informática.
g) Falta de bien jurídico tutelado por el Estado tanto en el delito de acceso ilícito a sistemas y equipos de informática y en el delito de daño a la propiedad ajena es el patrimonio.
h) Falta de medios idóneos para realizar el delito. Si no existen los medios idóneos para realizar el delito este no se producirá.

[163] MARTÍNEZ GARNELO, JESÚS. Op. Cit. pp. 15

i) Falta de circunstancias (tiempo, lugar, ocasión) Deben ser idóneas para realizar éstos delitos toda vez que no requieren ninguna circunstancia especial y a falta de circunstancias idóneas éstos no se producirán.

j) Falta de elemento subjetivo: No se requieren elementos subjetivos

k) Falta de elemento normativo: La atipicidad podría presentarse si no se presentaran los elementos normativos en el delito de acceso ilícito a sistemas y equipos de informática como son: autorización, modifique, destruya, sistema, equipos, informática, mecanismo.

3.6.3 CAUSAS DE JUSTIFICACIÓN

Cuando se presenta alguna causa o circunstancia en una conducta típica, imputable, punible pero exista ausencia de antijuridicidad o alguna causa de justificación, no se configura el delito por faltar este elemento imprescindible.

Las causa de justificación son "las que excluyen la antijuricidad de una conducta que puede subsumirse en un tipo legal; esto es, aquellos actos u omisiones que revisten aspecto de delito, figura delictiva, pero en los que falta, sin embargo, el carácter de ser antijurídicos, de contrarios al Derecho, que es el elemento más importante del crimen, las causas de justificación no son otra cosa que aquellos actos realizados conforme al Derecho."[164]

Son causas de justificación las siguientes:

a) Legítima defensa. "Es la repulsa de una agresión antijurídica y actual por el atacado o por terceras personas contra el agresor, sin traspasar la medida necesaria para la protección"[165]

La legitima defensa se encuentra regulada en el articulo 15 fracción IV del Código Penal Federal, establece que: "Se repela una agresión real, actual o inminente y sin derecho, en protección de bienes jurídicos propios o ajenos, siempre que exista necesidad de la defensa y racionalidad de los medios empleados y no medie provocación dolosa suficiente e inmediata

[164] JIMENEZ DE ASUA, LUIS. Op. Cit. pp. 284
[165] CASTELLANOS TENA, FERNANDO. Op. Cit. pp 191

por parte del agredido o de la persona a quien se defiende. Se presumirá como defensa legítima, salvo prueba en contrario, el hecho de causar daño a quien por cualquier medio trate de penetrar, sin derecho al hogar del agente, al de su familia, a sus dependencias o a los de cualquier persona que tenga la obligación de defender, al sitio donde se encuentren bienes propios o ajenos respecto de los que exista la misma obligación; o bien lo encuentren alguno de aquellos lugares en circunstancias tales que revelen la probabilidad de una agresión".[166]

La legitima defensa en el delito de acceso ilícito a sistemas y equipos de informática puede operar en cuanto se dañe la computadora y con ello se destruya o pierda la información contenida en ella, sin embargo no puede operar cuando esa perdida destrucción o modificación cuando el sujeto activo de instrucciones especificas a la computadora argumentando que se repele una agresión, real, actual o inminente y sin derecho, en protección de bienes jurídicos propios o ajenos, sin que medie provocación dolosa por parte del agredido, siempre que los medios empleados sean solo los necesarios para defenderse.

b) Estado de necesidad. "Es la situación en que se encuentre un sujeto en la que como medio necesario para evitar la pérdida de bienes jurídicos propios (o de un tercero en determinados casos), ataca a un bien jurídico extraño de menor cantidad que el que trata de salvar".[167]

Esta causa de justificación se encuentra previsto en el articulo 15 fracción V del Código Penal Federal "se obre por la necesidad de salvaguardar un bien jurídico propio o ajeno, de un peligro real actual o inminente no ocasionado dolosamente por el agente, lesionando otro bien de menor o igual valor que el salvaguardado, siempre que el peligro no sea

[166] AGENDA PENAL FEDERAL. Op. Cit. pp. 125
[167] MARTÍNEZ GARNELO, JESÚS. Op. Cit. pp.22

evitable por otros medios y el agente no tuviere el deber jurídico de afrontarlo".[168]

Por lo que hace al estado de necesidad en el delito de acceso ilícito a sistemas y equipos de informática se podría presentar toda vez que el sujeto activo al realizar su conducta lo hará por la necesidad de salvaguardar un bien jurídico propio o ajeno por ejemplo su vida ya que se encuentra amenazado de muerte siendo esto un peligro real actual o inminente el cual no fue ocasionado por él, lesionando así el bien jurídico tutelado del delito de acceso ilícito a sistemas y equipos de computo que en este caso es el patrimonio, toda vez que el peligro no es evitable por otros medios.

c) Cumplimiento de un deber. Se presenta cuando las personas en ejercicio de su función cumplen con la obligación que se encuentra consagrada en la ley, pero realizan un menoscabo en una esfera jurídica ajena.

El Cumplimiento de un deber se encuentra regulado en el articulo 15 fracción VI del Código Penal Federal mismo que establece: La acción o la omisión se realicen en cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional del medio empleado para cumplir el deber o ejercer el derecho y que este último no se realice con el solo propósito de perjudicar a otro.

Por lo que hace al cumplimiento de un deber tampoco puede operar esta causa de justificación toda vez que el sujeto activo no puede dañar o destruir una computadora e incluso no puede ingresar sin autorización a un sistema o equipo de informática y modificar, destruir o provocar la pérdida de información protegidos por algún mecanismo de seguridad, argumentando que lo hizo para cumplir un deber o ejercer un derecho, realizando con ello un detrimento patrimonial.

[168] AGENDA PENAL FEDERAL. Op. Cit. pp. 125

d) Consentimiento del interesado. Contemplado en el artículo 15 fracción III del Código Penal Federal, el cual a la letra dice:

Se actúe con el consentimiento del titular del bien jurídico afectado, siempre que se llenen los siguientes requisitos:

a) Que el bien jurídico sea disponible;
b) Que el titular del bien tenga la capacidad jurídica para disponer libremente del mismo;
c) Que el consentimiento sea expreso o tácito y sin que medie algún vicio; o bien, que el hecho se realice en circunstancias tales que permitan fundadamente presumir que, de haberse consultado al titular, éste hubiese otorgado el mismo.[169]

Esta causa de justificación si puede operar toda vez que el tipo penal establece que al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática, cuando se tuviera el consentimiento ya sea expreso o tácito, del titular del bien jurídico que en este caso es el patrimonio, aunado a que este bien es disponible que el titular tenga la capacidad jurídica de disponer del mismo.

3.6.4. INIMPUTABILIDAD

El maestro Pavón Vasconcelos, define a la inimputabilidad, como "la incapacidad para conocer la ilicitud del hecho o bien para determinarse en forma espontánea conforme a esa comprensión".[170] Para Fernando Castellanos Tena nos dice que las causas de inimputabilidad son "todas aquellas capaces de anular o neutralizar, ya sea el desarrollo o la salud de la mente, en cuyo caso el sujeto carece de aptitud psicológica para la delictuosidad".[171]

Las causas de inimputabilidad son las siguientes:

---

[169] AGENDA PENAL FEDERAL. Op. Cit. pp. 125
[170] PAVÓN VASCONCELOS. Op. Cit. pp 375
[171] CASTELLANOS TENA, FERNANDO. Op. Cit. pp. 223

a) Minoría de edad. "Se considera que los menores de edad carecen de madurez y por tanto, de capacidad para entender y querer" [172]

De conformidad con el articulo 4° párrafo segundo de la Ley para el tratamiento de menores infractores para el Distrito Federal en materia común y para toda la República en materia Federal; el cual nos señala que "Respecto de los actos u omisiones de menores de 18 dieciocho años que se encuentren tipificados en las leyes penales federales, podrán conocer los consejos o tribunales locales para menores del lugar donde se hubiere realizado, conforme a los convenios que al efecto celebren la Federación y los gobiernos de los Estados".[173]

Así mismo el artículo 6° del mismo ordenamiento, el cual establece el Consejo de Menores es competente para conocer de la conducta de las personas mayores de 11 y menores de 18 años de edad, tipificada por las leyes penales señaladas en el artículo 1° de esta Ley. Los menores de 11 años, serán sujetos de asistencia social por parte de las instituciones de los sectores público, social y privado que se ocupen de esta materia las cuales se constituirán en este aspecto, como auxiliares del Consejo". [174]

Esta causa de inimputabilidad si puede operar ya que por el tiempo en que vivimos el sujeto activo muchas veces es menor de edad ya que son los que se encuentran mas relacionados con la informática.

b) Trastorno mental. El trastorno mental incluye cualquier alteración o mal funcionamiento de las facultades psíquicas, siempre que impidan al agente comprender el carácter ilícito del hecho o conducirse acorde con esa comprensión. Puede ser transitorio o permanente, por ingestión de alguna sustancia nociva o por un proceso patológico. Sólo se excluye el caso en que el propio sujeto haya provocado esa incapacidad, ya sea intencional o imprudencialmente.

---

[172] AMUCHATEGUI REQUENA, IRMA G. Op. Cit. pp. 83
[173] AGENDA PENAL FEDERAL. Op. Cit. pp. 299
[174] ibidem pp. 299

El trastorno mental puede operar en cuanto se destruya la computadora o se dañe el hardware provocando con ello la modificación, destrucción o perdida de la información, por lo que hace que el sujeto activo le de instrucciones a la computadora no puede operar el trastorno mental toda vez que como ya lo hemos visto en diversas ocasiones el sujeto activo requiere de conocimientos de informática para provocar una modificación, destrucción o provocar la pérdida de la información contenida en un sistema o equipo de informática protegido por algún mecanismo de seguridad y no cualquier persona y menos aun, alguien que tenga trastorno mental puede ingresar a un equipo protegido por un sistema de seguridad aunado a que sea sin autorización, y que dicha persona no se puede conducir acorde con esa comprensión, provocando con ello al sujeto activo la incapacidad para entender y querer.

c) Desarrollo intelectual retardado. Es un proceso tardío de la inteligencia, que provoca incapacidad para entender y querer. La sordomudez será causa de inimputabilidad sólo si el sujeto carece de capacidad para entender y querer.

También puede operar en caso de que alguna persona con desarrollo intelectual retardado daño una computadora o el hardware para su funcionamiento, sin embargo no puede operar esta causa de justificación si se trata de dar instrucciones a la computadora toda vez que el sujeto activo si tiene la capacidad para entender y querer y conducirse con esa compresión.

Tanto el trastorno mental y el desarrollo intelectual retardado se encuentra regulado en la fracción VII del artículo 15 del Código Penal Federal.

En el delito en estudio podemos señalar que de las causas de inimputabilidad se da la minoría de edad ya que por el tiempo en que vivimos el sujeto activo muchas veces es menor de edad ya que son los que se encuentran mas relacionadas con la informática.

3.6.5. INCULPABILIDAD

Es el aspecto negativo de la culpabilidad.

Jiménez de Asúa define a la inculpabilidad como "la absolución del sujeto en el juicio de reproche".[175]

El maestro Fernando Castellanos Tena dice que la inculpabilidad "opera al hallarse ausentes los elementos esenciales de la culpabilidad: conocimiento y voluntad. Tampoco será culpable una conducta si falta alguno de los otros elementos del delito, o la imputabilidad del sujeto, porque si el delito integra un todo, solo existirá mediante la conjugación de los caracteres constitutivos de esencia".[176]

Las causas de inculpabilidad mas frecuentes en el ámbito jurídico son las que se mencionan a continuación:

A. El error: "Es un vicio psicológico consistente en la falta de conformidad entre el sujeto cognoscente y el objeto conocido, tal como este es en la realidad. El error es un falso conocimiento de la verdad, un conocimiento incorrecto; se conoce, pero se conoce equivocadamente."[177]

El error se subdivide en error de hecho y error de derecho.

Error de hecho o error facti "es el error que recae sobre el resultado o las circunstancias determinantes de éste; en tanto que el error iuris, o error de derecho es el que recae sobre la significación o valoración jurídica acerca de esa conducta y su resultado; es decir, la persona no sabe que su conducta y su resultado implican la violación de la ley penal y por tanto, que suponen un delito".[178]

Por lo que podemos decir que el error de derecho es cuando el sujeto activo actúa de manera antijurídica creyendo que lo hace lícitamente, y el error de hecho se presenta cuando el sujeto confunde la finalidad de su conducta, o el objeto jurídico protegido no es el mismo que pretende quebrantar el sujeto activo.

---

[175] JIMÉNEZ DE ASÚA, LUIS. Op. Cit. pp. 399
[176] CASTELLANOS TENA, FERNANDO. Op. Cit. pp 257
[177] ibidem. pp. 259
[178] MALO CAMACHO, GUSTAVO; "DERECHO PENAL MEXICANO", Ed. Porrúa, México 2003, quinta edición pp 714

El error de tipo y el error de prohibición se encuentra regulado en el articulo 15 fracción VIII del Código Penal Federal , el cual a la letra dice:

"Se realice la acción o la omisión bajo un error invencible:

A) sobre alguno de los elementos esenciales que integran el tipo penal; o

B) Respecto de la ilícitud de la conducta ya sea porque el sujeto desconozca la existencia de la ley o el alcance de la misma, o porque crea que esta justificada su conducta".[179]

Por lo tanto se puede hablar del error vencible y del error esencial invencible.

Error esencial vencible es "cuando subsiste la culpa a pesar del error.

Error esencial invencible es cuando no hay culpabilidad. Este error constituye una causa de inculpabilidad". [180]

El error de prohibición en el delito en estudio si puede operar toda vez que el sujeto activo puede realizar su conducta respecto de los elementos esenciales que integran el tipo penal, al realizarla cuando esta siendo autorizado para realizar la modificación, destrucción o perdida de la información, sin embargo la persona que le dio esa autorización no es quien debía hacerlo; y en cuando al error de prohibición el sujeto activo no puede pensar que su conducta es lícita, si ingresa a un sistema o equipo de informática sin autorización. Sin embargo si puede operar el error de prohibición cuando el sujeto activo destruye la computadora o el hardware para su funcionamiento pensando que dicha computadora al igual que la información contenida en ella es de su propiedad, por lo que puede pensar que su conducta es lícita.

B. Caso fortuito. Se encuentra regulada en la fracción X del Código Penal Federal. Se refiere cuando una persona produce un resultado por un accidente, no se encuentra presente la voluntad del agente.

En el delito de acceso ilícito a sistemas y equipos de informática, no se puede dar el caso fortuito toda vez que el sujeto activo no puede realizar la

---

[179] "AGENDA PENAL FEDERAL Y DEL DISTRITO FEDERAL" . Op. Cit. pp. 125

[180] AMUCHATEGUI REQUENA, IRMA G. Op. Cit. pp. 90

conducta tomando todas las medidas necesarias para no provocar el delito toda vez que debe dar instrucciones a la computadora para que ésta ejecute las ordenes enviadas, por lo que necesariamente se deben de realizar actos tendientes a modificar, destruir o provocar la pérdida de información protegidos por algún mecanismo de seguridad. Pero si nos referimos a que la información es destruida o se provoca la perdida de la misma a través de dañar o destruir algún hardware necesario para su funcionamiento o la computadora misma si puede operar el caso fortuito.

C. No exigibilidad de otra conducta. Esta causa de inculpabilidad se encuentra regulada en la fracción IX del Código Penal Federal, el cual a la letra dice: Atentas la circunstancia que concurren en la realización de una conducta ilícita, no sea racionalmente exigible al agente una conducta diversa a la que realizó, en virtud de no haberse podido determinar a actuar conforme a derecho.

No puede operar esta causa de inculpabilidad toda vez que no existen circunstancias que al sujeto activo lo lleven a realizar éste delito motivo por el cual si se le puede exigir conducirse conforme a derecho.

CAPÍTULO 4 ELEMENTOS DEL DELITO DE DAÑO EN PROPIEDAD AJENA

4.1. CONCEPTOS DAÑO, DESTRUCCIÓN Y DETERIORO

El delito que analizaremos en el presente capítulo es el delito de daño en propiedad ajena, abocándonos únicamente al artículo 399 del Código Penal Federal, el cual a la letra dice:"Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones del robo simple"[181].

A continuación mencionaremos las definiciones que dan los algunos autores respecto de lo que significa la palabra daño, destrucción y deterioro.

"La palabra daño deriva del frances antiguo dam, latin daummum, daño.

I. Perjuicio material o moral sufrido por una persona. El daño da lugar a la reparación cuando resulta del incumplimiento de una obligación contractual o legal, de un delito o cuasidelito, o de un hecho cuya responsabilidad es impuesta por la a una persona.

II. En sentido jurídico, Arturo Rocco ha definido el daño como la pérdida o disminución de un bien, el sacrificio o la restricción de un interés ajeno que la norma jurídica garantiza, sea objetivamente, respecto al sujeto (interés o bien jurídico), sea subjetivamente, en la forma de su derecho subjetivo concedido mediante el reconocimiento jurídico de la voluntad individual que el interés jurídico persigue. Para Carnelutti el daño no es sino la lesión de un interés y no la alteración de un bien ya que existe clara diferencia entre uno y otro concepto; en consecuencia, el daño es la disminución o afectación del interés". [182]

Por otra parte, "destruir una cosa tanto significa deshacerla, descomponer las partes que la integran, haciéndola inútil, como aniquilarla, en tanto deteriorar implica reducir su capacidad de servicio o hacerla inservible parcialmente sin destruirla, destrucción implica la acción de destruir, con el

---

[181] Op. cit; pp. 183

[182] VISION JURÍDICA. DIRCCIONARIO DE TERMINOS JURÍDICOS EDICIÓN 2003, VERSIÓN EN CD.

efecto de hacer insubsistente la cosa en su esencia, aunque no quede aniquilada en su materialidad, específica, en tanto deteriorar es estropear, menoscabar, echar a perder una cosa sin suprimir su existencia o disponibilidad total".[183]

Por su parte Griselda Amuchategui Requena, define el término dañar como "afectar la cosa, ya sea en forma total o parcial, se podría decir que dañar es el género y destruir y deteriorar son la especie.

Destruir: Se entiende como el daño o afectación total de la cosa, se destruye lo que pierde su integridad corpórea, lo que ya no tiene manera de ser arreglado.

Deteriorar: Es un daño o afectación parcial o reparable, equivale a una descompostura o alteración en la cosa, pero ésta puede volver a su estado anterior". [184]

Una vez analizadas éstas definiciones podemos decir que daño es causar una afectación a una cosa ya sea en parte o de forma total realizando con ello una disminución en el patrimonio de una persona.

Destruir: Es afectar una cosa en el sentido de que la misma deja de ser útil para lo que fue creado toda vez que no puede ser reparada, por que la misma se hace inservible para lo que fue creada.

Deteriorar: Es causar una alteración a una cosa quedando existente y la cual puede ser reparada y volver a su estado original.

4.2. CLASIFICACIÓN DEL DELITO

La clasificación del delito de daño en propiedad ajena:

1. Por la conducta: es de acción u omisión
2. Por el daño: de lesión
3. Por el resultado que produce: es de resultado material.

---

[183] PAVÓN VASCONCELOS, FRANCISCO. DICCIONARIO DE DERECHO PENAL, ED. Porrúa, 3° edición; México 2003, pp 276

[184] AMUCHATEGUI REQUENA, GRISELDA Op. Cit. pp. 457

4. Por su duración: es instantáneo.

5. Por la forma de persecución: es de querella

6. Por los sujetos que intervienen: es un delito unisubjetivo.

7. Por su autonomía: autónomo o independiente.

4.1. ELEMENTOS POSITIVOS DEL DELITO

Para que una acción u omisión sea considera como delito se deben de actualizar sus elementos positivos tales como:

1. Conducta
2. Tipicidad
3. Antijuridicidad
4. Imputabilidad
5. Culpabilidad

A continuación estudiaremos cada uno de estos elementos positivos en el delito de daño en propiedad ajena.

4.3.1. CONDUCTA

Como ya lo vimos en el capítulo anterior, la conducta es un comportamiento realizado por el hombre comportamiento: voluntario, de acción u omisión, encaminado a conseguir un propósito.

En el delito de daño en propiedad ajena la conducta puede ser de acción o de omisión, causando al ofendido una afectación al bien jurídicamente tutelado que en este caso es el patrimonio.

En este orden de ideas podemos decir que el delito en estudio es un delito de acción toda vez que implica un movimiento corporal voluntario para que se pueda llevar a cabo a través de un hacer, es decir, se debe de realizar una o varias actividades para poder provocar un daño, una destrucción o un deterioro de cosa ajena.

Puede ser también un delito de omisión, ya que por la abstención voluntaria de no hacer lo que se debía, se provoca el daño, la destrucción o deterioro de cosa ajena, es decir, se realiza a través de un incumplimiento del comportamiento en tal sentido de que esta inactividad por parte del activo repercute sobre un bien dañándolo, deteriorándolo o destruyéndolo.

4.1.2. TIPICIDAD

La tipicidad en el delito en estudio se va a dar cuando se reúnan todos los elementos del tipo penal establecido en el artículo 399 del Código Penal Federal, es decir, cuando alguna persona a través de cualquier medio idóneo cause algún daño, destrucción o deterioro de cosa ajena.

Es decir el delito de daño en propiedad ajena se va integrar cuando se den los elementos del tipo penal como son:

1. Conducta
2. Resultado
3. Nexo causal
4. Sujeto activo
5. Sujeto pasivo
6. Objeto materia
7. Bien jurídico tutelado
8. Medios utilizados
9. Circunstancias (tiempo lugar ocasión)
10. Elemento subjetivo
11. Elemento normativo

Por lo que analizaremos los elementos del tipo penal en el delito de daño en propiedad ajena:

1. Conducta: es realizar una acción u omisión para provocar un daño, una destrucción o deterioro de cosa ajena o propia en perjuicio de tercero.
2. Resultado: Por el resultado en el delito de daño en propiedad ajena hay un cambio en el mundo exterior.

3. Nexo Causal: Es la relación que existe entre la conducta y el resultado.
4. Sujeto activo: Dentro del tipo básico del delito de daño en propiedad ajena, el sujeto activo puede ser cualquier persona física, ya que no se requiere una calidad especifica para poder causar un daño destrucción o deterioro de cosa ajena.
5. Sujeto pasivo: Tampoco requiere ninguna calidad específica por lo que puede ser cualquier persona física o moral.
6. Objeto material: Es cualquier cosa ajena, ya que el Código Penal Federal no hace ninguna clase de distinción al respecto siempre que se dañe, se destruya o se deteriore.
7. Bien jurídico: Es la propiedad.
8. Medios: Es todo aquello que utiliza el sujeto activo para realizar el delito, pudiendo ser un palo, un vehículo, etc, en el delito de daño en propiedad ajena refiere que por cualquier medio idóneo se cause un daño, deterioro o destrucción de cosa ajena.
9. Circunstancias:

- De tiempo. No exige ninguna circunstancia de tiempo.
- De lugar: No requiere de ningún lugar en especifico.
- De ocasión: No requiere de ninguna ocasión especial.

10. Elemento subjetivo específico: No requiere un elemento subjetivo.
11. Elemento normativo: Requiere de elementos normativos toda vez que los términos daño, destrucción, deterioro requieren una valoración cultural y el término cosa requiere de una valoración jurídica.

De acuerdo a la clasificación de los tipos del delito de daño en propiedad ajena se clasifica de acuerdo a su:

1. Composición: Es normal toda vez que se encuentra conformado de elementos objetivos.

2. Ordenación metodológica: Es básico toda vez que es un tipo penal que constituye el fundamento de otro tipo.

3. Autonomía o independencia: Es un tipo autónomo o independiente toda vez que tiene vida propia.

4. Formulación: Es casuístico contiene varias hipótesis.

5. Daño que produce: Es un tipo de daño toda vez que protege al bien jurídicamente tutelado de la disminución o destrucción.

4.1.3. ANTIJURIDICIDAD

La antijuridicidad del tipo básico en el delito de daño en propiedad ajena se va a presentar cuando se lleve a cabo un daño, la destrucción o deterioro de cosa ajena, lesionando así el bien jurídico protegido por el Estado, que en este caso es la propiedad, además no debe encontrarse permitido por un ordenamiento legal.

4.1.4. IMPUTABILIDAD

La imputabilidad en el presente delito requiere el querer del sujeto activo para realizar un daño, destrucción o deterioro de una cosa ajena, debiendo tener capacidad para comprender y conducirse con arreglo a esa comprensión y así poder hacerlo responsable de la conducta que realiza.

4.1.5. CULPABILIDAD

Para que el sujeto activo en el presente delito sea responsable de la conducta realizada además de estar contemplada en un tipo penal debe de existir una reprochabilidad por haber cometido el delito de daño en propiedad ajena.

Por su culpabilidad el delito en estudio puede ser:

1. Doloso: El dolo se presenta cuando el sujeto activo voluntariamente realiza una de las conductas previstas en el articulo 399 del Código Penal Federal.

En el delito de daño en propiedad ajena se puede dar:

a) Dolo directo: Cuando el sujeto activo conoce que la conducta que va a realizar se encuentra tipificada en el delito de daño en propiedad ajena y aún así quiere el resultado.

b) Dolo eventual: En el delito de daño en propiedad ajena se puede dar toda vez que el sujeto activo preve el resultado y lo acepta.

El dolo directo y el dolo indirecto se encuentra regulado en el articulo 9 del Código Penal Federal.

2. También puede darse la culpa toda vez que el delito en estudio dentro del artículo 60 del Código Penal Federal, donde se establece que delitos pueden ser sancionados a través de la culpa.

Existen dos clases de culpa consciente y la culpa inconsciente, contemplada en el artículo 9 del Código Penal Federal.

a) La culpa consciente, con previsión o representación: Se va a presentar cuando el sujeto activo produce el delito de daño en propiedad ajena previendo como posible dicho resultado.

b) La culpa inconsciente, sin previsión o sin representación: Se presenta cuando no se prevé un resultado previsible, es decir el sujeto activo no prevé que su resultado producirá el delito de daño en propiedad ajena, sin embargo era posible prever dicha circunstancia.

4.4. ELEMENTOS NEGATIVOS DEL DELITO

Al hablar de los elementos negativos del delito por consecuencia se tendrá por inexistente éste, los elementos negativos son:

- Ausencia de conducta
- Atipicidad
- Causas de justificación
- Inimputabilidad
- Inculpabilidad

4.2.1 AUSENCIA DE CONDUCTA

Para la ejecución de un delito es necesaria la presencia de una conducta humana, y si ésta faltará; no se configuraría el delito.

Por lo que en delito de daño en propiedad ajena se requiere el elemento volitivo para que el sujeto activo del delito realice la conducta ya sea de acción u omisión ocasionando un daño, destrucción o deterioro de una cosa ajena, motivo por el cual en el delito en estudio puede operar la vis maior, la vis absoluta y los movimientos reflejos.

4.2.2. ATIPICIDAD

La atipicidad en el delito de daño en propiedad ajena se presenta cuando no se reúnen todos y cada uno de los elementos del tipo penal contemplado en el artículo 399 del Código Penal Federal, es decir que no se actualice alguna de las hipótesis contempladas en el delito de daño en propiedad ajena como son el daño, la destrucción o deterioro.

Por lo que la atipicidad se va a presentar cuando se aparezca algún elemento negativo del tipo penal como son:

1. Falta de conducta es decir sino existe la acción u omisión con la cual se destruya, dañe o deteriore una cosa ajena
2. Falta de resultado: Si no hay un cambio en el mundo exterior.
3. Falta de nexo causal: Si no existe una relación entre la conducta y el resultado.
4. Falta de sujeto activo
5. Falta de sujeto pasivo que en este caso seria la victima o el ofendido.
6. Falta de objeto material
8. Falta de bien jurídico tutelado por el Estado que en este caso es el patrimonio.
9. Falta de medios idóneos para realizar el delito.
10. Falta de circunstancias (tiempo, lugar, ocasión) idóneas para realizar el delito toda vez que no requiere ninguna circunstancia especial.
11. Falta de elemento subjetivo: Sin embargo el tipo básico en el delito de daño en propiedad ajena no requiere un elemento subjetivo especifico.

12. Falta de elemento normativo: Si no se dan los elementos normativos del delito de daño en propiedad ajena como son daño, destrucción, deterioro o cosa.

4.2.3. CAUSAS DE JUSTIFICACIÓN

Cuando exista la ausencia de antijuridicidad, es decir cuando aparezca alguna de las causas de justificación en el delito en estudio, no se configura éste, dentro de las cusas de justificación que pueden operar en el delito en estudio son:

1. Legítima defensa. Se encuentra regulada en el artículo 15 fracción IV del Código Penal Federal y en el delito de daño en propiedad ajena puede operar esta causa de justificación toda vez que cuando el sujeto activo provoca un daño, destrucción o deterioro de una cosa ajena por tratar de proteger bienes jurídicos propios o ajenos de una agresión real, actual o inminente la cual no este conforme a derecho, y no medie provocación de forma dolosa por parte del agredido o de la persona a quien se defiende.
2. Estado de necesidad. Se encuentra contemplado en el artículo 15 fracción V del Código Penal Federal, y en el delito de daño en propiedad ajena se va a dar cuando el sujeto activo dañe destruya o deteriore una cosa ajena por tratar de salvaguardar un bien jurídico propio o ajeno, de un peligro real, actual o inminente mismo que no fue ocasionado por él.
3. Cumplimiento de un deber. Puede operar en el delito en estudio y se presenta cuando una persona en ejercicio de su función cumple con una obligación consagrada en la ley, por ejemplo cuando un bombero trata de apagar un incendio y para ello tiene que dañar o destruir una puerta o cualquier otra cosa que le permita apagar el incendio.
4. Consentimiento del interesado. Es otra causa de antijuridicidad que puede operar en el delito de daño en propiedad ajena, cuando el propietario del bien disponible autoriza causar un daño, destrucción o deterioro a ese bien.

4.2.4. INIMPUTABILIDAD

Las causas de inimputabilidad que puede operar en el delito de daño en propiedad ajena son:

1. Minoría de edad. Puede darse toda vez que en el delito de daño en propiedad ajena el sujeto activo puede ser mayor de 11 años de edad y menor de 18 años de edad por lo que de ese ilícito conocerán los Consejos o Tribunales Locales para menores del lugar donde se hubiere realizado. Y los menores de 11 años de edad serán sujetos de asistencia social por parte de las instituciones de los sectores público, social y privado que se ocupen de esta materia las cuales se constituirán en este aspecto, como auxiliares del Consejo.
2. Trastorno mental. También puede operar en el delito en estudio y se va a presentar cuando el sujeto activo sea una persona que tenga cualquier tipo de alteración o mal funcionamiento de las facultades psíquicas, que le impidan comprender el carácter ilícito del hecho o conducirse acorde con esa comprensión, provocando al sujeto activo la incapacidad para entender y querer.
3. Desarrollo intelectual retardado. Puede operar en el delito en estudio y se va a presentar cuando el sujeto activo no tenga la capacidad para entender y querer.

4.2.5. INCULPABILIDAD

Es el aspecto negativo de la culpabilidad y las causas de inculpabilidad que pueden operar en delito en estudio son:

1. El error de tipo y el error de prohibición se encuentran regulados en el artículo 15 fracción VIII del Código Penal Federal, por lo que podemos decir que en el delito de daño en propiedad ajena puede operar el error de tipo toda vez que el sujeto activo puede realizar su conducta bajo un error invencible respecto de algunos de los elementos esenciales que integran el tipo penal, es decir que tenga un falso conocimiento respecto

de los elementos del tipo penal, asimismo puede operar el error de prohibición ya que el sujeto activo estima que su conducta es lícita toda vez que tiene un falso conocimiento de la realidad, puede presentarse cuando el sujeto activo al realizar su conducta la haga bajo una equivocada noción de la realidad dañando, destruyendo o deteriorando una cosa pensando que es suya.

2. Caso fortuito. En el delito de daño en propiedad ajena se puede dar el caso fortuito cuando el sujeto activo al realizar una conducta desencadena un resultado típico, siendo este el delito de daño en propiedad ajena, resultado que no pudo ser previsible ya que se tomaron todas las medidas necesarias para no provocarlo sin embargo por una causa ajena a la actuación del sujeto activo se provoco el delito.
3. No exigibilidad de otra conducta. Se encuentra regulada en el artículo 15 en su fracción IX del Código Penal Federal y también puede operar en delito en estudio cuando por las circunstancias en las que el sujeto activo realiza el delito de daño en propiedad ajena no pueda conducirse de una forma lícita.

CAPÍTULO 5 ELEMENTOS AFINES Y DIVERGENTES DEL DELITO DE ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA CON EL DELITO DE DAÑO EN PROPIEDAD AJENA

En el presente capítulo analizaremos los elementos afines y divergentes del delito de acceso ilícito a sistemas y equipos de informática previsto en el artículo 211 bis 1 párrafo primero con el delito de daño en propiedad ajena ambos del Código Penal Federal.

Comenzaremos a señalar que el delito de acceso ilícito a sistemas y equipos de informática previsto en el artículo 211 bis 1 párrafo primero del Código Penal Federal establece: "al que sin autorización modifique, destruya o provoque pérdida de información contenido en sistemas o equipos de informática protegidos por algún mecanismo de seguridad se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa."[185] Y el delito de daño en propiedad ajena en su artículo 399 del Código Penal Federal, establece: "Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones del robo simple"[186].

Como se puede observar el delito de acceso ilícito a sistemas y equipos de computo trata de proteger la información contenida en sistemas o equipos de computo, e indica al que sin autorización modifique, destruya o provoque la pérdida de la información, sin embargo se puede destruir la información, cuando uno destruye el hardware de una computadora, o cuando uno daña el hardware, por lo que al dañar o destruir el hardware estamos en presencia del delito de daño en propiedad ajena y no así del acceso ilícito a sistemas de informática.

A continuación analizaremos la clasificación de ambos delitos:

1. Por la conducta: es el delito de acceso ilícito a sistemas y equipos de informática es un delito de acción, en cambio en el delito de daño en propiedad ajena es un delito de acción u omisión.

[185] Op. Cit "AGENDA PENAL FEDERAL Y DEL DISTRITO FEDERAL"; Op.Cit pp. 152
[186] IBIDEM; pp. 183

2. Por el daño: ambos delitos son de lesión.
3. Por el resultado que produce: ambos delitos son de resultado material.
4. Por su duración: los delitos en estudio son instantáneos.
5. Por la forma de persecución: el delito de acceso ilícito a sistemas y equipos de informática es de oficio en cambio el delito de daño en propiedad ajena es un delito que se persigue por querella.
6. Por los sujetos que intervienen: ambos delitos son unisubjetivos.
7. Por su autonomía: ambos delitos son autónomos o independientes.

A continuación analizaremos las diferencias y similitudes de los elementos positivos del delito de acceso ilícito a sistemas y equipos de informática en relación con el delito de daño en propiedad ajena, los cuales a continuación se señalan:

1. Conducta
2. Tipicidad
3. Antijuridicidad
4. Imputabilidad
5. Culpabilidad

Como ya lo hemos vimos en capítulos anteriores, la conducta es un comportamiento realizado por el hombre comportamiento: voluntario, de acción u omisión, encaminado a conseguir un propósito.

Por lo que podemos decir que el delito de acceso ilícito a sistemas y equipos de informática es un delito de acción toda vez que se requiere la realización de un hacer voluntario y así poder llegar al resultado deseado que en este caso sería modificar, destruir o provocar la pérdida de información contenida en un sistema y equipo de informática.

En cambio como el delito de daño en propiedad ajena la conducta puede ser de acción o de omisión, es de acción toda vez que implica un movimiento corporal voluntario para que se pueda llevar a cabo a través de un hacer, es decir, se debe de realizar una o varias actividades para poder provocar un daño, una destrucción o un deterioro de cosa ajena y va a ser de omisión, ya que por la abstención voluntaria de no hacer lo que se debía, se provoca el daño, la destrucción o deterioro de cosa ajena, es decir, se realiza a través de un incumplimiento del comportamiento en tal sentido de que esta inactividad por parte del activo repercute sobre una cosa ajena dañándola, deteriorándola o destruyéndola.

La tipicidad en el delito de acceso ilícito a sistemas y equipos de informática se va a presentar cuando se reúnan todos los elementos del tipo penal contemplado en el artículo 211 bis 1 párrafo primero y en el delito de daño en propiedad cuando se reúnan todos los elementos del tipo penal establecido en el artículo 399 del Código Penal Federal

Por lo que a continuación los elementos del tipo penal tanto en el delito de acceso ilícito a sistemas y equipos de informática y en el delito de daño en propiedad ajena.

1. Conducta: En cuanto hace al delito de acceso ilícito a sistemas y equipos de informática, la conducta es de acción para que se modifique, destruya se provoque la pérdida de la información contenida en un sistemas y equipos de informática. Sin embargo la omisión no se puede dar toda vez que un dejar de hacer no puede ocasionar que se modifique, destruya o se provoque la perdida de la información, ya que es necesario darle siempre una instrucción a la computadora para que se actualice el delito contemplado en el artículo 211 bis 1 párrafo primero.

Por lo que hace al delito de daño en propiedad ajena la conducta es de acción u omisión para provocar un daño, una destrucción o deterioro de cosa ajena o propia en perjuicio de tercero.

2. Resultado: En el delito de acceso ilícito a sistemas y equipos de informática y el ilícito de daño en propiedad ajena en ambos hay un cambio en el mundo exterior.

4. Nexo Causal: Es la relación que existe entre la conducta realizada por el sujeto activo y el resultado.

En el tipo penal de acceso ilícito a sistemas y equipos de informática el nexo causal es la conducta de acción realizada por el sujeto activo para llevar a cabo el resultado material que en este caso es la modificación, destrucción o pérdida de la información contenida en un sistema de informática; y por lo que hace al delito de daño en propiedad ajena el nexo causal es la conducta de acción u omisión realizada por el sujeto activo y así provocar un cambio en el mundo exterior realizando un daño, destrucción o deterioro de una cosa.

5. Sujeto activo: Tanto en el delito de acceso ilícito a sistemas y equipos de informática como en el delito de daño en propiedad ajena, el sujeto activo puede ser cualquier persona física, ya que no se requiere una calidad especifica.
6. Sujeto pasivo: Es en quien recae la conducta del sujeto activo por lo que en ilícito de daño en propiedad ajena no hay sujeto pasivo sin embargo podemos decir que hay una victima que puede ser una persona física o moral y en el delito de acceso ilícito a sistemas de informática también existe un victima que en este caso será el titilar de la información contenida en un sistema o equipo de informática
7. Objeto material: Por cuanto hace al delito de acceso ilícito a sistemas y equipos de informática el objeto material es la información y en el delito de daño en propiedad ajena, en el tipo básico, el objeto material es cualquier cosa ajena, ya que el Código Penal Federal no hace ningún tipo de distinción al respecto.
8. Bien jurídico: En los delitos en estudio el bien jurídico tutelado es la propiedad.

9. Medios: En el delito de acceso ilícito a sistemas y equipos de informática los medios utilizados para llevar a cabo el delito son el sistema y equipo de informática, en cambio, en el delito de daño en propiedad ajena es todo aquello que utiliza el sujeto activo para realizar el delito, es decir cualquier medio idóneo se cause un daño, deterioro o destrucción de cosa ajena.

10. Circunstancias:

- De tiempo. Tanto en el delito de acceso ilícito a sistemas y equipos de informática y en el delito de daño en propiedad ajena no exige ninguna circunstancia de tiempo.
- De lugar: Tampoco en ninguno de los delitos mencionados se requiere de algún lugar en especifico.
- De ocasión: Al igual que no se requiere de ninguna ocasión especial en ninguno de los delitos en estudio.

11. Elemento subjetivo específico: Tanto el delito de acceso ilícito a sistemas y equipos de informática al igual que en el delito de daño en propiedad ajena especifico no requieren ningún elemento subjetivo.

12. Elemento normativo: Dentro de los elementos normativos del delito de acceso ilícito a sistemas y equipos de informática tenemos: autorización, modifique, destruya, sistema, equipos, informática, mecanismo y por lo que hace a los elementos normativos del delito de daño en propiedad ajena están: daño, destrucción, deterioro o cosa.

De acuerdo a la clasificación de los tipos en el delito de acceso ilícito a sistemas y equipos de informática y del delito de daño en propiedad ajena se clasifican de acuerdo a su:

1. Composición: Los delitos en estudio son anormales toda vez que se encuentran conformados de elementos objetivos.

2. Ordenación metodológica: Ambos delitos son básicos toda vez que son tipos penales que constituyen el fundamento de otro tipo.

3. Autonomía o independencia: Ambos delitos son autónomos o independientes toda vez que tiene vida propia.

Formulación: Los delitos en estudio son amplios.

4. Daño que produce: Ambos delitos por el tipo son de daño toda vez que protegen al bien jurídicamente tutelado de la disminución o destrucción.

La antijuridicidad en el delito de acceso ilícito a sistemas y equipos de informática se va a presentar cuando el sujeto activo sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad y en el delito de daño en propiedad ajena se va a presentar cuando se lleve a cabo un daño, la destrucción o deterioro de cosa ajena, lesionando en ambos delitos el bien jurídico protegido por el Estado, que en este caso es la propiedad, además no debe encontrarse permitido por un ordenamiento legal.

La imputabilidad tanto el delito de acceso ilícito a sistemas y equipos de informática y en el delito de daño en propiedad ajena se requiere el querer del sujeto activo y a su vez tener la capacidad para comprender y conducirse con arreglo a esa comprensión y así poder hacerlo responsable de la conducta que realiza.

En el delito de acceso ilícito a sistemas y equipos de informática, para que exista una conducta culpable en el sujeto activo es necesaria la acción dolosa ya que debe de existir una voluntad por parte del infractor para cometer este tipo de delito, en otras palabras, debe de ser un dolo directo, toda vez que la persona que ejecuta el acto quiere realizar la conducta por lo que sabe exactamente que tipo de instrucciones le debe de dar a la computadora para obtener el resultado deseado, sin embargo también puede existir el dolo eventual cuando el sujeto activo accese al sistema y equipo de informática que se encuentren protegidos por algún mecanismo de seguridad, logrando violar ese mecanismo, solo con la inquietud de conocer la información contenida en ese sistema, previendo que puede provocar la pérdida de la información aceptando ese resultado.

Por otra parte el delito que nos ocupa no se encuentra contemplado dentro del articulo 60 del Código Penal Federal motivo por el cual no se puede sancionar de manera culposa.

Por lo que respecta al delito de daño a la propiedad ajena para que su conducta sea culpable debe de existir una reprochabilidad por haber cometido el delito. Por su culpabilidad puede darse un dolo directo cuando el sujeto activo conoce que la conducta que va a realizar se encuentra tipificada en el delito de daño en propiedad ajena y aún así quiere el resultado y un dolo eventual toda vez que el sujeto activo prevé el resultado y lo acepta.

También en el delito de daño en propiedad ajena puede darse la culpa toda vez que el delito en estudio dentro del artículo 60 del Código Penal Federal, donde se establece que delitos pueden ser sancionados a través de la culpa y puede darse la culpa consciente e inconsciente.

Por lo que podemos concluir que en el delito de acceso ilícito a sistemas y equipos de informática puede darse y ser sancionado de forma dolosa, tanto el dolo directo como el dolo eventual, sin embargo el delito de daño en propiedad ajena se puede dar el dolo directo y el dolo eventual así como la culpa consciente e inconsciente.

A continuación analizaremos la diferencias y similitudes de los elementos negativos del delito de acceso ilícito a sistemas y equipos de informática y del daño en propiedad ajena, mismos que a continuación se enlistan:

- Ausencia de conducta
- Atipicidad
- Causas de justificación
- Inimputabilidad
- Inculpabilidad

Para la ejecución de un delito es necesaria la presencia de una conducta humana, y si ésta faltará; no se configuraría el delito.

Ahora bien, la conducta en el delito de acceso ilícito a sistemas y equipos de informática siempre va a estar manifestada mediante una acción, y nunca por omisión, en razón de que forzosamente para el funcionamiento de una computadora, es indispensable que el hombre haga uso de ella (desde encenderla hasta apagarla), le señale una serie de instrucciones y ordenamientos técnicos y lógicos a través de los comandos, y una vez realizado esto, obtendrá el resultado deseado que en este caso sería la destrucción modificación o la pérdida de la información. En este orden de ideas, la ausencia de la conducta en el tipo penal del articulo 211 bis 1 del Código Penal Federal solo opera cuando una persona en estado hipnótico lleve a cabo una conducta delictiva, existe también una ausencia de conducta. Por lo tanto este elemento negativo si se presentan en éste delito.

Por lo que respecta en delito de daño en propiedad ajena se requiere el elemento volitivo para que el sujeto activo del delito realice la conducta ya sea de acción u omisión ocasionando un daño, destrucción o deterioro de una cosa ajena, motivo por el cual en el delito en estudio puede operar la vis maior, la vis absoluta, los movimientos reflejos y el hipnotismo.

La atipicidad en los delitos en estudio se va a presentar cuando no se reúnen todos y cada uno de los elementos del tipo penal contemplado los artículos 211 bis 1 párrafo primero y en el artículo 399 del Código Penal Federal.

En este orden de ideas podemos señalar que la atipicidad se va a presentar cuando aparezca algún elemento negativo del tipo penal como son:

1. Falta de conducta: Por lo que hace al delito de acceso ilícito a sistemas y equipos de informátlca la conducta no se va a presentar sino existe la acción para provocar la modificación, destrucción o la pérdida de la información contenida en sistemas o equipos de informática y en el daño en propiedad ajena la falta de conducta se va a presentar cuando no exista la acción u omisión con la cual se destruya, dañe o deteriore una cosa ajena

2. Falta de resultado: En ambos delitos se va a presentar cuando no exista un cambio en el mundo exterior.

3. Falta de nexo causal: En los delitos en estudio no va a haber nexo causal cuando no existe una relación entre la conducta realizada por el sujeto activo y el resultado.
4. Falta de sujeto activo: En ambos delitos cuando no exista sujeto activo.
5. Falta de sujeto pasivo: Como ya lo hemos señalado el sujeto pasivo es la persona en quien recae la conducta, por lo tanto en ambos delitos no hay sujeto pasivo pero si hay una victima u ofendido.
6. Falta de objeto material: Tanto en el delito de acceso ilícito a sistemas y equipos de informática y en el delito de daño en propiedad ajena se presentara la atipicidad si no existe el objeto material que en el primer caso es la información contenida en sistemas o equipos de informática, y en el delito de daño en propiedad ajena es cualquier cosa que se dañe, destruya o deteriore.
7. Falta de bien jurídico tutelado por el Estado tanto en el delito de acceso ilícito a sistemas y equipos de informática y en el delito de daño a la propiedad ajena es el patrimonio.
8. Falta de medios idóneos para realizar el delito. En el delito de acceso ilícito a sistemas y equipos de informática y en el delito de daño en propiedad ajena si no existen los medios idóneos para realizar el delito este no se producirá.
9. Falta de circunstancias (tiempo, lugar, ocasión) tanto en el delito de acceso ilícito a sistemas y equipos de informática y en el delito de daño en propiedad ajena los circunstancias deben ser idóneas para realizar éstos delitos toda vez que no requieren ninguna circunstancia especial y a falta de circunstancias idóneas éstos no se producirán.
10. Falta de elemento subjetivo: No se requieren elementos subjetivos ni el delito de acceso ilícito a sistemas y equipos de informática.
11. Falta de elemento normativo: La atipicidad podría presentarse si no se presentaran los elementos normativos en el delito de acceso ilícito a sistemas y equipos de informática como son: autorización, modifique,

destruya, sistema, equipos, informática, mecanismo y por lo que hace al delito de daño en propiedad ajena también se podría presentar la atipicidad por la falta de sus elementos normativos tales como: daño, destrucción, deterioro o cosa.

Cuando exista la ausencia de antijuridicidad, es decir cuando aparezca alguna de las causas de justificación en el delito en estudio, no se configura éste, dentro de las causas de justificación que pueden operar en el delito en estudio son:

a) Legitima defensa.

b) Estado de necesidad.

c) Cumplimiento de un deber.

d) Consentimiento del interesado.

Por lo que a continuación analizaremos que causas de justificación pueden operar en el delito de acceso ilícito a sistemas y equipos de informática:

a) Legitima defensa. En el delito de acceso ilícito a sistemas y equipos de informática como ya lo analizamos si puede operar en cuanto se dañe la computadora y con ello se dañe o pierda la información contenida en ella, sin embargo, no puede operar cuando el sujeto activo de instrucciones especificas a la computadora argumentando que se repele una agresión, real, actual o inminente y sin derecho, en protección de bienes jurídicos propios o ajenos, sin que medie provocación dolosa por parte del agredido, siempre que los medios empleados sean solo los necesarios para defenderse.

b) Por lo que hace al estado de necesidad en el delito de acceso ilícito a sistemas y equipos de informática se podría presentar toda vez que el sujeto activo al realizar su conducta lo hará por la necesidad de salvaguardar un bien jurídico propio o ajeno por ejemplo su vida ya que se encuentra amenazado de muerte siendo esto un peligro real actual o inminente el cual no fue ocasionado por él, lesionando así el bien jurídico tutelado del delito de acceso ilícito a sistemas y equipos de computo que en

este caso es el patrimonio, toda vez que el peligro no es evitable por otros medios.

c) Cumplimiento de deber. No puede operar esta causa de justificación en el delito de acceso ilícito a sistemas y equipos de informática, toda vez que el sujeto activo no puede ingresar sin autorización a un sistema o equipo de informática y modificar, destruir o provocar la pérdida de información protegidos por algún mecanismo de seguridad, argumentando que lo hizo para cumplir un deber o ejercer un derecho, realizando con ello un detrimento patrimonial.

d) Consentimiento del interesado. Si puede operar esta causa de justificación toda vez que el tipo penal establece que al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática, cuando se tuviera el consentimiento ya sea expreso o tácito, del titular del bien jurídico que en este caso es el patrimonio, aunado a que este bien es disponible que el titular tenga la capacidad jurídica de disponer del mismo.

A continuación analizaremos las causas de justificación del delito de daño en propiedad ajena:

1. Legítima defensa. En el delito de daño en propiedad ajena puede operar esta causa de justificación toda vez que cuando el sujeto activo provoca un daño, destrucción o deterioro de una cosa ajena por tratar de proteger bienes jurídicos propios o ajenos de una agresión real, actual o inminente la cual no este conforme a derecho, y no medie provocación de forma dolosa por parte del agredido o de la persona a quien se defiende.
2. Estado de necesidad. Se encuentra contemplado en el artículo 15 fracción V del Código Penal Federal, y en el delito de daño en propiedad ajena se va a dar cuando el sujeto activo dañe destruya o deteriore una cosa ajena por tratar de salvaguardar un bien jurídico propio o ajeno,

de un peligro real, actual o inminente mismo que no fue ocasionado por él.

3. Cumplimiento de un deber. Puede operar en el delito en estudio y se presenta cuando una persona en ejercicio de su función cumple con una obligación consagrada en la ley, por ejemplo cuando un bombero trata de apagar un incendio y para ello tiene que dañar o destruir una puerta o cualquier otra cosa que le permita apagar el incendio.
4. Consentimiento del interesado. Es otra causa de antijuridicidad que puede operar en el delito de daño en propiedad ajena, cuando el propietario del bien disponible autoriza causar un daño, destrucción o deterioro a ese bien.

Por lo que podemos concluir que en el delito de acceso ilícito a sistemas y equipos de informática pueden operar como causa de justificación la legitima defensa, el estado de necesidad y el consentimiento del interesado y por lo que hace al delito de daño en propiedad ajena se puede dar la legitima defensa, el estado de necesidad, el cumplimiento de un derecho y el consentimiento del interesado.

Las causas de inimputabilidad son:

1. Minoría de edad
2. Trastorno mental
3. Desarrollo intelectual retardado

Por lo que a continuación analizaremos las causas de inimputabilidad que puede operar en el delito de acceso ilícito a sistemas y equipos de informática:

1. Minoría de edad. Si puede operar ya que por el tiempo en que vivimos el sujeto activo muchas veces es menor de edad ya que son los que se encuentran mas relacionados con la informática.
2. Trastorno mental. Puede operar en cuanto se destruya la computadora o se dañe el hardware provocando con ello la modificación, destrucción o perdida de la información, por lo que hace que el sujeto activo le de instrucciones a la computadora no puede operar el trastorno mental

toda vez que como ya lo hemos visto en diversas ocasiones el sujeto activo requiere de conocimientos de informática para provocar una modificación, destrucción o provocar la pérdida de la información contenida en un sistema o equipo de informática protegido por algún mecanismo de seguridad y no cualquier persona y menos aun, alguien que tenga trastorno mental puede ingresar a un equipo protegido por un sistema de seguridad aunado a que sea sin autorización, y que dicha persona no se puede conducir acorde con esa comprensión, provocando con ello al sujeto activo la incapacidad para entender y querer.

3. Desarrollo intelectual retardado. También puede operar en caso de que alguna persona con desarrollo intelectual retardado daño una computadora o el hardware para su funcionamiento, sin embargo no puede operar esta causa de justificación si se trata de dar instrucciones a la computadora toda vez que el sujeto activo si tiene la capacidad para entender y querer y conducirse con esa compresión.

Por lo que respecta al delito de daño en propiedad ajena analizaremos las causas de inimputabilidad:

1. Minoría de edad. También se puede dar en Puede darse toda vez que en el delito de daño en propiedad ajena el sujeto activo puede ser menor de 18 años de edad
2. Trastorno mental. También puede operar en el delito en estudio y se va a presentar cuando el sujeto activo sea una persona que tenga cualquier tipo de alteración o mal funcionamiento de las facultades psíquicas, que le impidan comprender el carácter ilícito del hecho o conducirse acorde con esa comprensión, provocando al sujeto activo la incapacidad para entender y querer.
3. Desarrollo intelectual retardado. Puede operar en el delito de daño a la propiedad y se va a presentar cuando el sujeto activo no tenga la capacidad para entender y querer.

Por lo que podemos concluir que tanto el delito de daño en propiedad ajena y acceso ilícito a sistemas y equipos de informática si pueden operar tanto la minoría de edad, el trastorno mental y el desarrollo intelectual retardado

A continuación analizaremos cuales son las causas de inculpabilidad que pueden operar en el delito de acceso ilícito a sistemas y equipos de informática son:

1. Error de prohibición si puede operar toda vez que el sujeto activo puede realizar su conducta respecto de los elementos esenciales que integran el tipo penal, al realizarla cuando esta siendo autorizado para realizar la modificación, destrucción o perdida de la información, sin embargo la persona que le dio esa autorización no es quien debía hacerlo; y en cuando al error de prohibición el sujeto activo no puede pensar que su conducta es lícita, si ingresa a un sistema o equipo de informática sin autorización. Sin embargo si puede operar el error de prohibición cuando el sujeto activo destruye la computadora o el hardware para su funcionamiento pensando que dicha computadora al igual que la información contenida en ella es de su propiedad, por lo que puede pensar que su conducta es lícita.

2. Caso fortuito. En el delito de acceso ilícito a sistemas y equipos de informática, no se puede dar el caso fortuito toda vez que el sujeto activo no puede realizar la conducta tomando todas las medidas necesarias para no provocar el delito toda vez que debe dar instrucciones a la computadora para que ésta ejecute las ordenes enviadas, por lo que necesariamente se deben de realizar actos tendientes a modificar, destruir o provocar la pérdida de información protegidos por algún mecanismo de seguridad. Pero si nos referimos a que la información es destruida o se provoca la perdida de la misma a través de dañar o destruir algún hardware necesario para su funcionamiento o la computadora misma si puede operar el caso fortuito.

3. No exigibilidad de otra conducta. En el delito de acceso ilícito a sistemas y equipos de informática no puede operar esta causa de inculpabilidad toda vez

que no existen circunstancias que al sujeto activo lo lleven a realizar éste delito motivo por el cual si se le puede exigir conducirse conforme a derecho.

Por lo que respecta al delito de daño en propiedad ajena las causas de inculpabilidad que pueden operar en delito en estudio son:

1. El error de tipo y el error de prohibición se encuentran regulados en el artículo 15 fracción VIII del Código Penal Federal, por lo que podemos decir que en el delito de daño en propiedad ajena puede operar el error de tipo toda vez que el sujeto activo puede realizar su conducta bajo un error invencible respecto de algunos de los elementos esenciales que integran el tipo penal, es decir que tenga un falso conocimiento respecto de los elementos del tipo penal, asimismo puede operar el error de prohibición ya que el sujeto activo estima que su conducta es lícita toda vez que tiene un falso conocimiento de la realidad, puede presentarse cuando el sujeto activo al realizar su conducta la haga bajo una equivocada noción de la realidad dañando, destruyendo o deteriorando una cosa pensando que es suya.

2. Caso fortuito. En el delito de daño en propiedad ajena se puede dar el caso fortuito cuando el sujeto activo al realizar una conducta desencadena un resultado típico, siendo este el delito de daño en propiedad ajena, resultado que no pudo ser previsible ya que se tomaron todas las medidas necesarias para no provocarlo sin embargo por una causa ajena a la actuación del sujeto activo se provoco el delito.

3. No exigibilidad de otra conducta. Se encuentra regulada en el artículo 15 en su fracción IX del Código Penal Federal y también puede operar en delito en estudio cuando por las circunstancias en las que el sujeto activo realiza el delito de daño en propiedad ajena no pueda conducirse de una forma lícita.

Por lo que en el delito de acceso ilícito a sistemas y equipos de informática solo puede operar el error de prohibición y el error de tipo y en el delito de daño a la propiedad pueden operar todos los casos de inculpabilidad.

CONCLUSIONES

PRIMERA. Como ya lo hemos visto la humanidad ha progresado con el uso de la computadora, en diferentes áreas de nuestras vidas cotidiana y con ello se ha simplificado un poco algunas de nuestras labores, utilizando de manera benéfica los avances derivados de la tecnología en sus diversas actividades y conforme trascurre el tiempo la tecnología cambia de una manera sorprendente por ejemplo lo que hoy es novedoso mañana es obsoleto,

SEGUNDA. Es necesario hoy en día buscar la forma de tipificar conductas que se realicen a través de una computadora y que estas conductas vayan en contra de intereses jurídicos, es decir, que el legislador trate de regular dichas conductas para proteger un bien jurídico que se dañe o lesione, toda vez que como se ha visto es poco lo que se ha legislado en cuanto a los llamados delitos informáticos, aunado a que únicamente el Distrito Federal y es Estado de Sinaloa han legislado sobre este punto.

TERCERA. Ha sido evidente que la sociedad ha utilizando 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 de los sistemas informáticos en general.

CUARTA. La tecnología trajo consigo varias ventajas y a pesar ser muy útil en la vida diaria de la sociedad, también trajo varias consecuencias como problemas económicos, sociales y políticos, por lo que es necesario actuar en conjunto tanto a nivel nacional e internacional a través de una cooperación, a efecto de llevar un adecuado desarrollo de las lesiones e instituciones que ataquen el uso y abuso de los sujetos activos que utilizan una computadora.

QUINTA. La falta de privacidad, que se refleja en la ausencia de protección contra la manipulación de datos personales y del rastreo de las actividades realizadas por el Internet, con las injerencia en la vida privada del usuario, como por ejemplo cuando se da respuesta a formularios que contiene datos personales para acceder a sitios restringidos o realizar transacciones comerciales en la red; existe también la ausencia de restringir las posibilidades técnicas de que alguien pueda recoger los datos incluidos en la informacion suministrada a cada computadora por el usuario, es decir la práctica de la substracción, modificación o borrado de la información almacenada en la computadora personal, pudiendo derivar en atentados contra la propiedad de bienes informáticos, como lo pudiesen ser la destrucción o daño de equipos, programas, archivos y colecciones de datos; y aun en contra de la propiedad intelectual mediante el copiado, transmisión, explotación, reproducción, venta, difusión, deformación, mutilación o modificación de obras protegidas por la legislación sobre derechos de autor.

SEXTA. El correo electrónico, puede ser utilizado para vender estupefacientes y como vía para el lavado de dinero, en las tiendas electrónicas, con una tarjeta bancaria, los compradores pueden pagar artículos que luego resultan de mala calidad o que nunca reciben, esos son delitos debidos a Internet, la cual simplemente es empleada para ilícitos que quizá de todos modos serían realizados o que han sido tipificados antes de que existiera la tecnología sin embargo hace posible la comunicación a través de ella, por otra parte se ha sabido de casos de personas que son atacadas cuando acuden a una cita con alguien o a quien conocieron a través de un chat.

SÉPTIMA. Los autores no concuerdan con cuentas generaciones de computadoras han existidos, sin embargo aparece una nueva generación hasta que se produce un nuevo cambio, por lo que el autor Gonzalo Ferreyra Cortes indica que nos encontramos en la sexta generación de computadoras, ya que actualmente las computadoras realizan un millón de operaciones por segundo.

OCTAVA. Es difícil concebir actualmente la vida sin la intervención que en ella tiene el uso de la informática, y al surgir ésta, surge el uso de las redes informáticas conocidas como Internet, red que interconecta a otras redes y computadoras en el ámbito internacional, utilizando en México, como medio de conexión. El Internet tiene como principal fin la trasmisión y recepción de información que se encuentra en el espacio telemático entre redes y usuarios, este espacio telemático o ciberespacio, es el espacio abstracto que contiene información, misma que es transmitida por medio de las redes de telecomunicaciones informáticas, es decir a través del Internet se puede tener contacto en cuestión de segundos con otros países, por lo que ha proliferado conductas delictivas.

NOVENA. Entre otras conductas que se pueden llevar a acabo a través de las páginas de Internet están las que se ofrecen servicios con algún costo, mismos que nunca se proporcionan; o ventas de productos realizadas por empresas inexistentes, con el único fin de obtener un provecho ilícito con perjuicio ajeno; también se evidencia en los envíos electrónicos de solicitudes, contratos, firmas y documentos falsificados con la intención de generar un perjuicio al titular, pudiendo de esta manera obtener un lucro indebido, conductas que actualmente se realizan por la tecnología que cada día avanza.

DÉCIMA. Internet, igual que todo medio de comunicación y todo espacio abierto a la interacción pública, ha sido empleada para propagar contenidos cuya divulgación , y ante su creación, son delictivos (por ejemplo y de manera destacada, la utilización de niños y niñas en imágenes de carácter pornográfico), hay delitos que aparentemente solo se cometen a través de las redes electrónicas, como la desviación de fondos de una cuenta bancaria a otra mediante la intromisión de algún especialista en informática en las bases de datos de una institución financiera, pero aunque tecnológicamente sofisticadas, ésas son

transgresiones que ya ocurrían con otros métodos, antes de Internet, el fraude y el robo siempre han existido.

DÉCIMA PRIMERA. Igual que hay quienes insultan amenazan por vía telefónica, el correo electrónico puede ser empleado para amagar y atemorizar. de igual manera que en la radio o la televisión es posible anunciar artículos cuya venta llega a constituir un fraude a los consumidores, en la red de redes hay estafas. no queremos restarle importancia a la comisión de delitos a través de Internet, sino insistir en que a través de ella pueden perpetrarse faltas que hace tiempo son padecidas en nuestras sociedades y de manera más amplia, por el género humano.

DÉCIMA SEGUNDA. Otras conductas que también se pueden realizar a través del Internet tenemos la piratería de programas computacionales principalmente, ya que son precisamente estos los que son copiados para después venderlos perjudicando esta conducta de manera notable a los titulares de los Derechos de Autor; ocasionando un clamor general no solo en nuestro país, sino en todo el mundo donde exista el Internet; también se puede llevar a cabo la difusión de contenidos ilegales como la pornografía; toda vez que existe una gran pugna por acabar o censurar por lo menos las páginas o sitios de la red, que contengan escenas pornográficas, ya que se queja la gente de que estos lugares deben terminar pues es un ataque a las buenas costumbres y a la moral; las sectas en el Internet es otro caso que se manifiesta, ya que la proliferación de sectas o religiones con tendencias satánicas o suicidas y quienes pertenecen a dichas sectas pueden realizar varias conductas ilícitas, las apuestas, la incitación a la prostitución ya que son bastantes las personas que ofrecen este tipo de servicios dentro de las páginas de Internet y el tráfico o venta de órganos humanos, compras-ventas de todo tipo de productos y mercancías que van desde aparatos industriales robados hasta la venta ilegal de armas, entre otros, los cuales se generan como consecuencia de que no existe una restricción en cuanto a la

información que pueda enviar el usuario a través del Internet, ya que basta su conexión para poder generar dichos contenidos y de esta manera exhibirlos en el ciberespacio al público de manera gratuita o restringida. La anterior relación nos muestra conductas antisociales que ya se daban antes de que surgiera el Internet, pero que se encuentran dentro de este medio para transformar o mejorar su operación, como las que constituyen fraudes, espionaje y falsificaciones.

DÉCIMA TERCERA. Encontramos actividades que nacen paralelamente con la aparición del Internet y que se relacionan con programas y documentos electrónicos, entre otras las que generan el acceso no autorizado, la destrucción de datos y la sustracción de información, mismas que deberían de estar debida y cuidadosamente reguladas; ahora bien, en virtud de que algunas de estas actividades no se encuentran insertas de manea especial en algún tipo penal, entonces únicamente se pueden considerar como actividades perjudiciales ya que por no ser atípicas no son delitos, y al describirlas, surgen entonces la necesidad de vincular estas actividades como una conducta que sea generadora de algún delito en atención a bienes jurídicos susceptibles de ser tutelados por la norma como lo es el patrimonio como bien jurídico.

DÉCIMA CUARTA. Por otra parte la falta de seguridad que existe en los contenidos e información al no ser manejados en forma adecuada pueden ser utilizados de manera indebida por sujetos preparados para ello, mediante conductas que buscan la filtración de información confidencial tal como lo son los datos personales, que van desde datos muy generales como el nombre, el domicilio, el estado civil, el sexo, la fecha y lugar de nacimiento; hasta datos más personales y específicos como lo pudieran ser: la historia clínica, las creencias religiosas, el modo de vida, las inclinaciones políticas, el historial bancario, los gustos y preferencias, la correspondencia por medio del correo electrónico, secretos profesionales o información reservada de una empresa al intercambiar datos en la red; la validación de identidad, es decir se busca hacerse pasar por una

persona, que realmente no es, la violación de seguridad en transacciones electrónicas en páginas o sitios comerciales y de servicios bancarios, la obtención clandestina de claves de acceso a sitios o páginas restringidas y falsificación de firmas electrónicas. Por lo que es necesario regular las conductas que actualmente se están llevando a cabo a través del avance de la tecnología.

DÉDIMA QUINTA. Con el crecimiento que hoy en día ha tenido el uso de las computadoras ha incrementado la necesidad de compartir recursos, utilizando mejor equipo y utilizando el trabajo de otros, creciendo así la necesidad de compartir y cooperar la gente involucrada y su necesidad de acceso rápido e intercambio de información; presentando nuevos problemas en la seguridad de la información.

DÉCIMA SEXTA. Las medidas de seguridad están orientadas a preservar la información, impidiendo cualquier intromisión que pudiera conducir a la destrucción o alteración de los archivos que forman la base de datos.

DÉCIMA SÉPTIMA. La seguridad se refiere al acceso ilegal a los archivos de la computadora en la red con el propósito de destruir, modificar o tener acceso a los datos sin permiso.

DÉCIMA OCTAVA. Los riesgos que puede sufrir la integridad de la información entre otros se encuentran los equipos con errores mecánicos, un error humano, virus, gamberrismo, los ataques de piratas informáticos y esto se hace para retar los sistemas de seguridad, encontrando así a los hacker, el Wracker, los lamber, los script kiddies, los phreaker, los craker.

DÉCIMA NOVENA. Existen algunas técnicas para poner en riesgo la información estas técnicas son: el sniffer, back door, spamming, cancelling.

VIGÉSIMA. Hoy día podemos contar con sistemas de seguridad para el acceso no autorizado entre estos se encuentran:; las claves de acceso, las tarjetas de contraseña, el contrafuegos, el cifrado, la técnica de firma electrónica, y contra el ataque de un virus existen los programas antivirus, no obstante ningún programa antivirus garantiza totalmente la protección al ataque de un virus.

VIGÉSIMA PRIMERA. Entre las categorías de los virus encontramos a los bug-ware, al caballo de troya, camaleón, las bombas lógica, el conejo, el gusano, el killer o retrovirus, el joke program, elk leopfrog o rana, la máscara, el mockinbird.

VIGÉSIMA SEGUNDA. Como sistema informático debemos entender a una red de computadora que trabajan bajo un mismo programa de datos, cuya información es compartida entre dos o mas de ellas, que cuenta con una central llamada servidor donde reside la información; el servidor es una computadora personalizada que administra y comparte recursos; y el equipo de informática lo será la computadora que no se encuentra conectada en red con otras computadoras o con un servidor que trabaja con su propio sistema y ella misma almacena su información.

VIGÉSIMA TERCERA. Ante la proliferación de los delitos informáticos, los cuales propician la aparición de nuevas lesiones de bienes jurídicos merecedores de una pena, surge la necesidad en nuestra legislación penal de tipificar este tipo de delitos, puesto que es vital tanto para la protección de los individuos como de las Instituciones financieras, gubernamentales y en general para todos aquellos que legalmente utilizan las computadoras.

VIGÉSIMA CUARTA. Sin embargo y toda vez que las acciones ilícitas cometidas por el mal uso o manejo de las computadoras, son muy complejas y a la vez múltiples, es menester particularizar lo mas posible tales conductas delictivas,

para que el juzgador al momento de aplicar la ley no aplique equivocadamente otros preceptos legales; es decir, no podemos elaborar tipos penales genéricos o que abarquen varias conductas ilícitas, sino que más bien tenemos que estatuir cada una de las acciones delictivas y enlazarlas a una sanción dependiendo del bien jurídico que se lesione.

VIGÉSIMA QUINTA. Por otra parte, el artículo 211 bis 1 en su párrafo primero señala "al que sin autorización modifique, destruya o provoque la perdida de la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad", pero al hablar de destruir estamos hablando propiamente del delito de daño a la propiedad, ya que como lo hemos visto dañar es causar una afectación a una cosa ya sea en parte o de forma total realizando con ello una disminución en el patrimonio de una persona, y no podemos decir que la información es una cosa, toda vez que no es tangible propiamente, es tangible hasta en tanto la información se encuentre impresa en una pagina o en un libro, o en su caso al poderla apreciar en el monitor de una computadora, por lo que podemos afirmar que si bien es cierto la información no se puede considerar como cosa, la información que se encuentra contenida dentro de un sistema, y dentro del almacenamiento de datos conocido como disco duro, éste si puede sufrir una alteración o destrucción de carácter físico, realizando así propiamente el delito de daño en propiedad ajena. Además de que para destruir o provocar la pérdida de la información contenida en algún sistema o equipo de computo se puede llevar a cabo al dañar el hardware de la computadora, a pesar de que ésta se encuentre protegida por algún mecanismo de seguridad, actualizándose el delito de daño en propiedad ajena y no el delito de acceso ilícito a sistemas y equipos de computo.

VIGÉSIMA SEXTA. Los sujetos activos de los delitos informáticos, son aquellas personas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, que dichos sujetos 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, por ejemplo los empleados de los bancos o casas de bolsa; o bien aunque no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos si son hábiles en el uso de los sistemas informáticos.

VIGÉSIMA SÉPTIMA. La información contenida en una base informática puede ser modificada mediante la intervención de un experto en informática que accese a la base de datos y modifique o provoque la perdida de los archivos informáticos que contengan alguna información en particular, así mismo la posibilidad de dañar los programas informáticos (software) se evidencia, ya que dichas conductas se pueden realizar con la intervención directa de una persona con conocimientos especiales en informática (craker, hacker, etc) modificando el mismo los archivos, o en su defecto mediante la colocación de programas conocidos como virus informáticos, a través de la red, a la computadora del pasivo o bien dejando en libertad al virus en las redes de telecomunicación para destruir los archivos y software de aquellos que se conecten a la red.

VIGÉSIMA OCTAVA. A través de los virus informáticos también la base de datos y el disco duro puede sufrir una alteración a su funcionamiento y como consecuencia del mismo provoca la modificación, destrucción o perdida de la información que en ella se encontraba, realizando así una disminución en el patrimonio de una persona, ya que un virus informáticos pueden contaminar a un gran número de computadoras, tienen efectos negativos y destructivos, puede infectar otros programas, suele pasar inadvertido hasta el momento de su propagación masiva y puede activarse con un suceso particular

VIGÉSIMA NOVENA. Como requisito indispensable para la integración del tipo, es necesario que la información se encuentre protegida por algún mecanismo de seguridad, es decir la acción de modificar destruir, conocer, copiar o provocar la

perdida, de la información del pasivo contenida en los sistemas informáticos o equipos de informática, y que no se encuentre protegidos por algún sistema de protección no será punible, recuso informático que la mayoría de las veces no tiene el usuario final, por lo que es necesario que se proteja todo tipo de información del particular contenida en sistemas informáticos o equipos de informática, este o no protegida por algún mecanismo de seguridad; esta modificación, o provocación de la perdida de la información puede ser realizada mediante la intervención a través de la Internet.

PROPUESTA

Se puede llevar a cabo el delito de acceso ilícito a sistemas y equipos de computo cuando se accesa a través de una computadora provocando con ello una modificación o perdida de la información protegida por algún sistema de seguridad ya sea a través de un virus, de técnicas para lograr un acceso a sistemas o equipos de computo, o simplemente dando instrucciones a la computadora para que lleve a cabo la modificación o la perdida de la información.

Sin embargo también se puede provocar la pérdida de la información contenida en un sistema o equipo de computo y la cual se encuentre protegida por algún mecanismo de seguridad cuando se ocasione un daño al hardware y en este caso estaríamos hablando del delito de daño en propiedad ajena por lo que es necesaria una reforma al artículo 211 bis 1 si lo que trata y lo que quiere proteger el legislador es la información que se encuentre dentro de una computadora y esta a su vez protegida por algún mecanismo de seguridad, de los accesos no autorizados de piratas informáticos o de cualquier persona con los conocimientos necesarios en informática que pueda llevar a cabo la modificación o pérdida de la información se debe incluir la palabra al que "accese", término que se utilizada en informática cuando una persona ingresa a un sistema.

Por otra parte se debe de derogar la palabra al que destruya, ya que al hablar de destruir nos encontramos ante el delito de daño en propiedad ajena, toda vez que al acceder no se puede destruir la información, solo se puede modificar y se puede perder, pero no destruir por que ésta palabra es utilizada para las cosas tangibles ya que se puede destruir aquello que pierde su integridad corpórea.

Además de que el tipo penal establece que la información debe de estar protegida por algún sistema de seguridad sin embargo es necesario que se proteja

todo tipo de información del particular contenida en sistemas informáticos o equipos de informática.

Motivo por el cual se propone la reforma al articulo 211 bis 1 párrafo primero, el cual deberá de ser: "al que accese y sin autorización de la persona que pueda darlo y modifique o provoque la pérdida de la información contenida en un sistemas o equipo de informática se le impondrá de dos años a seis años de prisión".

BIBLIOGRAFÍA

1. ANTONIO PRADO, PEDRO, **LA INFORMÁTICA Y EL ABOGADO** Ed. Abeledo-Perrot,, Buenos Aires, Argentina 1988

2. AMUCHATEGUI REQUENA, IRMA G; **DERECHO PENAL**, segunda edición , Ed. Oxford México 2002.

3. ARECHIGA GALLEGOS, RAFAEL, **INTRODUCCIÓN A LA INFORMATICA** Séptima Reimpresión Ed Limusa, México 1990,

4. CARRANCA Y TRUJILLO, RAÚL **DERECHO PENAL MEXICANO.** Parte general , vigésima segunda edición Ed. Porrúa, México 2004.

5 CASTELLANOS TENA, FERNANDO **LINEAMIENTOS ELEMENTALES DE DERECHO PENAL.** Parte General cuadragésimo quinta edición Ed. Porrúa, México 2004.

6. CLEMENTE DE BLAS, **GUÍA DEL USUARIOS**, Ed, Ra-Ma, primera edición, Madrid España 1990.

7. CUELLO CALÓN; EUGENIO **PARTE GENERAL TOMO I**; Bosch Casa Editorial, edición décimo octava, Barcelona 1981.

8.DE LA CUADRA, ENRIQUE **REGULACIÓN JURÍDICA DE LA INFORMÁTICA COMPUTACIONAL.** Temas de Derecho Año II No. 3.1987,Universidad Gabriela Mistral. Santiago de Chile

9. DE MARCELO RODAO, JESUS **PIRATAS CIBERNÉTICOS** Editorial Alfaomega, México 2002.

10 GARCIA MAYNEZ, EDUARDO, **INTRODUCCIÓN AL ESTUDIO DEL DERECHO.** Quincoagesima séptima edición. Ed. Porrúa, México 2004.

11. FERREYRA CORTÉS, GONZALO, **INFORMÁTICA, PASO A PASO,** Ed. Alfaomega, México 2000.

12. GATTON PIERRE, **"PROTECCIÓN INFORMÁTICA"**, Ed. Trillas, México 1998

13. GOMEZ QUINTANILLA, JOSÉ ARTURO **DERECHO PENAL MEXICANO PARTE GENERAL Y PARTE ESPECIAL.**

Séptima edición, México 2004.

14. GONZÁLEZ QUINTANILLA, JOSÉ ARTURO; **"DERECHO PENAL MEXICANO PARTE GENERAL"**, Ed. Porrúa, México 1991

15. GUTIÉRREZ Y GONZÁLEZ, ERNESTO. **DERECHO SUCESORIO, INTER.-VIVOS Y MORTIS CAUSA**, sexta edición . Porrúa, México 2002.

16. HERNÁNDEZ HERNÁNDEZ, ARTURO. **GUÍAS Y TEXTOS DE COMPUTO; VIRUS INFORMÁTICO**; Ed. Dirección General de Servicios de Cómputo Académico

17. JIMÉNEZ DE ASUA, LUIS; **PRINCIPIOS DEL DERECHO PENAL LA LEY Y EL DELITO**, Argentina 1990, cuarta edición Ed. Abelardo –Perrot.

18. M. FALCON, ENRIQUE **¿QUÉ ES LA INFORMÁTICA JURÍDICA? DEL ABACO AL DERECHO INFORMÁTICO** Ed.Abeledo-Perrot, Buenos Aires 1993.

19 MALO CAMACHO, GUSTAVO **DERECHO PENAL MEXICANA**

quinta edición, Ed. Porrúa, México 2003.

20. MARQUEZ PIÑERO, RAFAEL; **DERECHO PENAL PARTE GENERAL**, Ed. Truillas, quinta edición, México 1999.

21. MARTÍNEZ GARNELO, JESÚS: **LA INVESTIGACIÓN MINISTERIAL PREVIA**; Ed. CGS Editores.

22. PAVÓN VASCONCELOS, FRANCISCO **DELITOS CONTRA EL PATRIMONIO.** Décima edición, Ed. Porrúa , México de 2001.

23. PAVÓN VASCONCELOS, FRANCISCO. **DERECHO PENAL MEXICANO**; Décima Edición, S.A, Ed. Porrúa; México 1991

24. REYNOSO DAVILA; ROBERTO **"DELITOS PATRIMONIALES;** Ed. Porrúa, Méx. 1999

25. RODRÍGUEZ, LUIS ÁNGEL; **SEGURIDAD DE LA INFORMACIÓN EN SISTEMAS DE COMPUTO**, Ed. Ventura

26. SEOANE, JOSÉ ALBERTO **ACOSO DIGITAL: PREVENCIÓN Y ANTIDOTOS**; Ed. Macchi, México 2001

27. TÉLLEZ VALDEZ, JULIO, **DERECHO INFORMÁTICO**, Ed. Universidad Nacional Autónoma de México; México 1987

28. UREÑA LOPEZ, L. ALFONSO, **FUNDAMENTOS DE LA INFORMÁTICA**, Ed, Alfaomega, México 1999.

29. VILLANUEVA, ERNESTO **DERECHO COMPARADO DE LA INFORMACIÓN**, segunda edición; Ed. Porrúa; México 2002.

LEGISLACIÓN

CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS
Editorial Sista, México 2005.

AGENDA PENAL FEDERAL Y DE DF 2005
Editorial Raúl Juárez Carro Sociedad Anónima de Capital Variable México 2005

PAGINAS WEB

http://www. monogrfias.com/tabajos/marcohistocomp/marcohistocomp.shtml

http://www.cyberlatino.com.mx/info/pc/main.htm#COMPUTADORA

http://www.monografias.com/trabajos/refercomp/refercomp.shtml

www.tny.vasnet.mx/prof/cln/der/silvia/leyint.htm.

www.tny.vasnet.mx/prof/cln/der/silvia/leyint.htm.

www.mir.es/policia/viti/legisla.htm

http://tiny.uasnet.mx/prof/cln/der/silvia