UNIVERSIDAD LATINA

INCORPORADA A LA UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

DELITOS INFORMATICOS.

La Responsabilidad Penal de los Proveedores de Software ó Programas de Cómputo.

T E S I S

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN DERECHO

P R E S E N T A :

Antonio Muñoz Botello

Asesor: Lic. Aníbal Cuen Rodríguez

MEXICO, D.F. 2001

UNIVERSIDAD LATINA, S.C.

INCORPORADA A LA U.N.A.M.

Coyoacán México, 03 de Julio de 2001.

C. DIRECTOR GENERAL DE REVALIDACIÓN
E INCORPORACIÓN DE ESTUDIOS DE LA UNAM
P R E S E N T E:

El C. **MUÑOZ BOTELLO ANTONIO**, ha elaborado la tesis profesional titulada ***Delitos Informáticos. La responsabilidad penal de los proveedores de Software o rogramas de cómputo "***, bajo la dirección del **LIC. ANÍBAL GUILLERMO CUEN RODRÍGUEZ**, para obtener el Título de Licenciado en Derecho.

l alumno ha concluido la tesis de referencia, misma que llena a mi juicio los requisitos arcados en la Legislación Universitaria y en la normatividad escolar de la Universidad atina para las tesis profesionales, por lo que otorgo la aprobación correspondiente para todos s efectos académicos correspondientes.

ATENTAMENTE
"LUX VIA SAPIENTIAS"

LIC. SANDRA LUZ HERNÁNDEZ ESTÉVEZ
DIRECTORA TÉCNICA
LICENCIATURA EN DERECHO
CAMPUS SUR

México, D.F., a 27 de Marzo de 2001

LIC. SANDRA LUZ HERNÁNDEZ ESTÉVEZ
DIRECTORA TÉCNICA DE LA LICENCIATURA
EN DERECHO DE LA UNIVERSIDAD LATINA
P R E S E N T E.

Me dirijo a usted para hacer de su conocimiento que el alumno **ANTONIO MUÑOZ BOTELLO,** egresado de la Universidad Latina, S C. Campus Sur, con número de cuenta 94860078-8, que cursó en esta Institución la Licenciatura en Derecho, solicitó la asesoría del suscrito para que supervisara su trabajo de tesis titulado **"DELITOS INFORMÁTICOS, LA RESPONSABILIDAD PENAL DE LOS PROVEEDORES DE SOFTWARE O PROGRAMAS DE COMPUTO".**

El **C. ANTONIO MUÑOZ BOTELLO,** concluyó su trabajo, lo ha presentado y ha sido debidamente revisado por el suscrito, con la finalidad de que el mismo cumpla con los requisitos académicos necesarios.

Por lo antes expuesto, solicito a usted se sirva autorizar la revisión de la tesis en mención para sustentar el examen profesional.

Atentamente

LIC. ANÍBAL GUILLERMO CUEN RODRÍGUEZ
ASESOR DE TESIS.

A mis Padres. Por el apoyo incondicional de su parte, el cual ha sido siempre una fuente de fuerza por luchar y seguir siempre adelante, sus consejos fueron y seguiran siendo la base de mi formación tanto espiritual como humana. Gracias.

A mi esposa Adriana. Gracias por todo.

A mi hijo Maximiliano. Sigue tan saludable y sonriente como hasta ahora, pues es la mejor forma de demostrarnos tu felicidad.

A mis hermanos. Cada uno de ustedes contribuyeron para que se realizara este momento tan importante, cada uno de forma diferente, pero siempre valiosa para mi.

A mis sobrinos. El estudio constante y la dedicación al mismo, es la mejor forma de llegar a el triunfo, igualmente es el poder realizar cada uno de los sueños que se tienen durante toda esta etapa de desarrollo.

A la Biblioteca Lic. Emilio Portes Gil., de la Procuraduría General de la República, fuente inagotable de conocimientos, parte importante de mi vida y desarrollo profesional.

A mis compañeros de trabajo. Todos y cada uno de ustedes me ayudaron de distinta forma y sin condición alguna, logrando con esto el que haya podido llegar a esta meta tan importante. Gracias.

A mis compañeros y amigos de Licencitura. Vale la pena realizar un pequeño esfuerzo más.

DELITOS INFORMÁTICOS.

LA RESPONSABILIDAD PENAL

DE LOS PROVEEDORES DE SOFTWARE

O PROGRAMAS DE COMPUTO

INDICE

CAPÍTULO III

DELITOS INFORMÁTICOS

CAPÍTULO IV

PROTECCIÓN JURÍDICA DEL SOFTWARE NACIONAL E INTERNACIONALMENTE

CAPÍTULO V

CRIPTOLOGÍA, MARCO CONCEPTUAL Y CRÍTICA A DICHO SISTEMA

Introducción

Actualmente la era de la informática nos tiene atrapados, y sin salida alguna que nos proporcione el medio eficaz para evitar su uso. Al contrario, avanza sin mirar hacia atrás y sin contratiempo alguno, su marcha es a pasos gigantescos; la informática avanza a la par de la tecnología. Sin embargo, no todo este avance es para bien. Hemos visto que desde el inicio del auge informático, se han dado conductas que dañan los intereses de los sujetos que han creado, diseñado o inventado un sinnúmero de software y hardware, el cual ha sido protegido principalmente por la vía autoral, tratando de otorgarles un resguardo lo más seguro y total, pero hasta el momento no ha sido posible ofrecer la protección que se desea para evitar la delincuencia informática, las diversas conductas que representan una lacra del autor o titular de los derechos del programa o software y hardware.

En este sentido, me atrevo a decir que tal ineficiencia es producto de la equivocada política o línea que se ha seguido durante bastante tiempo, es decir, se ha tratado a estos ilícitos bajo el esquema clásico del delito –lo cual estaremos tratando y viendo en el transcurso del presente estudio–. Es un hecho que bajo el esquema clásico, este tipo de conductas no se han podido quitar del mapa informático; al contrario, han aumentado. Las medidas de seguridad y política criminal no han servido de mucho; por otro lado, el aumentar las penas y sanciones tampoco ha dado resultados satisfactorios. Como lo señalamos anteriormente, las erróneas formas de legislar para con estas conductas nos han dado el anterior resultado. Así pues, si se toman en cuenta el presente estudio y su propuesta puedo decir sin temor a equivovarme que varias conductas delictivas,

y en especial la de piratería de programas de software, se pueden controlar.

Desde que tomé mis primeros cursos de informática, y en particular de programación –así como algunos otros para tener una actualización constante–, me di cuenta del potencial técnico y científico que se les proporciona a los sujetos que adquieren estos conocimientos, así como del potencial criminológico que se obtiene o se crea al relacionar estos conocimientos con un sujeto capaz de adquirir y a la vez aplicar lo aprendido en cualquier tipo de circunstancias. El interés por la informática y especialmente por este tema nace como ya lo mencione anteriormente a partir de mis primeros estudios en computación, y posteriormente como programador en software de aplicación, donde me di cuenta de la potencialidad que tiene, en primera instancia, el programador ante una computadora, pues puede hacer que ésta haga casi cualquier cosa diseñando previamente un programa para determinadas necesidades o problemas a resolver, así como el crear o inventar equipo que trabaje conjuntamente con estos programas, formando un solo ente o medio criminológico; en segunda instancia, al considerar la potencialidad criminológica del conocedor quien, mediante sus conocimientos y contando con la computadora como medio, puede realizar acciones diversas, conductas que se encuentran ya tipificadas pero que por las características de su actuar y los medios empleados eran en un principio, imposible de detectar.

En la actualidad sigue siendo difícil, laborioso y algunas veces imposible castigar al autor ya sea intelectual o material. En tercera y última, aquella de los sujetos que tienen conocimientos básicos en informática así como de la computadora con sus componentes físicos necesarios y esenciales en la actualidad, con los cuales pueden llevar a cabo verdaderos actos vandálicos e inclusive dejar en ban-

carrota al empresario más prominente y viceversa. Es así como tuvimos la noción y posteriormente el ánimo de realizar la presente investigación y tratar de demostrar la responsabilidad penal del programador como partícipe principal dentro del delito de piratería.

Con lo anterior no quiero decir que estos sujetos son los únicos que realizan actos ilícitos o que son los autores intelectuales siempre, sino que forman parte importante de las empresas al ser ellos los que crean, inventan o desarrollan un programa llamado software así como también el hardware que ha de aplicar el software previamente diseñado.

En el caso de las empresas, estos sujetos muchas veces actúan por orden directa de su patrón o dueño de ésta, situación que pone en entredicho su culpabilidad como autores directos de algún acto nocivo o que ayuda y facilita la comisión de alguna conducta ilícita, pues ellos sólo cumplen órdenes o responden a peticiones de otras empresas que necesitan de este material informático, sin tomar en cuenta y realizar un previo análisis del alcance jurídico y especialmente penal, del uso del software o hardware creado o diseñado. Pareciera que estamos a pocos pasos de sacar a la venta el programa que tiene los medios idóneos para cometer algún delito –específicamente el de piratería en su modalidad de copia ilegal de software de computadora–, sin que exista alguna restricción para usuarios que no tienen la titularidad inicial para la cual fue creado el programa originalmente.

Es por lo anterior que hemos realizado el siguiente estudio sobre los delitos informáticos, buscando tratar en él las diversas áreas y estructuras de la informática y el Derecho, teniendo como antecedente la interrelación de que son objeto éstos dos y generando lo que conocemos como el Derecho Informático. No analizaremos totalmen-

te las diferentes ramas o apartados que lo conforman, sólo aquellas que son importantes para nuestra tesis y, consecuentemente las que mencionan o tienen alguna relación con los proveedores y su responsabilidad.

Es importante señalar que hemos realizado el presente trabajo de una forma tal que podamos primeramente darnos cuenta y entender a la informática, sus principios, sus características, su relación con el derecho y seguidamente al propio derecho informático como una rama jurídica que tiende a ser independiente con sus principios, sus características y su relación con la regulación inminente de las conductas que se dan con la aplicación de los diversos medios informáticos.

Igualmente de importante es el mencionar que el desarrollo que le hemos dado es para tener un amplio panorama de los delitos informáticos en todos los posibles aspectos que nos pudieran dar y que de hecho lo hacen, las bases para fundamentar a la presente tesis y su propuesta; así pues una vez ya conocidos los anteriores temas podremos entender por que tratamos como responsables de una conducta indebida a los sujetos propuestos en nuestro trabajo y por que a la vez se les considera como los intocables, así como los sujetos a los cuales se les daña su patrimonio, tratando por ende la autoridad de proteger siempre sus derechos principalmente intelectuales, sin considerar hasta este momento que ellos tienen una responsabilidad grande la cual se puede ver poniendo sólo un poco de atención a su trabajo, el fin de esté, y a la vez que nuestros legisladores conozcan más a fondo el tema, que se alleguen en dado caso de personas expertas en este rubro, así como de personas que tengan la capacidad para entender la interrelación del derecho y la informática, la forma de en que se comenten las conductas y la forma en que se utiliza al equipo informático, tanto como medio para co-

meter el ilícito como el fin de dicha acción. Es de esta forma como tratamos de dar al lector una visión amplia de la forma en que se realizó el presente estudio, tratando de que siempre este presente el análisis de la conducta de los sujetos a tipificar.

En el primer capítulo hacemos el análisis histórico de la computadora, sus características principales, su desarrollo y su estado actual, la cibernética, y de igual forma la informática, con el fin de que podamos tener un amplio panorama de la forma en que se fue dando, creando, moldeando la historia de la informática actual, así como de la tecnología aplicada a la misma, para poder comprender de manera más completa a los hechos, el por qué y el cómo es que los programadores –ya sea al servicio de otros o por si mismos– deben de tener responsabilidad ante el Derecho, por su conducta omisiva.

En nuestro segundo capítulo tratamos a los principios jurídicos, los cuales son fundamentales para nuestro estudio pues a partir de éstos explicamos –y también en cierta forma fundamentamos jurídica y filosóficamente– la tipificación de la conducta propuesta, pues siendo ésta realizada por un sujeto que considera no irregular su conducta jurídica, empresarial y social, no es fácil hacer que entienda su nueva posición ante la ley, por lo que trataría de que no se le aplicara exponiendo que se limita al ejercicio de su garantía constitucional de ejercer cualquier trabajo o profesión. Sin embargo, no es el caso; se trata de legislar sobre la conducta omisiva de un hacer previamente reglamentado, que si el sujeto respeta nunca tendrá problema alguno.

En el tercer capítulo tenemos el estudio de los delitos informáticos, señalando en el mismo desde el origen, y el concepto de delito, hasta la regulación de los mismos dentro de la informática a nivel nacional e internacional.

Es importante señalar que este capítulo tiene una singular importancia por ser el tema central de nuestro estudio y por contener las figuras delictivas actuales, contemporáneas, las cuales han sido reguladas y tipificadas en diversos países. Podremos encontrar en dicho capítulo antecedentes y las diversas formas de control que han aplicado algunos países tratando de regular a estas conductas ilícitas, así como tratados, convenios o acuerdos, mediante los cuales se intenta de garantizar y obligar a los países firmantes a otorgar una seguridad informática en el uso de sistemas, redes, programas y hardware, así como el emitir una regulación uniforme para poder en el caso de que se cometa una conducta ilícita, castigar a los delincuentes informáticos.

Como podemos darnos cuenta en éste capítulo analizaremos a los delitos informáticos, y las conductas que se consideran parte de estos. De igual forma encontraremos que tanto a nivel nacional como internacional se les ha tratado de una forma diversa; como se ha definido a la computadora como medio y fin de las conductas típicas de los delitos informáticos; a los sujetos que presentan dicha conductas se les ha catalogado dentro de las diferentes definiciones de delincuentes, sin que hasta el momento se haya regulado la conducta del proveedor, creador o diseñador de programas o software, pues recordemos que estos son los que proporcionan directamente a la computadora y a quien la utiliza la herramienta para poder trabajar o realizar verdaderos actos ilícitos.

En el capítulo cuarto se analizará la protección jurídica que se ha aplicado principalmente al software nacional e internacional, revisando sus antecedentes y los aspectos fundamentales así como las ramas del Derecho que tienen alguna relación protectora con éstos, las cuales son: Derecho Civil, Derecho Penal, Derecho de Patentes, así como

Derecho de Autor. En este apartado podremos encontrar las diversas formas que han adoptado los países europeos, y americanos para proteger sus sistemas informáticos, software y hardware, tanto interna como externamente.

En el capítulo último revisaremos a la criptología de manera global, es decir, desde sus fundamentos hasta elaborar una crítica de dicho sistema, el cual carece de verdadera seguridad informática, como lo demostraremos posteriormente.

Es así como ante la innegable relación que existe entre el Derecho y la Informática, es importante dejar en claro que tanto los juristas como los abogados y todo aquel que tenga que ver con esta rama del Derecho, debemos tener presente que esta relación es el principio de un fenómeno mundial –el cual debemos de estudiar y considerar dentro de nuestros acervos– al que, si se le deja avanzar sin que el Derecho marque sus pasos conforme a su propio avance tecnológico, pronto generará un sinnúmero de problemas, no sólo en cuanto a la tipificación de las conductas que se den a conocer como nuevas figuras delictivas sino en cuanto a la creación o proliferación de software y hardware de manera indiscriminada y con un fin totalmente ilegal.

CAPÍTULO PRIMERO

ANTECEDENTES HISTÓRICOS

1.1 Orígenes de la computadora

Desde tiempos muy remotos el hombre, al verse en la necesidad de cuantificar sus pertenencias animales, objetos de caza, pieles, etcétera, ha tenido que procesar datos. En un principio este procedimiento fue muy rudimentario: utilizaba sus manos y almacenaba toda la información, porque al no existir representaciones fijas de los elementos que se tenían en el proceso determinado, las conclusiones a las que llegaba resultaban ser meras especulaciones. El hombre para contar estaba limitado al número de sus dedos; esto fue superado cuando empezó a utilizar otros medios como cuentas, granos y objetos similares.

Posteriormente, inventó sistemas numéricos que le permitieron realizar sus operaciones con mayor confiabilidad y rapidez, e ideó algunas herramientas que le ayudaron en su afán de cuantificar.

Entre las primeras creaciones del hombre dirigidas a facilitar las operaciones de cálculo tenemos:

a) El ábaco

Fue el primer dispositivo mecánico para realizar cálculos. Este invento aparece en forma independiente en varias culturas de la antigüedad, aunque generalmente se ha atribuido el crédito de su realización al pueblo babilónico.

La palabra ábaco encuentra su raíz etimológica en la voz fenicia "aback", que significa tabla lisa cubierta de arena. Estas tabletas de arcilla tienen una antigüedad de cuatro mil años y con ellas se llevaban registros de barcos y empresas de préstamos que funcionaban en aquella época.

El Código de Hammurabi[1] incluye referencias de transacciones de negocios tales como contratos, escrituras, bonos, recibos, inventarios, ventas y otros tipos de operaciones semejantes. El ábaco que actualmente conocemos apareció a fines del Imperio Romano y con él se pueden realizar con impresionante rapidez, operaciones de suma y resta así como multiplicación y división. El ábaco ha resistido la prueba del tiempo, y la velocidad con la que realiza las operaciones resulta aún hoy en día extraordinaria, teniendo en cuenta que se trata de un proceso manual. En culturas donde aún se utiliza el sistema arábigo persiste su uso.[2]

b) Tablas de logaritmos (1614)

La dificultad para realizar operaciones de multiplicación y división motivó a John Naiper a crear un método que redujera de manera notable ese trabajo. Fue así como surgieron las tablas de logaritmos, a través de las cuales es posible realizar multiplicaciones en forma sencilla y rápida; las multiplicaciones se traducen en sumas y las divisiones en restas. Sin embargo, había que crear las tablas y sus antilogaritmos e imprimirlas. Esto representaba un enorme trabajo, que fue realizado por un compañero de Naiper, H. Briggs. No obstante la magnitud del esfuerzo que realiza-

[1] *Cfr.* AWARD, Elías M. *Procesamiento automático de datos.* México, 1982. pág.35.
[2] TÉLLEZ VALDÉS, Julio. *Derecho Informático.* Segunda edición. McGraw-Hill. México, 1999, pág.6

ron, las tablas tuvieron errores que fueron detectados tiempo después.[3]

c) Regla de cálculo (1630)

Poco tiempo después de que Naiper inventó la tabla de logaritmos, surgió otro nuevo invento, menos exacto pero mucho más fácil de utilizar: la regla de cálculo. Esta funciona con base en la medición de longitudes entre dos reglitas que guardan relación, utilizando la escala logarítmica. Esta herramienta ha sido sumamente utilizada, inclusive en la actualidad, y los resultados de las operaciones que se realizan con ella se aproximan con suficiente exactitud. No es sino hasta estos últimos años que han sido desplazadas por las calculadoras electrónicas de bolsillo.[4]

d) La Máquina de Pascal (1642)

Blas Pascal ideó una máquina que podría sumar cantidades. Consistía en un sistema de ruedas engranadas, en cada una de las cuales estaban marcados los dígitos del cero al nueve. Cada vez que una regla completaba una vuelta, la siguiente a la izquierda caminaba un elemento y así sucesivamente, dando como resultado la suma de varias cantidades. A está sumadora se le considera como la primera máquina de calcular construida por el hombre.[5]

e) La Tarjeta perforada (1804)

Joseph Marie Jacquard, en Francia, construyó una máquina para tejer complicados diseños de tela. Esta má-

---

[3] *Idem.*
[4] *Ibidem*, pp.6-7.
[5] *Ibidem*, pág.7

quina funcionaba con tarjetas perforadas que contenían información del camino que debían seguir los hilos de la tela para lograr un diseño determinado. Esta idea y otras más participaron en el desarrollo de los sistemas de proceso de datos que hoy día se manejan. La idea de Jacquard tuvo grandes repercusiones: introdujo la automatización y con ella se convirtió en el Padre de las tarjetas perforadas.[6]

f) La Máquina de Babbage (1834)

Uno de los más notables contribuyentes al desarrollo de las máquinas de cálculo fue el inglés Charles Babbage, quien obtuvo el apoyo de su gobierno para realizar una máquina que fuera capaz de efectuar cálculos complejos y de esta forma eliminar los errores en que frecuentemente se incurría. Esta máquina trabajaba con base en el "método de las diferencias", y fue creada para corregir los errores de las tablas de logaritmos. No obstante la utilidad que representaría este proyecto, el trabajo no pudo concluirse ya que el gobierno británico, después de haber gastado 17,000 libras, suspendió la subvención.[7]

Tiempo después, Babbage ideó una máquina analítica que sería capaz de ejecutar procesos más complicados como la multiplicación y la división, almacenando resultados intermedios en el dispositivo interno: "contaba con las tablas de logaritmos, efectuaba decisiones simples y finalmente entregaba un resultado impreso de manera automática. [...] el invento de Babbage fue superior a la capacidad técnica de su época y por lo tanto no pudo realizarse. Sin embargo, la máquina de Babbage fue determinante en el desarrollo de las computadoras actuales, pues

[6] *Loc. Cit.*
[7] *Loc. Cit.*

cien años después de que él la concibió, sus bases sirvieron de pauta para la realización de la primera computadora electrónica".[8]

g) El Código de Herman Hollerith (1880)

El año de 1880 fue el principio de la época moderna de la tarjeta perforada. En ese año, Herman Hollerith, especialista en estadística, trabajaba en la Oficina de Censos de los Estados Unidos como agente especial para acelerar el procedimiento de los datos en los censos.[9]

El censo de 1886 requirió siete años y medio para terminarse. Se usaron métodos manuales de tabulación para el recuento de una población de cincuenta millones de habitantes y fueron completamente inadecuados.[10]

Evidentemente el censo de 1890 no podía realizarse con los mismos medios si se quería que los resultados fueron realmente útiles. El doctor Hollerith se propuso mecanizar la operación de los censos. Para 1887 había completado un sistema que empleaba el principio de la tarjeta perforada. Aunque la primera máquina utilizaba tiras de papel con agujeros perforados de acuerdo con una clave, las tiras de papel resultaron poco prácticas, así que se desarrolló una tarjeta de tamaño normal y el sistema finalmente utilizó tarjetas de tres por cinco pulgadas, con las esquinas cortadas, una prensa de alfileres, contadores electromagnéticos y una caja distribuidora.[11]

En 1896 Hollerith organiza la compañía de máquinas tabuladoras para desarrollar sus máquinas y ven-

---

[8] *Ibidem*, pp.7-8.
[9] *Ibidem*, pág.8.
[10] *Idem*.
[11] *Idem*.

derlas al público. En 1901 presentó la forma básica de un teclado perforado numérico y se hicieron otras mejoras al sistema antes de su retiro en 1914. Con el sistema de Hollerith se necesitaron únicamente dos años y medio para reunir los datos del censo de 1890, a pesar de que la población se había incrementado en un 25% respectó de la de 1880.[12]

Hasta este momento sólo hemos conocido la historia o desarrollo básico del inicio de las computadoras, la forma mediante la cual se fue dando un rotundo cambio y actualización de la ciencia y tecnología para realizar las tareas primordiales que al hombre le costaban tiempo, trabajo y dinero, en un tiempo corto y con buenos resultados. Pero esto no es todo pues apartir de Herman Hollerith la evolución de las computadoras fue a pasos agigantados, tecnológicamente hablando, para el bien y/o ayuda de la ciencia y el ser humano, como lo podemos ver enseguida:

a) La Mark (1937-1944)

La primera máquina que llevó a la realidad el sueño de Babbage fue la Mark I o ASCC (Automatic Séquense Controlled Calculator). En 1937 Howard Aiken, profesor de Harward, se fijó la meta de construir una máquina calculadora automática que cambiaría la tecnología eléctrica y mecánica con las técnicas de tarjetas perforadas de Hollerith. Con la ayuda de estudiantes de posgrado e ingenieros de la IBM, el proyecto se completa en 1944. El aparato terminado se denominó como se vio al principio de este inciso, Computadora digital "Mark I". Las operaciones internas se controlaban automáticamente con relevadores electromagnéticos, y los contadores aritméticos eran mecá-

[12] *Loc. Cit.*

nicos; así la "Mark I" era una computadora electromecánica. En muchos aspectos era el sueño de Babbage hecho realidad. Esta máquina "medieval" se exhibe actualmente en la Universidad de Harvard.[13]

b) La ENIAC (1943-1945)

Las primeras computadoras electrónicas fueron desarrolladas en el Aireraft Research Institute por Konrad Suez.[14]

La máquina norteamericana conocida como ENIAC (Electronic Numerial Integrator and Calculator), no tenía partes mecánicas, utilizaba bulbos (alrededor de 18,000). Era capaz de realizar cinco mil operaciones por segundo y fue utilizada principalmente para resolver problemas de balística y aeronáutica. Su mayor mérito fue el de tener gran cantidad de componentes y trabajar de manera simultánea con ellos; sin embargo, era demasiado grande y se calentaba con mucha rapidez.[15]

c) La EDVAC (1945-1952)

El mismo que trabajó en la construcción de la ENIAC, Eckert y Mauchly, construyó una segunda máquina, mayor que la ENIAC, con el nombre de EDVAC (Electronical Discrete Variable Automatic Computer), capaz de realizar operaciones aritméticas con números binarios y almacenar instrucciones internamente.[16]

---

[13] H. SANDERS, Donal. *Informática Presente y Futuro* [trad. Roberto Luis Escalona]. Segunda edición. McGraw-Hill. México, 1993, pág.45.
[14] TÉLLEZ VALDÉS, Julio, *op. cit.*, pág.9.
[15] *Idem*
[16] *Idem.*

d) La UNIVAC (1951)

La Compañía Remington Rand fundada por los mismos Eckert y Mauchly desarrolló la UNIVAC (Universal Automatic Computer), que fue la primera computadora de uso comercial, y que apareció en 1951.[17]

Entre sus características principales encontramos el uso de cinta magnética para la entrada y salida de datos, la capacidad de aceptar y procesar datos alfabéticos y numéricos, así como el uso de un programa especial capaz de traducir programas en un lenguaje particular a lenguaje de máquina.[18]

Estas máquinas constituyen la llamada primera generación de computadoras, que utilizaron bulbos de alto vacío como componentes básicos de sus circuitos internos. Como consecuencia, eran demasiado voluminosos, consumían mucha energía y producían calor; no fueron tan confiables como se había esperado, eran rápidas pero no lo suficiente y tenían capacidad de almacenamiento interno pero limitado.

El siguiente avance tecnológico en la industria de las computadoras fue la sustitución de los bulbos por transistores que redujeron las deficiencias y mejoraran las ventajas ya existentes, introduciendo las memorias de ferrita que permitieron reducir el tamaño. Así surgió la segunda generación de computadoras.

En 1963 aparecen en el mercado las computadoras de la tercera generación, en las que encontramos como principal característica el uso de circuitos integrados monolíticos, que aumentaron considerablemente la velocidad de operación, incrementaron su confiabilidad y disminuyeron su costo y tamaño.[19]

---

[17] *Ibidem* pág.10.
[18] *Idem.*
[19] *Idem.*

A partir de la tercera generación, los avances en la industria de la computación han sido tan numerosos y frecuentes que de alguna manera han hecho que el hombre de nuestro tiempo pierda su capacidad de asombro. Las computadoras han invadido la industria, el comercio, la administración, la educación y han llegado hasta nuestros hogares, constituyéndose esta industria en la segunda en importancia en el mundo, después de la automotriz.[20]

Así, tenemos la llamada cuarta generación, con la integración a la larga escala (LLS1) y la aparición de microcircuitos integrados en plaquetas de silicio (chips) con notorias mejoras, en especial a nivel de la llamada microprogramación (Firmware).[21]

Sin embargo, el desarrollo computacional no se detiene aún.

1.1.1 Nociones y concepto

El uso de las computadoras, sobre todo las computadoras personales, se ha extendido tan rápidamente que ya no es posible hacer caso omiso de su existencia. Todas las personas necesitan acostumbrarse a estas máquinas para poder funcionar en una sociedad moderna. Si se desea lograr la iniciación en informática, es preciso comprender las posibilidades y limitaciones de los sistemas de cómputo y saber cómo trabajar con estos sistemas para producir los resultados prácticos que se desean y así sacar el mayor provecho de éstas en el momento de su uso.

Las computadoras pueden manipular símbolos, tanto numéricos como no numéricos. Los datos son he-

[20] *Loc. Cit.*
[21] *Loc. Cit.*

chos, la materia prima de la información, y se representan por medio de esos símbolos. La información es el conocimiento relevante que resulta del procesamiento y arreglo de los datos en una forma ordenada y útil. El procesamiento de datos consiste en: a) capturar los datos de entrada, b) manipularlos, implicando técnicas de agrupación, cálculo, clasificación y síntesis y c) almacenar, recuperar, comunicar y reproducir los resultados finales de la manipulación.

El tamaño y costo de los componentes de las computadoras se ha reducido drásticamente, en tanto que su velocidad, capacidad de almacenamiento y confiabilidad han aumentado. En el área de programación, los avances incluyen el desarrollo de lenguajes de programación y programas traductores (compiladores). Además, las mejoras en los programas de sistemas operativos que controlan el funcionamiento general de las computadoras han aumentado la productividad y utilización del equipo.

Por lo que respecta a su concepto tenemos que: a nivel operacional, la computadora puede ser definida como la máquina automatizada de propósito general, integrada por elementos de entrada, procesador central, dispositivo de almacenamiento y elementos de salida.[22]

Otro concepto más amplio, pero que no por eso deja de ser importante para su mención, es el siguiente: Un ordenador es una maquina electrónica capaz de resolver problemas, en sistema de numeración binario, realizando cálculos y operaciones lógicas a gran velocidad, según las instrucciones de un programa y datos almacenados en su memoria, y algunos con capacidad de retroalimentarse (feedback) para modificar sus instrucciones: la salida alimenta la entrada modificando el proceso. Los datos por sí mis-

---

[22] *Ibidem*, pág.9

mos no dicen nada, deben ser procesados y convertidos en información, para ser significativos.[23]

Por último, nosotros también podemos dar una definición de computadora: una computadora es un sistema manipulador de símbolos (datos) rápido y exacto, diseñado para aceptar y almacenar datos de entrada, procesarlos y producir resultados, dirigido por un programa almacenado de instrucciones detalladas.

1.1.2 Características de las computadoras

Por lo que concierne a este punto y una vez revisadas las características de las primeras computadoras a nivel general, me abocaré a las computadoras actuales para el desarrollo del presente punto.

Por lo que respecta a las clases de ordenadores (de este modo se conoce y define a la computadora en España) o computadoras como las conocemos nosotros, hay tres tipos principales, que son los siguientes:

DIGITALES: Las magnitudes que en ellos se almacenan varían de una forma discreta, sus unidades están separadas, manejan datos caracterizados por ser números positivos enteros (dígitos). Funcionan secuencialmente, instrucción por instrucción. Los ordenadores personales son digitales, constituyen la mayor parte de los ordenadores.[24]

ANALÓGICOS: Procesan datos analógicos representados por magnitudes que varían de una forma continua, sus unidades no están separadas unas de otras. Se emplean circuitos y magnitudes eléctricas capaces de simu-

---

[23] BARRIUSO RUÍZ, Carlos. *Interacción del Derecho y la Informática.* Dykison. Madrid, 1996, pág.21.

[24] *Idem.*

lar por analogía los más variados fenómenos físicos. Tiene como dispositivos de entrada-salida, por ejemplo, amplificadores, servomecanicos, potenciómetros, etc. Funcionan con rapidez pero tienen un 1 por 100 de errores, por lo que no pueden ser usados en trabajos de gran precisión.[25]

HÍBRIDOS: Con partes digitales para los cálculos en los que no se admite error y analógicos para ganar en velocidad. Son los ordenadores utilizados para calcular las trayectorias de los vehículos espaciales.[26]

Así pues, en cuanto a un equipo de cómputo se puede hablar de cuatro elementos o partes:

a) Elementos de Entrada

Representan la forma de alimentación de información a la computadora, por medio de datos e instrucciones realizados por elementos periféricos tales como pantallas, lectoras de soportes magnéticos, cintas, diskettes, etcétera.[27]

b) Procesador Central

Dispositivo en que se ejecutan las operaciones lógico-matemáticas, conocido más comúnmente como unidad central de proceso (CPU en inglés).[28]

c) Dispositivo de Almacenamiento

Contiene o almacena la información que se ha de procesar.[29]

---

[25] *Ibidem*, pp.21-22.
[26] *Ibidem*, pág.22.
[27] TÉLLEZ VALDÉS, Julio, *Op. Cit.* Pág.11.
[28] *Idem.*
[29] *Idem.*

d) Elementos de Salida

Medios en los que se reciben los resultados del proceso efectuado (pantalla, impresoras, graficadores).[30]

Otra estructura que forma parte indispensable de una computadora es el Hardware o partes físicas de la computadora; se toman como tales el disco duro, teclado, mouse, monitor, procesador, tarjeta madre, memoria -la cual se divide en dos RAM y ROM,- unidad lectora de CD-ROM y, en su caso, unidad de escritura mejor conocida como "quemador", unidad lectora de disco flexible (*floppy*), fax-modem, unidad lectora de cintas magnéticas, impresora, escanner, pluma óptica, tarjeta lectora reproductora de videos (DVD) y video cámara integrada en monitor; estos elementos, *en su mayoría,* son parte indispensable de una computadora, y sin ellos a cualquiera se tacharía de obsoleta o anticuada para los tiempos en que vivimos.

Estas partes son las encargadas de la captación, almacenamiento y procesamiento de información, así como la obtención de resultados. Es de suma importancia para el presente estudio mencionar que todo equipo de cómputo se puede ya sea armar por partes o inclusive pedirlo con características técnicas especiales, dependiendo del trabajo que se ha de realizar con él; es decir, si se va a realizar un acto de piratería de discos compactos, mejor conocidos como CD, se deberá de tener un equipo con las características que se señalaron anteriormente y a la vez un conocimiento mínimo del manejo de las computadoras y programas que se necesitan para realizar dicha actividad.

Una de las partes sustanciales y de igual importancia que el hardware en una computadora es el software, también conocido como programa. Esto porque una com-

[30] *Loc. Cit.*

putadora sin un programa que la maneje tanto a ella como a sus elementos integrantes físicos es un vegetal, es un aparato sin sentido y sin interés alguno; hay por ende una gran diversidad de programas y dependiendo del trabajo que se vaya a realizar, el usuario de una computadora puede instalarlos o pedir a una persona capacitada la instalación del mismo; estos programas constituyen la estructura lógica que permite a la computadora la ejecución del trabajo que se ha de realizar.

Esta parte lógica del sistema se compone de:

Firmware, Bios: programas residentes en la memoria principal de control interno.[31]

Sistema Operativo (Operating System): sistema lógico que regula la ejecución de programas y que puede comprender funciones o servicios, tales como la asignación de recursos, la planificación y supervisión, el control de entrada-salida y la gestión de ficheros, datos y memorias.[32]

Programa (program): conjunto de instrucciones agrupadas en módulos interrelacionados y ensamblados enlazando subrutinas, con un propósito determinado, que resuelve una aplicación concreta.[33]

El uso de programas se ha facilitado para toda la gente. Un ejemplo de esto es el programa conocido como "Windows" en diversas versiones, así como Office de Microsoft, Lotus, Corel Draw, etc. Aunado a esto, la mayoría de estos se encuentran en idioma español para su mejor uso, comprensión y trabajo diario. Así podemos deducir que una persona con un mínimo de conocimiento,

---

[31] *Ibidem*, pág.31.
[32] *Idem.*
[33] *Idem.*

ya sea en hardware o en software, así como conocimientos técnicos, puede realizar tantas tareas como quiera tan sólo con un programa adecuado para éstas, sin importar límites, los cuales se imponen primeramente por el hardware del equipo y la efectividad de los programas utilizados y en segundo caso, que debería de ser el primero, el límite que impone el Derecho en este caso la Ley penal.

Hasta este momento sólo se han mencionado los programas más conocidos y de fácil uso, pero, hay otro tipo de software que requiere un mayor nivel técnico y profesional, por parte de quien los utiliza y aplica, y en particular de quien es el usuario final. Estos son:

a) FORTRAN. (Formula traductora), aparecido en 1957 y caracterizado por sus fines eminentemente científicos y matemáticos.

b) ALGOL. (Lenguaje algorítmico), surgido en 1938 y también con propósitos fundamentalmente científicos.

c) COBOL. (Lenguaje orientado a negocios comunes), creado en 1960 con aplicaciones administrativas.

d) BASIC. (Código de instrucciones simbólicas para principiantes de todo propósito), aparecido en 1958 y caracterizado por su relativa sencillez y pronunciada potencia y versatilidad, pretendiendo unificar y facilitar el acceso general a las computadoras.

e) PASCAL. Como un lenguaje de propósito general con un enfoque de programación estructurada.

f) ADA. Utilizado fundamentalmente por el Departamento de Defensa de los Estados Unidos.

g) OTROS. PL/I, CANDE, APL,[34] Etcétera.

---

[34] *Ibidem*, pág.12.

1.2 Orígenes históricos de la cibernética

La cibernética representa uno de los avances científicos más significativos. La obra de Wiener –en este caso el otorgar a ciertos fenomenos el nombre de Cibernética–, considerado el padre de la cibernética, se ha comparado en importancia a las obras de Galileo, Malthus, Rousseau o Mill, y surge ante la creciente necesidad de una ciencia básica para el dominio de la máquina y el potenciamiento intelectual y de la acción, con apoyo electrónico.[35]

Su origen, hacia la segunda mitad del siglo XX, se encuentra en un dominio fronterizo entre las ciencias biológicas, la tecnología, la matemática, y la lógica matemática. Norbert Wiener la describe de la siguiente manera "[...] así pues, hace cuatro años, el grupo de científicos agrupados en torno al Dr. Rosenblueth y yo habíamos llegado a reconocer la unidad esencial de la comunicación, el control y la mecánica estadística, bien en la máquina, bien en un tejido viviente... Decimos denominar a toda la materia referente al control y teoría de la comunicación, ya sea en la máquina o en el animal, con el nombre de cibernética..." y continúa "[...] En cada estadio de la ciencia desde Dédalo o el Héroe de Alejandría, la habilidad del artesano para producir un simulacro activo de un organismo viviente ha intrigado siempre al pueblo...[...]".[36]

Su aparición obedeció principalmente a tres factores, a saber:

a) Un factor social, porque eran tiempos que requerían un aumento en la producción, y por consiguiente, en el capital. Eran tiempos duros, sin embargo, se necesitaba más que una emergencia nacional para que se gestara

[35] BARRIUSO RUÍZ, Carlos. *Op. Cit.*, pág.37.
[36] *Idem.*

una nueva ciencia. Fue así como Stafford Beer en *Cibernética y Administración*[37], señaló que el clima intelectual debe ser tal que favorezca el surgimiento de una nueva disciplina.

b) El factor técnico-científico fue muy importante porque varias líneas de pensamiento, originados en muy diversas esferas de actividad, como lo fue la ciencia y la técnica, se empezaron a reunir, y lograron avances tales que hicieron menester una ciencia que facilitara su interrelación y desenvolvimiento.

c) Un factor técnico, el histórico, porque surge de la mencionada necesidad del nacimiento de una ciencia de unión que controlara y vinculara a todos los demás. Surge entonces la cibernética como una unidad multidisciplinaria. Para Wiener esto es lo que constituye el propósito de la cibernética: abarcar de manera total y multidisciplinaria a todas las ciencias.

Ya Engels en su *Dialéctica de la naturaleza* escribió que en los puntos de unión o contacto de las ciencias es donde se podían esperar los mejores resultados. Él vislumbraba ese punto de unión interdisciplinario, aunque sólo hablara de las Ciencias sin incluir a las técnicas.

Efectivamente, se han obtenido resultados muy fructíferos de estas uniones, la humanidad ha realizado inventos y descubrimientos que le dan al hombre la oportunidad de tener una vida más ligera, más cómoda, pero también han surgido problemas sociales, económicos y jurídicos especialmente. La cibernética y en específico la informática, son tan necesarias en nuestras vidas, como la regulación legal de éstas.

---

[37] *Cfr.* BEER, Stafford. *Cibernética y administración.* México, 1965. pág.20.

1.2.1 Nociones y concepto

Cibernética, en la actualidad significa el poder de gobernar y de informar, abarcando un amplio campo de actuación interdisciplinario. Etimológicamente, proviene del vocablo griego "KUBERNETES", que significa piloto; en la antigua Grecia, estos pilotos tenían la misión de gobernar las embarcaciones y de ello dependía la victoria. Así con su pericia y su conocimiento del estado del mar, de la dirección del viento, y del itinerario previsto, adoptaban sus decisiones para seguir el rumbo, moviendo el timón hasta donde fuera necesario, corrigiendo la desviación entre el rumbo real del barco y el deseado [...].[38]

La cibernética, según Lozano, proporciona a la dogmática un medio de forma ordenada y exhaustiva de dominio, sistematización y recuperación de la totalidad de las normas de un sistema, y según K. Haag, permite aplicar técnicas de regulación y control a conductas jurídicas y técnicas de control social, y ayuda, como indica Ulrich Klug, a que el jurista gane tiempo y libertad creadora al verse exonerado de los procesos subalternos de la investigación.[39]

El concepto de "cibernética" ha sido utilizado en diversas disciplinas que parten desde un estudio de carácter propiamente derivado de la ciencia política, hasta estudios con enfoques matemáticos.[40]

Fue utilizado por primera vez en 1848 por el francés Ampere en una clasificación de las ciencias políticas, ya que él había introducido el término "cibernética" para indicar el arte del gobierno entendido en sentido político.

---

[38] BARRIUSO RUÍZ, Carlos. *Op. Cit.*, pág.38.
[39] *Ibidem*, pág.91.
[40] RÍOS ESTAVILLO, Juan José. *Derecho e Informática en México*. UNAM, 1997, pág.35.

Cibernética es el vocablo griego que indica el arte del gobierno, arte de guiar.[41]

Y siguiendo con el análisis de su concepto tenemos que: [...] La cibernética es la inquisición interdisciplinaria hacia la naturaleza y base física de la inteligencia humana, con el propósito de reproducirla en forma sintética, mientras que para Neville Moray, la cibernética es la ciencia que relaciona las entradas y las salidas de un sistema, sus *inputs y outputs*.[42]

[...] Según sus raíces griegas, es la ciencia que se ocupa de los procesos de dirección en los sistemas dinámicos complejos y que tiene por fundamento teórico las matemáticas y la lógica, así como el empleo de la automática; la cibernética se basa en toda una serie de ramas de la ciencia y las técnicas modernas, y, a su vez, influye favorablemente en su desarrollo.[43]

De acuerdo a lo anterior y para tener un concepto acorde al presente estudio podemos decir que la cibernética es: la ciencia que se ocupa de la creación de instrumentos, ya sean físicos (hardware) o programas (software), mediante los cuales se simulan actividades propias, en principio, del ser humano.

1.2.2 Características de la Cibernética

La cibernética, en sus aspectos más generales, trata del empleo de métodos científicos para explicar fenómenos en la naturaleza o en la sociedad y la forma de representación del comportamiento humano de forma matemática en una maquina.[44]

---

[41] *Idem.*
[42] RÍOS ESTAVILLO, Juan José. *Op. Cit.* pág.37.
[43] *Ingeniería en Cibernética ...y temas afines!.* http:/www.mxl.cetys.mx/Escuelas/Ingenieria/alumnos/mo13645/ciber.htm.
[44] RÍOS ESTAVILLO, Juan José. *Op. Cit.* pág.39.

La cibernética, entre otros aspectos, trata de la creación de instrumentos informáticos que simulen actividades del hombre, por ejemplo, robots; desarrollo de la inteligencia artificial; utilización de métodos heurísticos;[45] entre otros.

La cibernética implica en esencia un sistema en el cual puede o no existir la relación entre las partes (isomorfismo).[46]

La cibernética está en contacto interdisciplinario con el resto de las ciencias, incluso ha producido la penetración de estructuras matemáticas, fundamentando muchas corrientes de investigación y desarrollo; pero no puede armonizar y hacer el estudio y análisis de conjunto sobre la significación, alcance, fundamento, estructura y repercusiones de este nuevo marco (Filosofía y cibernética), en la Filosofía jurídica en particular en la Filosofía en general.[47]

En el marco de la teoría jurídica, según Antonio E. Pérez Luño hay una triple repercusión de la cibernética:[48]

1. En cuanto teoría de la información puede afectar el objeto tradicional de la dogmática jurídica, contribuyendo a propiciar el análisis y sistematización de los contenidos normativos de un ordenamiento jurídico concreto.

La cibernética entendida como teoría de la información, proporciona a la dogmática un aparato técnico ca-

---

[45] Los métodos heurísticos son característicos del desarrollo de la inteligencia artificial. Consisten en darle a la máquina facultades de decisión en la búsqueda de soluciones en un caso concreto, o sea, existen programas computacionales que previenen una solución predeterminada para dar un tipo de respuesta por parte de la máquina [..]. *Idem.*

[46] *Idem.*

[47] BARRIUSO RUÍZ, Carlos. *Op. Cit.*, pág.88.

[48] *Ibidem*, pág.140.

paz de suministrarle, de forma ordenada y exhaustiva, el dominio, sistematización y recuperación de la totalidad de las normas de un sistema, una vez traducidas al lenguaje formal del ordenador.

2. Como teoría de los sistemas, regulación y control, interesa a la sociología jurídica, ofreciendo métodos de análisis cuantitativo de los hechos jurídicos.

3. La cibernética, considerada como teoría de los sistemas y sus interpretaciones, penetra en los dominios de la filosofía jurídica.

1.3 Orígenes Históricos de la Informática

A lo largo de la historia, el mundo ha sufrido diversas revoluciones tecnológicas relacionadas con la información, mismas que han repercutido en tal forma, que han transformado y reorganizado la economía, la sociedad y el Derecho.

Desde los primeros tiempos de la informática, en los años cuarenta, hasta la sofisticación de las redes telemáticas existentes hoy día, se ha recorrido un largo camino en lo que a evolución técnica se refiere, ya que la sociedad moderna no sería posible, en muchos adjetivos con que se ha intentado asignar al momento en que vivimos: la era atómica, la era espacial... han llevado a considerar que nos encontramos en la era de la informática.[49]

La era de la informática, es posible, que sea una de las denominaciones que tenga mayor arraigo en el futuro, ya que si la revolución industrial cambió la forma de vida de millones de personas, la aparición del ordenador

[49] Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura-Mérida. *Informática y Derecho. Revista Iberoamericana de Derecho Informático, "Jornadas Marco Legal y Deontológico de la Informática"*, Mérida, 1998, actas volumen I, pág.34.

puede modificar profundamente el mundo de cara al próximo milenio –dentro del cual ya nos encontramos– en que se prevé, en ciertos países, más de la mitad de la población activa tendrá una ocupación que, de una forma u otra, dependerá de la informática.[50]

La informática surge de la misma inquietud racional del hombre, el cual, ante la cada vez más difícil adecuada toma de decisiones, es impulsado a formular nuevos postulados y a desarrollar nuevas técnicas que satisfagan dichos propósitos, utilizando todos los medios necesarios para esto; el hombre (en este caso el creador de software y/o hardware) no repara en el daño que puede hacer a la humanidad, a la sociedad y así mismo como parte de ésta, en la creación desmedida de "arte informático" mejor conocido como tecnología de punta.

En la actualidad, como lo sostienen algunos autores, estamos sufriendo una nueva revolución tecnológica. La Informática, junto con sus micros, minis y macrocomputadoras, los bancos de datos, las unidades de tratamiento y almacenamiento, la telemática, etcétera, están transformando de manera indudable nuestro mundo.[51]

El ordenador está por todas partes y son pocas las áreas de los negocios, la industria, la ciencia y la educación que no utilizan ampliamente la informática; con ella nos hacen el recibo del agua, el de la luz, controlan nuestras cuentas bancarias y nuestras reservas de dinero pueden ser una serie de números almacenados en los discos

[50] *Idem.*
[51] TÉLLEZ VALDÉS, Julio, *Op. Cit.*, pág.4.

magnéticos del ordenador de nuestro banco; el ordenador puede ser repetidor de lecciones, puede limitarse a comprobar los conocimientos y puede por sí solo dar verdaderas clases.[52]

En los últimos años el desarrollo de la tecnología de la información, en especial la amplia difusión de INTERNET, ha tenido una influencia social de tal grado que las prácticas tradicionales de las más diversas disciplinas del conocimiento se han modificado sustancialmente. Tal es el caso de la medicina (asistencia de manera remota al diagnóstico, operación o consulta de un paciente), la ingeniería e incluso el Derecho.[53]

Nadie duda, en la década de los noventa, de esos espectaculares avances de las nuevas tecnologías de la información y de la comunicación y que Internet, esa red de redes que conecta más de dos millones de ordenadores, está siendo el fenómeno estelar, con más de treinta millones de usuarios, de aquí que cada día sean más los que consideran que deberían ir acompañadas, igualmente, de una nueva regulación jurídica para evitar que la tecnología no aplaste al hombre aun cuando, por razones de progreso, se vea obligado a cambiar de hábitos y de sus concepciones tradicionales.[54]

Junto a las incuestionables ventajas derivadas de las inmensas posibilidades de conocimiento, actuación y de comunicación que permita la navegación por el ciberespacio, que es otra cosa que un microcosmos digital en el que no existen fronteras, distancias ni autoridades centralizadas, Internet ha hecho surgir en los tiempos, graves motivos de inquietud -tráfico de imágenes de prostitu-

[52] Universidad Nacional de Educación a Distancia. *Op. Cit.*, pág.34.
[53] *Idem.*
[54] *Ibidem*, pp.34-35.

ción infantil, propaganda de bandas terroristas- que han llevado a millones de ciudadanos a poner de manifiesto lo peligroso que entrañan determinadas manipulaciones de las nuevas tecnologías.[55]

Como se pueden dar cuenta, la informática ha tomado parte en el desarrollo científico y de la información procesada por medios electrónicos, en este caso por una computadora a nivel mundial, y en la actualidad es un área dentro de la cual se conforman principalmente el hardware y software para la supuesta mejor toma de decisiones, tanto lógica como matemáticamente.

1.3.1 Nociones y Concepto

La informática como tal, ha sido comúnmente considerada como una ciencia particular integrada a la cibernética. Aunque esta opinión parece en sí misma lógica y evidente, existen sin embargo diferencias de objeto finalidad entre ambas disciplinas. [...] La informática, por su parte, si bien hace uso de las tecnologías desarrolladas con auxilio de la cibernética, se centra en cuestiones de tratamiento, representación y manejo automático de la información.[56]

El término informática fue creado en Francia, a mediados de la década de los setentas "INFORMATIQUE, de information automatique", con el objeto de designar las ciencias y técnicas de la comunicación que intervienen en la recopilación y utilización de datos a fin de elaborar decisiones, extendiéndose de allí y a partir de esa época, a todo el mundo.[57]

---

[55] *Ibidem*, pág.35.

[56] RÍOS ESTAVILLO, Juan José. *Op. Cit.*, pp.39-40.

[57] ACEDO QUEZADA, Octavio R. *Cursos de Informática en las Escuelas de Derecho*, en *Revista Tribunal*, Poder Judicial de Jalisco, 1997, número 4, pág. 35.

Por lo que respecta a su concepto, tenemos varios autores que nos dan el suyo y dentro de los cuales está siempre presente la palabra automatización e información, como lo vemos enseguida:

En sentido general, "la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones desde el punto de vista de un sistema integrado". [58]

"Mario G. Lozano caracteriza a la informática como producto de la cibernética, en tanto un proceso científico relacionado con el tratamiento automatizado de la información en un plazo interdisciplinario" .[59]

"La Informática, palabra compuesta por los términos "información" y "automática", es la ciencia del tratamiento automático o automatizado de la información, primordialmente mediante las computadoras" .[60]

Un último concepto, el cual nos da el punto de vista de Europa y en particular España, es el siguiente: "La informática (*Computer Science*) son los conocimientos científicos y técnicos que hacen posible el proceso de datos con medios automáticos y electrónicos. La información (*Computerización*) es la automatización de los procesos por medio de ordenadores" .[61]

El proceso de datos (*Data Processing*) hace posible la conversión de los datos en información. Ha sido definido como: "el dar la información correcta a la persona adecuada en el momento preciso, transformando los datos en información útil. La utilización de ordenadores en el proceso electrónico y automático de datos, resuelve

[58] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pág.5.
[59] *Idem.*
[60] RÍOS ESTAVILLO, Juan José. *Op. Cit.*, pág.5
[61] BARRIUSO RUÍZ, Carlos. *Op. Cit.*, pág.31.

eficaz y eficientemente esta finalidad, con la ejecución sistemática de operaciones" .[62]

1.3.2 Características de la Informática

De lo anteriormente mencionado se puede desprender que la informática tiene dos características principales:

- "La informática parte del estudio de las computadoras, de sus principios básicos y de su utilización. Comprende materias tales como programación; estructura de la información; ingeniería del software; lenguajes de programación; hardware; arquitectura de las computadoras, entre otras" .[63]
- "La informática es un instrumento de apoyo para el desarrollo de la propia cibernética".[64]

Estas características, aunque son únicamente dos, muestran con gran acierto los puntos precisos, exactos, del ser mismo de la informática, el porqué de su existencia y su importancia en la actualidad. No nos dejan en ningún momento dudas en cuanto a su propia forma y tendencia de estudio e investigación, así como la inventiva hacia una nueva era donde habrán de "gobernar como tecnología de moda y punta las computadoras", llevando de la mano a la propia sociedad como parte intrínseca de la revolución diaria de esta tecnología; es decir, son la causa y efecto de la propia sociedad, o mejor dicho el ser humano.

---

[62] *Idem.*
[63] *Ibidem.* pág.39.
[64] *Idem.*

Una última característica es que: "necesitamos recurrir a ella para conocer cuáles son las conductas que la comunidad científica tecnológica considera que deben protegerse por el derecho, mientras que el derecho debe indagar qué es el delito para posteriormente cuestionar si la utilización masiva de las computadoras y la telemática pueden cambiar la naturaleza y alcance de la ley penal".[65]

1.3.3 Fenómeno informático

Este fenómeno tiene gran importancia y a la vez ciertas particularidades que lo distinguen de otros que han sucedido en el mundo en que vivimos. En un principio tuvo muchos contratiempos; entre estos uno, quizá el más importante que era convencer a la gente, empresarios primordialmente, de los beneficios económicos, independientemente de los de orden social, que traería la utilización de equipos de cómputo.

Cuando los empresarios vieron su utilidad comercial a principios de la década de los sesenta, se le dio el impulso necesario para su producción a gran escala. Los grandes precursores de las computadoras no imaginaban las repercusiones que dicho instrumento tendría en nuestra actualidad; "...es impresionante la medida en que ha progresado esté fenómeno pues ha llegado a tal grado que hoy en día se habla de una verdadera revolución informática como liberadora de las enormes cargas intelectuales en los individuos, así como anteriormente se presentó una revolución industrial en la que la liberación se presentó en los trabajos y rutinas de orden físico".[66]

---

[65] RÍOS ESTAVILLO, Juan José. *Op. Cit.*, pág.114.
[66] TÉLLEZ VALDÉS, Julio. *Op. Cit,*. pág.15.

Actualmente las computadoras son la fuerza motriz de la revolución informática, la cual está provocando serios cambios en los individuos, algunos positivos como: nuevas oportunidades de trabajo, mayor satisfacción en el trabajo y aumento en la productividad, etc. Así pues, los beneficios generados por las computadoras en la mayoría de las ocasiones sólo tienen como límite al propio ingenio humano y la imaginación.

Por otra parte, las computadoras también traen consigo implicaciones negativas como lo son: continua amenaza de desempleo, problemas físicos y psicológicos y problemas jurídicos como se verá posteriormente.

Existen áreas generales de injerencia de las computadoras a nivel de transferencia institucional y privada para fines de gestión, y su existencia ha permitido un sin número de avances que se reflejan en numerosos ámbitos, como lo son: las oficinas y el resurgimiento de la llamada Ofimática[67], Gerencial, Supervisión y Control, Administración, Industrial y el surgimiento de la llamada robótica[68], Bancario, Salud, Hogar, mejor diseño y construcción de edificios, casas, carreteras, mejor y mayor comunicación de despachos noticiosos, mejor control de bibliotecas, desarrollo de nuevas ideas publicitarias, control del tráfico y contaminación, localización de personas extraviadas, recuperación de vehículos robados, predicciones meteorológicas, mejor desarrollo de la educación e investigación, fotografía y animación por computadora, diversión y entretenimiento, etc.

---

[67] Término proveniente del francés *burotique* y alusivo a la informatización o automatización de oficinas. *Ibidem., pág.17.*

[68] Término alusivo a la informatización de las fábricas. *Idem*

CAPÍTULO SEGUNDO

PRINCIPIOS JURÍDICOS GENERALES

2.1 Principios fundamentales del derecho en General

Comenzaremos el presente apartado haciendo una breve revisión de los antecedentes del Derecho, pero es importante señalar que sólo en aquellos aspectos que son base para el presente estudio. Así pues, la exigencia de una reglamentación imperativa o coercitiva de las relaciones humanas aparece en el momento en que surgen los grupos, las familias, los clanes, las tribus, etcétera. De esta forma es como el Derecho se crea, es producto de la organización social y en cuanto al hombre, éste no puede prescindir de su relación con los demás cuando ha alcanzado cierto grado de evolución. La máxima conforme a la cual el grupo social requiere de un orden jurídico: *Ubi societas, ibi jus,* significa que la sociedad es la condición necesaria y suficiente para la manifestación del fenómeno jurídico; alude a su vez a la necesidad de existencia del Derecho para que sea posible la convivencia humana. De esto se desprende que el Derecho necesita de la sociedad y ésta del Derecho y de aquí su importancia.[69]

Basado en las ideas de Rousseau y de Montesquieu, Becaria sostenía que: [...] las leyes son las condiciones con que los hombres aislados e independientes se unieron en sociedad, cansados de vivir en un continuó es-

[69] *Ibidem.* pág.19.

tado de guerra, y de gozar de una libertad que les era inútil en la incertidumbre de conservarla. La suma de todas estas porciones de libertad, sacrificadas al bien de cada uno, forma la soberanía de una nación, y el soberano es su administrador y legítimo depositario.[70]

El Derecho del Soberano para castigar los delitos se funda en "la necesidad de defender el depósito de la salud pública (contra) las particulares usurpaciones; y tanto más justas son las penas, cuanto es más sagrada e inviolable la seguridad, y mayor la libertad que el soberano conserva a sus súbditos". Para Beccaria "el daño hecho a la sociedad es la verdadera medida de los delitos"; y, siguiendo a Montesquieu, afirma que toda pena que no se deriva de la absoluta necesidad es tiránica; de manera más general propone: "Todo acto de autoridad de hombre a hombre, que no se derive de la absoluta necesidad, es tiránica". En estos razonamientos se asienta el postulado de que el Derecho de castigar debe ser el mínimo necesario para la defensa de la sociedad.[71]

La voz latina "jus", con la que se designó en Roma al Derecho, no es sino una contracción de *jussum,* participio del verbo "*jubere*", que significa mandar. Es así como la palabra "derecho" ha sido utilizada empleando para ella diversas acepciones, a saber:

Como el conjunto de reglas o preceptos de conducta de observancia obligatoria que el Estado impone a sus súbditos; como la disciplina científica que tiene por objeto el conocimiento y la aplicación de esas reglas de conducta; como el conjunto de facultades que tiene un in-

[70] Cámara de Diputados del H. Congreso de la Unión. *Derechos del pueblo mexicano. México a través de sus constituciones.* Porrúa, 2000, tomo III, artículos 12-23, pág.101.
[71] *Ibidem*, pp.101-102.

dividuo y que le permiten hacer o dejar de hacer algo frente a los demás y frente al Estado mismo.

Con base en estos elementos, son muchos los conceptos que se han vertido sobre el Derecho. De ellos nos ha parecido pertinente resaltar el formulado por el Maestro Villoro Toranzo, por considerar que este engloba en forma general los rasgos más importantes de dicha disciplina. En esté sentido tenemos que el Derecho es el "Sistema racional de normas Sociales de conducta declaradas obligatorias por la autoridad, por considerarlas soluciones justas a los problemas surgidos de la realidad Histórica".[72]

En lo que respecta a la clasificación del Derecho, si bien es cierto que tradicionalmente (o al menos desde la célebre sentencia del jurisconsulto Ulpiano) se ha manifestado la existencia de un Derecho Privado como régimen regulador de intereses particulares, y un Derecho Público como régimen regulador de intereses colectivos, también hay opiniones en el sentido de que es muy difícil determinar este tipo de intereses en función de manejos inapropiados de criterios formales y materiales o sobre valores objetivos y subjetivos o que aquellos que mencionan que sólo existe un Derecho, el Público, o de que dicha distinción carece de fundamento, desde el punto de vista teórico, y sólo posee importancia práctica, primordialmente política.[73]

Ahora bien, atendiendo a la eventual existencia de dicha división, se considera que dentro del Derecho Privado tenemos fundamentalmente al Derecho Civil y mercantil, mientras que en el Derecho Público existen las

---

[72] TÉLLEZ VALDÉS, Julio, *Op. Cit.*, pág.20.

[73] GARCÍA MÁYNEZ, Eduardo. *Introducción al Estudio del Derecho.* Porrúa. México, 1997, pág.135.

demás ramas (Constitucional, penal, administrativa, etcétera). Por otra parte, no podemos soslayar los postulados pronunciados por algunos autores en el sentido de que en la actualidad debemos reconocer la existencia de una nueva categoría que es la de Derecho Social.

2.1.1 Concepto de Derecho Informático

En lo que concierne a este concepto, el Maestro Julio Téllez Valdés señala que aunque es difícil de conceptualizar por el variado número de peculiaridades y muy a pesar de los opuestos puntos de vista que pudiera provocar, podemos decir que el Derecho Informático es una rama de las Ciencias Jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática).[74]

Por otra parte, la Doctora Emma Riestra Gaytán señala que el Derecho Informático es el conjunto de normas jurídicas que regulan la creación de las nuevas tecnologías de la información, y de la comunicación en cualquier área, y relaciona los efectos jurídicos que de ella se desprendan en su aplicación.[75]

Para el Profesor Daniel Ricardo Altmark, el Derecho Informático "es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática".[76]

No cabe duda de que el Derecho Informático es una materia inequívocamente jurídica; "conformada por el sector normativo de los sistemas jurídicos contemporáneos,

---

[74] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pág.22.

[75] RIESTRA GAYTAN, Emma. Instituto Nacional de Ciencias Penales. *Curso de Introducción a los delitos Informáticos. La Experiencia Mexicana.* México, 4 al 20 julio 2000.

[76] ACEDO QUEZADA, Octavio R. *Op. Cit.*, pág.37.

integrado por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telepática. Asimismo integran el derecho informático las sentencias de los tribunales sobre materias informáticas y las proposiciones normativas, es decir, los razonamientos de los teóricos del derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar al sector normativo que disciplina la informática y la telepática; en este sentido, es claro que el derecho informático altera la concepción tradicional de la clasificación del orden jurídico".[77]

Ahora bien, si hacemos un estudio etimológico breve pero conciso del Derecho Informático, podemos hacer nuestra propia definición. En lo que respecta a la palabra Derecho, todos sabemos la diversidad de posibilidades en cuanto a su definición; sin embargo, todas llegan al mismo fin: regular la conducta del hombre dentro de la sociedad. En lo que respecta a la palabra Informática, el Maestro Julio Téllez Valdés nos dice que la Informática es: "La Ciencia del tratamiento racional, particularmente por máquinas automáticas, de la información considerada como el soporte de conocimientos humanos y de comunicaciones en los aspectos técnico, económico y social o bien [...]Conjunto de disciplinas científicas y de técnicas específicamente aplicables al tratamiento de datos efectuados por medios automáticos".[78]

De lo anteriormente expuesto, podemos recopilar información y hacer nuestra propia definición del Derecho Informático, quedando como sigue: Es el conjunto de normas mediante las cuales se regula la creación y utilización de los diversos medios o instrumentos electróni-

---

[77] *Idem*, pp.37-38.
[78] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pág.282.

cos-automatizados en los entornos social, económico y científico, para lograr un desarrollo informático pleno.

2.2 Generalidades del Derecho Informático

El intercambio intenso de mercancías más allá de aranceles y costumbres, la simbiosis de las culturas o mejor dicho, su adaptación y asimilación en nuevos contextos, la veracidad con que se transmiten informaciones de toda índole, forman parte de esa idea general a la que conocemos como globalización y que pone de manifiesto que la solución jurídica de estos problemas sea todavía confusa y enrarecida, ya que la rapidez con que suceden los cambios obliga a las personas y a las organizaciones a realizar modificaciones constantes, a fin de no perder el contacto ni quedar al margen de este flujo de innovaciones tecnológicas. De aquí que las distintas ramas del Derecho se vean afectadas. Cada día está tomando más cuerpo un Derecho de la Informática o Derecho Informático o Derecho de las Nuevas Tecnologías, según los autores, dado que el papel que juega el ordenador en la sociedad postindustrial hace emerger esta nueva rama del Derecho, todavía en el umbral de su desarrollo histórico, y cuyo contenido no ha sido más que parcialmente definido.

Si bien es cierto que los precursores informáticos nunca imaginaron los alcances que llegarían a tener las computadoras en general o aun en campos tan aparentemente fuera de influencia como el jurídico, todavía más difícil hubiera sido el concebir que el Derecho llegaría a regular a la Informática.[79]

De esta forma, a finales de los sesenta y luego de cerca de diez años de aplicaciones comerciales de las com-

[79] TÉLLEZ VALDÉS, Julio, *Ibidem.*, pág.57.

putadoras, empezaron a surgir las primeras inquietudes respecto a las eventuales repercusiones negativas motivadas por el fenómeno informático y que requerían un tratamiento especial.[80]

El Derecho de la Informática, como instrumento regulador en la sociedad, no ha sido estudiado igual que la informática jurídica, quizá porque sea dado más importancia a los beneficios que a los eventuales perjuicios que pueden traer consigo las computadoras.[81]

Pero dentro del reducido grupo de tratadistas sobre el Derecho de la Informática, tenemos a algunos que consideran al mismo como categoría propia que obedece a sus reglas, que surge como una inevitable respuesta social al fenómeno informático. Y que, por lo mismo, es un Derecho en el que su existencia precede a su esencia.[82]

Si el punto anterior implica dificultades, qué decir de la conceptualización de este Derecho de la Informática. Sin duda alguna que esta área, al igual que la informática jurídica, permite una creatividad muy amplia, sin que esto necesariamente trascienda a niveles demasiado imaginativos o especulativos.[83]

"[...], podemos deducir que el ordenador plantea nuevos problemas de tipo jurídico con los que se han de enfrentar los hombres dedicados a la creación, interpretación y aplicación de las leyes: se trata, como hemos dicho, del Derecho Informático, que va adquiriendo carta de naturaleza, aún cuando no está todavía universalmente consagrado como nueva rama del Derecho, aunque sí existen numerosas disposiciones legales, una variedad de jurispru-

---

[80] *Idem.*
[81] *Idem.*
[82] *Ibidem.*, pp.57-58.
[83] *Ibidem.*, pág.58.

dencia y bastantes textos doctrinales relativas al estudio de la materia".[84]

En España la materia no es aún, salvo en contadas excepciones cada día más numerosas, objeto de asignatura de estudio a nivel universitario, pero sí, frecuentemente, en cursos, seminarios y encuentros para intentar clarificar su contenido y también si debe o no constituir una asignatura autónoma, como el Derecho Procesal o el Derecho Mercantil, etc., o por el contrario analizarse y estudiarse en cada una de las disciplinas de la Facultad de Derecho, lo que haría más difícil su sistematización y encontrar especialistas en la materia, a excepción del Derecho Penal donde cada día va tomando cuerpo un Derecho Penal de la informática; pero también es necesario analizar las peculiaridades de los contratos informáticos, acceso a la información contenida en los bancos de datos, flujo de datos transfronterizos, *protección jurídica del software,* etc., que hacen prever, como apunta Mario G. Lozano, que en el futuro será necesario tratar sistemáticamente el Derecho privado de la informática, el Derecho público de la informática, el Derecho penal de la Informática, etc., lo que puede llevar a que la informática sea objeto de estudio simultáneo en las distintas ramas especiales del Derecho[...].[85]

Como podemos ver el Derecho Informático tiene un largo camino por recorrer iniciando con la filosofía, el derecho sustantivo y adjetivo, hasta el derecho procesal, ejemplificándose mejor de la siguiente manera: "El Filósofo debe bajar de su torre de marfil y profundizar en estas implicaciones de las nuevas tecnologías. Y el jurista, prever las implicaciones de estos hechos nuevos, en el hombre y la sociedad. Con las leyes de protección de datos, de

[84] Universidad Nacional de Educación a Distancia. *Op. Cit.,* pág.36.
[85] *Ibidem.,* pp.36-37.

bases de datos, de programas, etc., se está dotando de defensas a los individuos de ataques contra su intimidad, derechos de autor, y derechos patrimoniales, pero la cibernética (teoría de la regulación y control) y la informática (proceso automático de datos), afecta a muchas más situaciones que es preciso regular específicamente con una valoración ética, ideológica, para que no haya disociación entre la ciencia y la sociedad".[86] El Derecho Informático, antes o después, será una realidad, máxime cuando estamos en el convencimiento de que nos encontramos frente a un gran cambio en la civilización y por tanto también en el Derecho.

2.2.1 Principios Fundamentales del Derecho Informático

Una vez analizados los elementos básicos anteriores, toca el turno a los puntos torales del Derecho Informático.

Empecemos por los antecedentes del Derecho Informático el cual, siendo una nueva rama del conocimiento jurídico, es una disciplina en continuó desarrollo, teniendo en su haber -al menos hasta esta fecha- incipientes antecedentes a nivel histórico; sin embargo, podemos decir que las alusiones más especificas sobre esta interrelación -que, se verá con mas cuidado en el tema siguiente- las tenemos a partir del año 1949 con la obra de Norbert Wiener, en cuyo capitulo IV consagrado el derecho y las comunicaciones, nos expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico. Dicha interrelación se da a través de las comunicaciones, a lo que habría que mencionar que si bien estos postulados tienen cerca de

[86] BARRIUSO RUÍZ, Carlos. *Op. Cit.*, pág.91.

cuarenta años, en la actualidad han adquirido matices que probablemente ni el mismo Wiener hubiera imaginado.[87]

Por otra parte, en ese mismo año el juez norteamericano Lee Loevinger publicó un artículo de 38 hojas en la revista *Minnesota Law Review* titulado "The next step forward", en donde menciona que "el próximo paso adelante en el largo camino del progreso del hombre, debe ser el de la transición de la Teoría General del Derecho hacia la Jurimetría, que es la investigación científica acerca de los problemas jurídicos...[88]

Es importante mencionar que en la reiterada interrelación Derecho-Informática, en los términos de un Derecho Informático se contemplan una serie de implicaciones de orden social, económico, técnico, práctico y evidentemente jurídico, suscitadas por el uso de la informática [...],[89] lo que como se dijo anteriormente, se verá más explícitamente en el siguiente punto a tratar.

En función de su concepto, es notorio que la clasificación del Derecho Informático obedecerá a dos vertientes fundamentales: la informática jurídica y el derecho de la informática.

En lo que respecta a sus fuentes y para atribuir una eventual autonomía a esta disciplina jurídica, es menester hacer alusión, entre otras cosas, a aquellas de donde emana propiamente este conjunto de conocimientos.

A nivel interdisciplinario tenemos a aquellas provistas por el mismo Derecho, como es el caso de la legislación, que como ya mencionamos, es relativamente incipiente al respecto; sin embargo, aquí cabría señalar a aquellas disposiciones sobre otras áreas caracterizadas por

---

[87] *Ibidem.*, pág.21.
[88] *Ibidem.*, pág.22.
[89] *Idem.*

guardar un nexo estrecho con respecto al fenómeno informático, como es el caso de los ordenamientos en materia constitucional, civil, penal, laboral, fiscal, administrativa, procesal, internacional, etcétera.[90]

Asimismo, en cuanto a la jurisprudencia, doctrina y literatura sobre el particular, existen algunos pronunciamientos, teorías y artículos respecto a los problemas jurídicos suscitados por la informática.[91]

Por otra parte, en cuanto a las fuentes transdisciplinarias tenemos a aquellas provistas por ciencias y técnicas tales como la Filosofía, Sociología, Economía, Estadística, Comunicación, entre otras, y desde luego, la informática.[92]

Para un desarrollo informático adecuado es necesaria una planificación a través de normas, que a su vez conforman una política (en este caso informática) diferente de una legislación, en cuanto a que esta última se refiere a aspectos más específicos.

Así tenemos que dentro de esta política informática algunos de los principales puntos contemplados son el desarrollo adecuado de la industria de construcción de equipos de cómputo y de programación [...].[93] A diferencia de la política informática tenemos a la legislación informática, como un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso (fundamentalmente inadecuado) de la informática, es decir, que aquí se trata de una reglamentación de puntos específicos, [...].[94]

---

[90] *Ibidem.*, pág.58.
[91] *Idem.*
[92] *Idem.*
[93] *Ibidem.*, pág.59.
[94] BARRIUSO RUIZ. *Op. Cit.*, pág.17.

2.3 Relación entre Derecho e Informática

El progreso del Derecho debe ir paralelo al resto de disciplinas y al desarrollo social. Ya Hegel evidenció el nexo inescindible que vincula al hombre y sus construcciones intelectuales con la realidad que le sirve de marco; por lo que es tarea del investigador del derecho, adaptar éste para que pueda beneficiarse de los avances del proceso informático-cibernético o señalar las modificaciones técnico informático-cibernéticas precisas para su adaptación, compatibilidad y regulación jurídica.[95]

Si se tuviera que señalar una fecha precisa para el nacimiento de esta disciplina tendríamos que decir que fue el año de 1949.[96]

Del uso de los ordenadores o computadoras en el mundo jurídico se comenzó a hablar en los años en que nace la cibernética de Norbert Wiener; es decir, 1948. Las referencias que en tal obra se dieron influyeron probablemente en un artículo publicado un año después por Lee Loevinger en el que habla por primera vez de jurimetría; es decir, del uso de los ordenadores en el derecho.[97] En el año 1968 y después de estudiar un poco los fenómenos científicos que representaba la utilización de la computadora en el campo del Derecho, Mario Lozano propuso sustituir el término de "jurimetría" por el de "iuscibernética", [...].[98]

El avance de la tecnología informática en el campo del Derecho representa hoy en día, en nuestro medio, un importante y necesario campo de estudio que trate de delimitar los alcances y contenidos que derivan de esta re-

---

[95] BARRIUSO RUIZ, Carlos. *Op.Cit.*, pág.17.
[96] RÍOS ESTAVILLO, Juan José, *Op. Cit.*, pág.50.
[97] *Ibidem.*, pág.51.
[98] *Ibidem.*, pág.52.

lación. En el campo del estudio tradicional y desde un punto de vista integral, se ha señalado la importancia de estudiar la informática y el derecho desde dos perspectivas: por un lado, la informática jurídica; y por el otro, el derecho de la informática.[99]

Así pues se analizará brevemente cada una de las perspectivas antes mencionadas, con el fin de tener presente su ámbito de estudio e investigación.

Para el desarrollo de la informática jurídica es necesario considerar ciertos elementos de origen, como son la aplicación de la lógica del derecho o raciocinio jurídico análisis del discurso jurídico, aplicación de la teoría de los sistemas, aplicación de la teoría de la información, entre otras. Tales elementos constituyen la base fundamental para cumplimentar el objeto mismo de la informática jurídica.[100]

Al respecto, Marcelo Bauza señala que el punto de partida deriva de la constatación de un fenómeno: el razonamiento jurídico, el cual no constituye una operación aislada, sino que se íntegra dentro de un proceso compuesto de varias etapas. Cada una de las etapas en las que se desenvuelve este proceso constituye otros tantos sectores de desenvolvimiento para la informática jurídica, que requieren indudablemente de una fase de investigación pura como paso previo para desembocar luego en productos de aplicación concreta.[101]

Sin profundizar en el estudio de la lógica del raciocinio jurídico, se ha señalado que: el origen de la informática jurídica parte de un sistema lógico-interpretativo del mismo, ya que al respecto se ha determinado que la lógica del derecho es el estudio sistemático de la estructura de las

[99] *Cfr.* RÍOS ESTAVILLO. Juan José. Op. Cit. pág.1.
[100] *Ibidem.*, pág.45.
[101] *Idem.*

normas, los conceptos, y los razonamientos jurídicos[...]; esto es porque aluden siempre al orden del ser y aseveran que a tal o cual objeto conviene o no, tal o cual determinación.[102]

Lo anterior es porque quien trabaja para el desarrollo de la misma informática jurídica tiene como principal función la ordenación (que conlleva al tratamiento) y el análisis del discurso jurídico en el cual se anexan estudios del lenguaje jurídico, y su fin es la creación de instrumentos que permitan el acceso a la información jurídica.[103]

Por lo que concierne a su concepto, el Maestro Julio Téllez Valdés nos dice que: Informática jurídica es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación.[104]

Otro concepto que a nuestro juicio es el que nos da un panorama más amplio de esta área de estudio es el que define Enrique Cáceres: estriba en reconocer las propiedades necesarias y suficientes y así determinar los tipos de coordinación en conocimiento que se dan entre la informática y el derecho. Por tales motivos, relaciona estas materias entre sí como la documentalística, la lingüística, la lógica jurídica, la sociología, la estadística y la pedagogía (dependiendo de qué clasificación sea objeto de estudio).

La informática jurídica, vista como una forma de análisis u ordenación de la información jurídica, está dividida en diversas ramas:

---

[102] *Ibidem.*, pág.46.
[103] *Idem.*
[104] *Ibidem.*, pág.56.

a) Informática jurídica documental;
b) Informática jurídica de control y/o gestión y/o administración;
c) Informática jurídica de ayuda a la decisión y/o metadocumental y/o meta decisional.[105]

Por lo que respecta al Derecho de la Informática, lo primero a señalar es en cuanto a su integración terminológica, por la cual estamos en presencia de información automatizada, por lo que, al conjugarla con el derecho, lo primero que tenemos que determinar es precisamente algo jurídico, normativo y regulador de los efectos en el uso (activo o pasivo de una computadora).[106]

La irrupción del ordenador, la cibernética, la informática y la electrónica, en el tejido social, han hecho surgir unas regulaciones legales, cuyo objeto lo constituyen la tecnología electrónica, la informática y la cibernética. Lo que impone una regulación lo más completa posible para resolver todos los problemas socio-jurídicos que se presentan, permitiendo el ejercicio de los derechos, facultades, deberes y obligaciones.[107]

La interrelación de la informática y el derecho obliga, pues, a un profundo estudio de sus orígenes y sus posibles implicaciones y una sistematización y metodología de las normas dimanantes. Ya que esta interrelación posiblemente haga surgir una nueva rama del derecho, para la que hoy se generaliza el nombre de "Derecho Informatico", en caso contrario tendrá que potenciarse el estudio especifico dentro de cada una de las distintas ramas del derecho, hoy imperantes.[108]

---

[105] *Ibidem.*, pág.57.
[106] *Ibidem.*, pág.70.
[107] BARRIUSO RUÍZ, Carlos. *Op. Cit.*, pág.63.
[108] *Idem.*

El nuevo fenómeno, en cuanto tiene como objeto central a la persona y sus valores, e incide además abiertamente en los bienes de carácter patrimonial y contractual, extendiéndose a toda la materia de obligaciones y contratos, afecta en este caso especialmente a la rama jurídica ya consagrada del derecho civil.[109]

Pero también afecta en mayor o menor medida a todas las demás ramas del derecho entre las que destacamos: la filosofía del derecho, como responsable de fundamentar este nuevo hecho y coordinar las distintas partes implicadas: [...] la procesal, definiendo y valorando las pruebas efectuadas por medios electrónicos -informáticos y estableciendo procesos adecuados a la realidad informática: *la penal,* con el cometido de tipificar y sancionar las nuevas acciones y conductas delictivas que surgen; la administrativa, estableciendo procedimientos más ágiles, etc.[110]

El Derecho Informático, la Informática como objeto del Derecho, comprende actualmente:

a) La protección de la intimidad, datos personales, programas de ordenador, bases de datos.
b) Contratos informáticos.
c) Responsabilidad civil derivada de la informática.[111]
d) La contratación realizada por medios electrónicos.
e) Prueba en el proceso judicial a través de sistemas electrónicos e informáticos.
f) Falta y delito informático.
g) Mundo laboral; legislación, etc.

---

[109] *Ibidem.*, pp.63-64.
[110] *Ibidem.*, pág.64.
[111] *Idem.*

De lo anteriormente expuesto se puede concluir que los abogados debemos abocarnos más al estudio, análisis y regulación de la relación que hay entre el Derecho y otras ciencias, en nuestro caso la Informática, como lo señala Barriuso Ruíz: Afrontamos con el rigor crítico necesario la interacción del Derecho y la Informática, señalando la trascendencia que subyace al desarrollo del universo de los ordenadores y de la cibernética, proyectados al campo Jurídico-Social y a su vez como objeto mismo del Derecho, constitutivos de la Informática Jurídica y del Derecho Informático.[112]

2.4 Concepto de Propiedad Intelectual

Concepto que comprende aquellos derechos que se ejercen sobre bienes incorpóreos como lo son la producción artística, científica o literaria, es decir, los llamados derechos de autor, asimilando estos derechos y su ejercicio a los derechos de propiedad. Asimilación fundamentada en la equiparación teórica de la explotación exclusiva de los beneficios que tales producciones generan con las formas de apropiación y posesión, y en que a esa explotación también le son aplicables los atributos de la propiedad (goce y disposición).[113]

Comprende, pues, diversas especies dependiendo del tipo de producción a que se refiera: propiedad artística, propiedad dramática, propiedad científica y propiedad literaria.[114]

---

[112] BARRIUSO RUÍZ, Carlos. *Op. Cit.*, pág.15.
[113] INSTITUTO DE INVESTIGACIONES JURÍDICAS. *Diccionario Jurídico Mexicano.* Porrúa, Novena Edición, México, 1996, v.4., pág.2606.
[114] *Idem.*

Por otro lado también tenemos otro concepto más formal en cuanto a la naturaleza de éste, el cual dice así: La denominación del concepto ha sido muy debatida en la doctrina, al igual que la teoría en que se sustenta. Inicialmente se consideraba que la llamada propiedad de bienes corporales, inclusive era susceptible de adquirirse vía prescripción positiva. Ante esta postura se argumenta que los derechos de autor no son un derecho de propiedad, ya que la protección que la ley concede a los autores se limita a la reproducción e imitación de la obra sin el consentimiento del autor o sus herederos.[115]

Oscar Morineau (citado en Rojina Villegas, p.557) rescata el concepto de propiedad intelectual afirmando que "es indiferente que a un fenómeno se le llame A o B, con tal que separamos la naturaleza del objeto designado por la palabra"; lo importante, es la protección jurídica que se le da a determinada creación de la inteligencia.[116]

En este contexto, son tres los requisitos para la existencia jurídica del derecho de propiedad intelectual: a) la manifestación externa de la idea; b) la existencia de una norma jurídica que reconozca una facultad o atribución al autor de esa manifestación, y c) el ejercicio de la facultad concedida por la norma, mediante el registro de la obra intelectual.[117]

Y por último, otro punto relativo al concepto de propiedad intelectual es aquel por el cual se le entiende "como el conjunto de normas que regulan las prerrogativas y beneficios que las leyes reconocen a favor de los autores y de sus causahabientes por la creación de obras artísticas, científicas, industriales y comerciales."[118]

---

[115] *Idem.*

[116] *Ibidem.*, pp.2606-2607.

[117] *Idem.*

[118] RANGEL MEDINA, *David. Panorama del Derecho Mexicano.* McGraw-Hill, México, 1998, pág.1.

En la medida que las obras apuntan a la satisfacción de sentimientos estéticos o tienen que ver con el campo del conocimiento y de la cultura en general, las reglas que las protegen integran la propiedad intelectual en un sentido estricto o derecho de autor y atañen al campo de los derechos de autor de los creadores intelectuales en su acepción más amplia.

2.4.1 Relación entre Derecho Informático y Propiedad Intelectual

Una de las dialécticas más interesantes que la materia plantea es la que se deduce de la relación entre la creación intelectual de productos informáticos y las normas que el Derecho ha arbitrado para proteger los derechos de sus autores. Como dice nuestro Legislador, la propiedad intelectual es un "supraconcepto" que engloba los derechos personales y patrimoniales que la Ley reconoce en exclusiva al autor sobre su obra. Con ello se asegura al creador toda una variada gama de posibilidades de actuación sobre las distintas vertientes de su obra, pues le permite adoptar toda una serie de "decisiones" con respecto al destino y explotación del objeto del derecho. No obstante, hemos de tener muy presente la función social que cumplen las obras artísticas, literarias y científicas, razón por la cual son muy diversas las limitaciones que la Ley impone en este campo de actuación de la voluntad humana.[119]

De otro lado, a nadie escapa hoy la relevante dimensión económica que estas obras poseen en muchos casos y que se acentúa en el campo de las creaciones de

[119] Universidad Nacional de Educación a Distancia. *Op. Cit.*, (volumen I), pág.902.

productos informáticos. Efectivamente, el "mercado de la cultura" forma parte de los sectores más dinámicos y crecientes de nuestros días. Ello se debe, entre otras razones, a la pluralidad de objetos en que puede plasmarse tal y como las leyes sobre la materia se encargan de reflejar con una encomiable visión de futuro. Libros, impresos, obras, planos, etcétera, forman parte de ese versátil y flexible conjunto de obras originales "expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro", a las que la Ley protege atribuyendo a los autores la propiedad sobre las mismas.[120]

Estamos pues ante una realidad material o inmaterial que es producto de la actividad creadora de la persona, plasmada en un soporte material o inmaterial que le hace perceptible, que aporta un "quid novi" al patrimonio artístico, literario o científico precedente y sobre el cual la Ley confiere una serie de derechos, "ab origine", a su autor. Tal protección se dispensa con independencia de factores como su valor o mérito, su utilidad o de que se comunique públicamente o no. Como puede deducirse de la legislación sobre la materia, el campo de actividades humanas en las que pueden producirse obras protegidas es muy diverso, pues abarca desde las "tradicionales" como pintura, literatura, escultura, música, docencia, dramaturgia, cinematografía o fotografía, hasta otras propias de las ciencias empíricas o de la técnica como ingeniería, arquitectura, topografía o geografía.[121]

Lógicamente, la informática como campo de la actividad humana en la que se producen creaciones intelectuales, no podía quedar ajena a este fenómeno pues era necesario proteger los derechos de las personas y empre-

[120] *Ibidem.*, pp.902-903.
[121] *Ibidem.*, pág.903.

sas dedicadas a la investigación y desarrollo de nuevos productos. Sin embargo, se planteaba el problema de que, inicialmente, los productos informáticos poseían una aplicación básicamente industrial o militar. [...]. En consecuencia, es lógico pensar que los primeros equipos tenían unas aplicaciones muy claras y determinadas por lo que se atendió a protegerlos atendiendo a su dimensión industrial, razón por la cual su tutela quedó adscrita al campo de las normas de la Propiedad Industrial. En principio, el centro de atención lo integraban los equipos (hardware), cuyo costo y limitaciones hacían muy restringida su utilización a determinados ámbitos y tareas. Sin embargo, con la difusión de los ordenadores por su aplicación a otros distintos ámbitos de la actividad humana, se acentuó su capacidad multifuncional pues un mismo equipo podía ya realizar muy diversas tareas en función de las instrucciones que se le facilitaran. Emerge así la importancia de un nuevo elemento que permite adaptar el ordenador a muy diversos usuarios y destinos: los programas o soporte lógico (software). Ellos permiten que personas no preparadas específicamente para programar un ordenador puedan obtener de éstos toda una diversidad de utilidades: laborales, de ocio y recreo, de comunicación y de tratamiento de información. He aquí pues un nuevo y relevante elemento, producto de la capacidad creadora del ser humano, que aporta nuevas metas y soluciones y que ha de ser protegido adecuadamente: el programa de ordenador.[122]

Por otra parte, es de sobra conocido que nuestra época es conocida como la de la "sociedad de la información", dado que ésta se ha erigido como el más deseado instrumento de poder económico y político. Pero el problema no es sólo adquirir la información, sino saber

[122] *Ibidem.*, pp.903-904.

sistematizarla y relacionarla adecuadamente según la finalidad perseguida. Ello quiere decir que no basta con almacenar información, sino que hemos de contar con un instrumento que permita al ordenador poder tratarla adecuadamente para las distintas finalidades que se puedan perseguir. Es por ello que las bases de datos poseen hoy tal relevancia que se hace necesario dotarlas también de protección jurídica adecuada en su faceta de objeto de propiedad intelectual.[123]

Del estudio de esta relación se desprende la importancia de la protección de los derechos intelectuales de los programadores; ¿pero dónde queda su responsabilidad como tales en los casos en que estos mismos crean programas para realizar actos de piratería o también cuando crean herramientas (hardware) para realizar dichos actos e inclusive al utilizar a las computadoras u ordenadores?. Este es el punto medular del presente estudio así como de su propuesta. Durante el estudio y análisis del presente trabajo hemos de demostrar que estos personajes de la informática tienen una gran responsabilidad al crear tanto "Software" como "Hardware", pues saben y entienden las consecuencias de sus actos siendo que estas creaciones tienen un fin cierto y único, y que debe ser un delito sancionado tanto por la Ley Federal de Derechos de Autor en primera instancia y seguidamente por el Código Penal Federal, que a mi parecer es donde debe de tipificarse esta conducta.

[123] *Ibidem.*, pág.904.

CAPÍTULO TERCERO

DELITOS INFORMÁTICOS

3.1 Origen de los Delitos Informáticos

Es indudable que así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un instrumento u objeto útil en la comisión de verdaderos actos ilícitos. Este tipo de actitudes concebidas por el hombre -y no por la máquina, como algunos pudieran suponer- en cuentran sus orígenes desde el mismo surgimiento de la tecnología informática, ya que es lógico pensar que de no existir las computadoras, estas acciones no existirían. Por otra parte, la misma facilitación de labores que traen consigo dichos aparatos propició que en un principio el usuario se encontrara ante una situación de ocio, la cual canalizaba a través de las computadoras, cometiendo, sin darse cuenta, una serie de ilícitos, pues en ese tiempo aún no estaba tipificado y más aún no se le daba la importancia necesaria ni se le otorgaba el valor jurídico a las consecuencias que pudiera traer el dejar en libertad total el uso indiscriminado de las computadoras u ordenadores por parte de personas capacitadas, ya no sólo para la realización de trabajos específicos en sus empleos sino por medio de sus conocimientos profesionales y/o técnicos. Esta gente podía llevar a cabo actos ilícitos sin un medio que los detuviera y aun sigue sin detener actualmente. Para que la sociedad viva como tal, es imprescindible la regulación de estos avances tecnológicos, ya sea por

los mismos medios tecnológicos o más rígidamente, de una forma jurídica-penal.

Por otro lado, con el mismo egoísmo humano se establece una especie de "duelo"entre el hombre y la máquina, lo cual en última instancia provoca el surgimiento de ilícitos en su mayoría no intencionados, por ese "deseo" del hombre de demostrar su superioridad frente a las máquinas, y en este caso específico las computadoras. Veremos también, posteriormente, qué tan intencionados o no intencionados pueden ser estos actos, pues dependiendo del sujeto que lo realiza y basándonos en sus conocimientos podemos dar nuestro punto de vista.

Por último, también está el querer demostrar a los demás y en casos particulares al "Estado represor" que se puede más que él, el burlar su seguridad tanto técnica como jurídica, el poder violentar sin ejercer violencia física o moral, sólo con su inteligencia y una computadora, el realizar actos que pueden destruir a una empresa, una Secretaría de Estado, e inclusive atacar áreas estratégicas de un país en actos terroristas; en fin, son muy variadas las conductas, las cuales pueden ser como ya se dijo por diversas causas, pero en este estudio trataremos particularmente la piratería de software así como de hardware; también se verán los sujetos del delito, los cuales se analizarán más adelante con sus características propias así como el modo de realizar el delito, el cual no deja de sorprender aún a estas alturas donde se ha tipificado como conducta antijurídica, y sin embargo se sigue realizando, principalmente por intereses económicos tanto nacional como mundialmente.

Según el maestro Julio Téllez Valdés podemos decir que estas acciones, más que resultado de una situación socioeconómica, se derivan de una actitud antropológica y psíquica, aunque en el terreno de los he-

chos son una realidad sociológica bien determinada y que requiere, por ende, de un tratamiento jurídico específico.[124]

Ciertamente son diversas las causas que provocan estas conductas, pero difiero de la opinión del maestro Julio Téllez Valdés en cuanto a que la situación socioeconómica en la actualidad, sí es determinante, principalmente en las conductas de piratería, tema de este estudio. Por ejemplo cuando una persona contacta a otra que tiene la capacidad y conocimientos técnicos en cuanto al área de informática para poder realizar-crear programas (software) o equipo (hardware) con fines ilegales; la primera persona le pagará al creador cierta cantidad de dinero la cual éste no podría acceder en un trabajo normal, por lo que no es muy difícil encontrar que dichos técnicos se presten y acepten el pago para crear programas o equipo con las características técnicas necesarias.

Otro medio diferente pero que en esencia reproduce la conducta anterior, es la que se realiza en empresas, en sus áreas de creación y producción. Una de estas y quizá la más conocida es Microsoft, en cuyas áreas se realizan o más bien dicho se crean, por medio de trabajadores-técnicos -previa orden-, programas y equipos para realizar copias -las cuales no dejan de ser ilegales-, pero por ser una empresa con todas las características y requisitos legales para realizar sus labores no son perseguidos por ello, pero independientemente de si tienen o no facultad para ello o si tiene permiso previo del propietario, está el que los programas que utilizan para realizar copias, así como sus equipos salen posteriormente al mercado sin restricción de ningún tipo, mucho menos penal, logrando así que personas independientes y con recursos económicos puedan comprar estas herramientas de trabajo y reali-

[124] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pág.103.

zar así actos ilícitos de piratería. Con esto quiero llegar a las preguntas siguientes: ¿dónde queda la responsabilidad de los programadores independientes y en su caso de los dueños de las grandes empresas (persona moral), quienes ordenan a sus propios programadores crear programas o equipo con determinadas características y de acuerdo a necesidades palpables y de facto?.

Una factor más que no puede quedar sin mencionar es que, según palabras textuales de un ingeniero en informática, expresadas en el Curso de Introducción a los Delitos Informáticos al cual asistí: "nosotros creamos programas dañinos ocasionalmente para terceros e inclusive para nuestro patrón, como una forma de protesta ante éste por la explotación de que somos objeto en cuanto a nuestros conocimientos y la aplicación de éstos, y por su mala paga principalmente y que en algunos casos el patrón se queda con nuestros inventos y no recibimos nada a cambio siendo que nosotros somos sus padres, por lo cual paralelamente creamos otro programa de seguridad el cual nos traerá un beneficio a nosotros, ya sea económico o el mantenernos en el trabajo como elemento indispensable para la empresa, y también es una forma de atraer mercado de usuarios caseros dañando sus equipos y posteriormente ofrecer nuestros servicios obteniendo ganancias considerables, y en otros casos específicos como una protesta ante el Estado o Gobierno por causas diversas; éstas pueden ser culturales, sociales, económicas e inclusive terroristas, entrando a sus sistemas o redes y manifestarlo o simplemente destruir todo lo que se encuentre en éstos[...]".[125]

Es así como nos proponemos señalar que estos sujetos tienen una responsabilidad amplia, plena y clara que se puede regular mediante la creación de subprogramas

[125] Instituto Nacional de Ciencias Penales. *Curso de Introducción a los delitos Informáticos*. México, 4 al 20 julio 2000.

que impidan la realización de actos de piratería, así como la creación de equipo el cual conjuntamente con el programa principal , hace posible la existencia ilícita de copias ilegales de software. Con esto la autoridad puede tener un amplio control de quien crea, produce y tiene en su propiedad los elementos físicos y técnicos que en un caso determinado, hayan podido hacer copias ilegales, definidas penalmente como actos de piratería.

3.1.1 Definiciones de delito

Al incluir en la definición de delito busco tener presente el fundamento desde el cual pretendemos hacer responsable de su conducta al sujeto -programador o, en su caso persona moral-, básandonos en primera instancia en el concepto mismo de delito y en segunda instancia en el párrafo segundo del artículo séptimo del código penal, como responsable por omitir o al actuar dolosamente al no llevar a cabo determinada conducta -la cual se desarrollará más adelante-, con el fin de proteger y evitar a la vez al máximo la creación, el uso de programas y equipos para realizar la conducta delictiva, mejor conocida como piratería, en su modalidad de realizar copias ilegales de programas (software) que manejan o utilizan las computadoras a nivel general.

Pasando a la definición, veremos a continuación diferentes conceptos que sin embargo presentan ciertas coincidencias, pues siempre ha habido dentro de la sociedad entera el interés de proteger y salvaguardar los derechos de la misma ante los diversos actos delictivos y por ende definir lo que es delito, como una forma previa de señalar las conductas que forman parte de éste, las cuales están prohibidas y sancionadas por la Ley penal. Si bien es cierto que estas definiciones ya estaban conceptualizadas como

tales, también lo es que han ido cambiando de acuerdo a su tiempo específico así como a los avances tecnológicos, en nuestro caso; un ejemplo de esto es el texto siguiente expresado por el maestro Fernando Castellanos Tena: "El delito ha existido siempre, vieran ustedes qué novedades, pero no siempre se ha visto de igual manera, por eso el concepto va variando con el tiempo; sin embargo los estudiosos como lo saben mejor que yo, con investigaciones realizadas en distintos pueblos y en distintas épocas, han logrado advertir en casi todos, ciertas similitudes, ciertas semejanzas, porque en determinado tiempo y época, ha preponderado el principio que permite ubicar aquella época, conjuntamente con la de otros pueblos y de otros tiempos, [...]".[126]

Ciertamente el Maestro Fernando Castellanos Tena habla de que el concepto de delito siempre ha existido; tiene razón, éste sólo a cambiado. Podríamos inclusive aplicar el principio matemático que señala que "la energía no se crea ni se destruye, sólo se transforma"; asimismo el delito se transforma de acuerdo al avance de la propia sociedad, pero conservando sus características esenciales así como sus fines.

La teoría del delito nos dice que el delito es la conducta típica, antijurídica y culpable, a la que se asocia una pena como consecuencia. Afirmada la existencia del delito, procede la consecuencia o aplicación de la pena.[127]

Partiendo de esto, el primer concepto de delito a estudiar se encuentra en el Título primero, sobre la Responsabilidad Penal, Capítulo I de las Reglas sobre Delitos y Responsabilidad, artículo séptimo del Código Penal, el

---

[126] *Cfr.* CASTELLANOS TENA, Fernando. *Concepto de Delito. Antología Jurídica 1992-1996.* Consejo Nacional de Egresados de Posgrado en Derecho, Poder Judicial del Estado de Morelos, 1997. pág.419.

[127] RÍOS ESTAVILLO, Juan José. *Op. Cit.*, pág.114.

cual dice así: "Delito es el acto u omisión que sancionan las leyes penales"[128] [...].

Según José Arturo González Quintanilla, "el delito es un comportamiento típico, antijurídico y culpable". Contempla al delito como una estructura técnica, utilizando el tipo como el dato que le da unidad fenomenológica.[129] El tipo lo definimos como la descripción de la conducta, cuya realización la hace acreedora de pena y viene a ser la fuente de la punibilidad. [...].[130]

Es importante tener presente la forma en que otros países definen al delito. Un ejemplo de esto es el código penal español, en el cual se encuentra el concepto de delito en el artículo diez, señalándolo como sigue: "*son delitos o faltas las acciones y omisiones dolosas o imprudentes penadas por la Ley*". Un sector de la doctrina ha tendido a darle un significado dogmático-conceptual a este precepto. Lo cierto es que resulta difícil encontrar en él los componentes del delito, esto es, tipicidad, antijuricidad y culpabilidad y aun punibilidad. Está claro que no es una definición completa, pues no hay una alusión a los elementos antijuricidad y culpabilidad. Todo lo más se podría observar una referencia a la tipicidad y a la punibilidad, con la reserva de que esta última como elemento del delito, según se ha visto, resulta discutible, pues no hace referencia a su estructura [...] Pensamos que su papel es mucho más limitado, pero no menos importante. Si sólo hace alusión a la tipicidad, quiere decir que su función no es dogmática sino político criminal, pues establecería el principio

---

[128] *Código Penal para el Distrito Federal. Leyes y Códigos de México.* 59ª edición. Porrúa, 2000, pág.8.

[129] Estudio filosófico de los fenómenos, que consiste esencialmente en describirlos y en descubrir las estructuras de la conciencia que tienen que ver con ellos. Diccionario Enciclopédico Larousse, tercera edición, 1998, pág.445.

[130] GONZÁLEZ QUINTANILLA, José Arturo. *Derecho Penal Mexicano.* Porrúa, México 1997, cuarta edición, pág.193.

"*nullum crimen nulla poena sine lege*", [131] El cual señala en general que no habrá crimen ni mucho menos pena si la conducta no esta previamente regulada.

Una definición de delito más amplia y en la que podemos ver sus características principales es la que nos da el Diccionario de Derecho Procesal Penal, el cual define al delito como: Acto u omisión que sancionan las leyes penales. Acción punible entendida como el conjunto de los presupuestos de la pena. Infracción culpable de la norma penal. Su concepto ha variado en el tiempo, según la Doctrina y las legislaciones. Sin embargo, en términos generales, se les reconocen las siguientes características partiendo de la definición más común: Delito es la acción típica, antijurídica y culpable; de esto se deduce: es una acción penal humana; lo que no es acción no interesa al Derecho Penal. Típica, porque la acción tiene que concordar con lo descrito en la norma penal. Antijurídica, porque la acción penal debe oponerse al orden jurídico penal vigente y no estar justificada por una causa de exclusión del injusto. Culpable, por que puede reprocharse al agente, intencionado o negligente, del delito cometido, dada la relación de causalidad existente entre el agente y su acción. El delito es punible, porque está sancionado expresamente con una pena señalada en la norma penal. Al efecto el Código Penal establece: Articulo 7°.– "Delito es el acto u omisión que sancionan las leyes penales."[132]

Por último y sólo como una forma de ratificar la coincidencia entre la mayoría de los autores la teoría del delito, tenemos la definición dada por Esteban Righi y

---

[131] BUSTOS RAMÍREZ, Juan J., HORMAZÁBAL MALARÉE, Hernán. *Lecciones de Derecho Penal.* Trotta, Madrid, 1999, v.II, pp.24-25.

[132] DÍAZ DE LEÓN, Marco Antonio. *Diccionario de Derecho Procesal Penal y de Términos usuales en el Proceso Penal.* Porrúa, México, 1997, tomo I, tercera edición, pág.641.

Alberto A. Fernández: "[...], podemos concluir que el delito puede ser definido como una acción típica, antijurídica y culpable."[133]

Como podemos ver la mayoría de las definiciones anteriores concuerdan, convirtiéndose en un claro ejemplo de lo expresado por el Maestro Fernando Castellanos Tena. Y por lo que respecta a nuestra opinión, creemos en la teoría del delito la cual ya fue expresada en un principio, como el medio para definir y tipificar a los "delitos informáticos".

Por lo que respecta al segundo párrafo del artículo mencionado al inicio, lo debemos tener en cuenta a lo largo del presente estudio por las características propias de la conducta del sujeto a tipificar. Este párrafo segundo dice así: "En los delitos de resultado material también será atribuible el resultado típico producido al que omita impedirlo, si éste tenía el deber jurídico de evitarlo. En estos casos se considera que el resultado es consecuencia de una conducta omisiva, cuando se determine que el que omite impedirlo si éste tenía el deber de actuar para ello, derivado de una ley, de un contrato o de su propio actuar precedente".[134]

3. 2 Definición de Informática

Por lo que respecta a este punto y dando continuidad a lo que concierne a esta rama de apoyo para la cibernética, consideramos que la definición más adecuada para ello es la que nos da Europa y en particular España: "La informática (Computer Science) son los conocimientos científicos

[133] RIGHI, Alberto / FERNÁNDEZ, Alberto A. *Derecho Penal. La Ley. El Delito. El proceso y la pena.* Hammurabi S.R.L. Buenos Aires. 1996, pág.121.
[134] *Código Penal para el Distrito Federal. Leyes y Códigos de México. Op. Cit.*, pág.8.

y técnicos que hacen posible el proceso de datos con medios automáticos y electrónicos. La información (Computerización) es la automatización de los procesos por medio de ordenadores".[135]

Hemos de considerar a esta definición como aquella que se ha de ocupar para futuras comparaciones y análisis de conductas ilícitas en los siguientes apartados, en los cuales es importante tener ya presente qué es la informática y los medios que la conforman, para tener una visión de cómo interactúan entre sí el ser humano y la computadora y viceversa. Teniendo ya establecido este punto pasemos al análisis de los conceptos típicos y atípicos, los cuales tienen también una relación muy estrecha con la definición de la informática.

3. 3 Concepto Típico y Atípico

Antes de conocer dichos conceptos, es importante tener presente la definición y características del tipo y la tipicidad, así como de la atipicidad, para tener más claro los posteriores conceptos a manejar. Iniciemos pues con el tipo: "es así como la expresión tipo es usualmente utilizada por la doctrina para aludir a la descripción de una conducta prohibida realizada por una norma jurídico-penal, en tanto que la tipicidad es atendida como la característica de una acción de adecuarse a una disposición legislativa. Por ello, en derecho penal se dice que un comportamiento es típico cuando coincide con lo previsto en un tipo penal [...].[136]

Es evidente, en consecuencia, que aun cuando las expresiones tipo y tipicidad son conceptualmente di-

---

[135] Ver *Supra.*, pág.17.
[136] INSTITUTO DE INVESTIGACIONES JURÍDICAS. *Op. Cit.*, pág.3091.

versas, deben ser tratadas conjuntamente ya que son notoriamente interdependientes.[137]

El tipo penal es un instrumento legal, lógicamente necesario y de naturaleza predominantemente descriptiva; que tiene por función la individualización de conductas humanas penalmente relevantes (por estar penalmente prohibidas).[138] El tipo pertenece a la Ley. Es en la Ley donde hallamos los tipos penales: en la "parte especial" del Código Penal y en las leyes especiales, [...] "tipos" son las fórmulas legales mismas de la especie que mencionamos, es decir, las fórmulas que nos sirven para individualizar las conductas que la ley penal prohíbe.[139]

En cuanto a las características del tipo podemos decir que: el tipo es lógicamente necesario, por que sin el tipo no podríamos averiguar la antijuricidad y la culpabilidad de una conducta que, en la mayoría de los casos, resultaría sin relevancia penal alguna. Así por ejemplo, si tuviésemos que averiguar si es delito la falta de pago de una cuota del precio de compra de un lavarropa y dispusiéramos del concepto del tipo penal, primero veríamos que se trata de una conducta; luego comprobaríamos que la conducta es antijurídica porque el incumplimiento de una obligación civil es contrario a derecho; luego comprobaríamos que es culpable y, por último, después de todas esas verificaciones, resultaría que esa conducta antijurídica y culpable no es delito porque no está conminada con una pena por la Ley Penal. De esto depende nuestra afirmación de que el tipo es lógicamente necesario para una racional averiguación de la delictuosidad de una conducta.[140]

---

[137] *Idem.*

[138] ZAFFARONI, Eugenio Raúl. *Manual de Derecho Penal.* Parte General, 4ª reimpresión. Cárdenas Editor. México, 1998, pág.408.

[139] *Idem.*

[140] *Ibidem.*, pág.392.

El tipo es predominantemente descriptivo porque los elementos descriptivos son lo más importantes para individualizar una conducta y, entre ellos, de especial significación es el verbo, que es precisamente la palabra que sirve gramaticalmente para connotar una acción.[141] La función de los tipos es la individualización de las conductas humanas que son penalmente prohibidas. De esta función depende la necesidad lógica del tipo, de la que nos hemos ocupado.[142]

Por lo que respecta al tipo y a la tipicidad, es importante mencionar que: "No debe confundirse el tipo con la tipicidad. El tipo es la fórmula que pertenece a la ley, en tanto que la tipicidad pertenece a la conducta. La tipicidad es la característica que tiene una conducta en razón de éstas, adecuada a un tipo penal, es decir, individualizada como prohibida por un tipo penal, [...] Típica es la conducta que presenta la característica especifica de tipicidad (Atípica la que no la presenta); tipicidad es la adecuación de la conducta a un tipo; tipo es la fórmula legal que permite averiguar la tipicidad de la conducta."[143]

[...] la tipicidad se traduce en la adecuación de una conducta a un tipo, resultando de esto que en la materia criminal la tipicidad se obtiene de la comparación que haga el órgano jurisdiccional de la acción particular, concreta y temporal, que realiza el agente, con el texto genérico, abstracto y permanente de una ley (típica), para ver si existe entre ellas una adecuación: desprendiéndose de esto que el tipo viene a ser ese enunciado normativo perteneciente a la legislación, [...] salta a la vista la importancia del tipo, ya que para que una conducta sea punible se requiere

[141] *Idem.*
[142] *Ibidem.*, pág.393.
[143] *Idem.*

de la tipicidad, entendida como la adecuación de la acción a un tipo como descripción legal que en forma abstracta la prevé. La conducta es típica si puede clasificarse en un tipo, es decir, en una de las descripciones legales del aspecto externo de la acción punible.[144]

La acción típica es sólo aquella que se acomoda a la descripción objetiva, aunque saturada a veces de referencias a elementos normativos y subjetivos del injusto de una conducta que generalmente se reputa delictuosa, por violar, en la generalidad de los casos, un precepto, una norma, penalmente protegida. La tipicidad es la exigida correspondencia entre el hecho real y la imagen rectora expresada en la Ley en cada especie de infracción. Adecuación típica significa pues, encuadramiento o subsunción de la conducta principal en un tipo de delito y subordinación o vinculación al mismo de las conductas accesorias.[145]

Se concluye así que típico es todo aquello que incluye en sí la presentación de otra cosa y, a su vez, es emblema o figura de ella.[146]

Es importante mencionar que el tipo penal de "delitos informáticos" no está tipificado como tal en nuestra legislación; sin embargo, hay una urgente necesidad de esto pues cada día que pasa se llevan a cabo muchas conductas delictivas, las cuales se pueden y deben ubicar dentro de los "delitos informáticos".

Como una forma más clara y explicativa de este fenómeno, a continuación hago mención de la opinión del Maestro Julio Téllez Valdés, la cual dice así: "dar un concepto sobre delitos informáticos no es labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el

---

[144] DÍAZ DE LEÓN, Marco Antonio. *Op. Cit.*, pág.2559.
[145] *Ibidem.*, pág.2560.
[146] *Ibidem.*, pág.2566.

sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos-penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos, –por lo que respecta a este punto España ya tiene actualmente tipos penales en cuanto a esta conducta los cuales los identifica como "delitos telemáticos", los cuales se verán más ampliamente con posterioridad– no ha sido objeto de tipificación aún;[...].[147]

Por otro lado, señala Juan José Ríos Estavillo que: "para poder determinar la posible existencia de los delitos informáticos, es necesario determinar que se debe recurrir precisamente a las dos materias que integran la relación de la que hemos venido hablando en el transcurso del presente estudio y son: la informática y el derecho, en la cual cada una aporta su horizonte de proyección".[148]

Respecto a la informática, necesitamos recurrir a ella para conocer cuáles son las conductas que la comunidad científica-tecnológica considera que deben protegerse por el derecho, mientras que el derecho debe indagar qué es el delito, para posteriormente cuestionar si la utilización masiva de las computadoras y la telemática pueden cambiar la naturaleza y alcance de la Ley Penal.[149]

Cuando queremos averiguar qué es delito informático necesariamente debemos buscar la respuesta en la parte especial del Código Penal, pero aquí surgen algunas posibles interrogantes: ¿en el Federal, en el local, en las leyes penales especiales?.[150]

La legislación penal en México está compuesta por el Código Penal en Materia Federal en todo el país y

[147] TÉLLEZ VALDÉS, Julio, *Op. Cit.*, pp.103-104.
[148] RÍOS ESTAVILLO, Juan José. *Op. Cit.*, pág.114.
[149] *Idem.*
[150] *Ibidem.*, pp.114-115.

en Materia Común en el Distrito Federal, además de las normas penales que como apéndices se encuentran dispersas en leyes, sobre todo administrativas federales, y los ordenamientos estatales que reproducen la situación antes prevista.[151]

Las estadísticas sobre tipos penales varían. Al efectuar un análisis documental legislativo respecto a este problema podemos afirmar que, con excepción del estado de Sinaloa, [...] en nuestro país, ya sea a nivel federal o local, los delitos informáticos, como tales, no existen, ya que los mismos no se encuentran tipificados.[152]

La desventaja la encontramos en la confusión, en llamar "delito" o "crimen" a lo que posiblemente sólo sea una conducta indebida, ilícita o ilegal, y que en el campo de la informática podría ser considerada de protección penal en el futuro – desde mi punto de vista no es a futuro sino aquí y ahora–[...].[153]

Para tratar a los delitos informáticos, María de la Luz Lima define el delito por computadora como cualquier acto ilícito penal en el que las computadoras, su técnica y funciones desempeñan un papel ya sea como método, medio o fin.

Otras definiciones citadas por dicha autora son:

- Aquellos en que se utiliza una computadora como instrumento u ocupación criminal.
- Delito en el campo de la información: cualquier acción ilegal en la que la computadora es el instrumento u objeto del delito (Ticdemann).

---

[151] *Ibidem.*, pág.115.
[152] *Idem.*
[153] *Ibidem.*, pág.116.

– Algunos autores prefieren hablar de abusos de computadoras. Señalan que son aquellos actos asociados con la tecnología de la computadora, en los cuales una víctima ha sufrido una pérdida y el autor intencionalmente ha obtenido una ganancia (Parker).[154]

Otra definición es: "Cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadoras 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. También comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras o los datos contenidos en la misma, en la base, sistema o red.[155] (Proyecto de Ley Informática del Ministerio de Justicia de Chile).

Como podemos darnos cuenta conceptos hay muchos, pero ninguno señala que hay una regulación típica de estos delitos, salvo como ya se dijo en Sinaloa, pero sólo como fuero Local y no Federal –en España ya hay tipos penales–; es por esto que proponemos la regulación de los mismos y en especial la tipificación de la conducta propuesta, las cuales una vez tipificadas darían buenos resultados en cuanto se trataría primeramente de persuadir a infractores y posteriormente, si continúan, aplicarles una pena, un castigo sin fianzas ni prerrogativas.

Como parte de lo anteriormente expuesto podemos citar al Maestro Julio Téllez Valdés, el cual señala

[154] *Idem.*
[155] *Ibidem.*, pág.117.

como concepto típico al siguiente: "*las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico).*[156] Esta puede ser una forma o concepto de tipo penal aunque deja fuera áreas muy amplias.

Respecto al concepto atípico, si tomamos en cuenta que en el diccionario se le define como "el que no se encuentra regulado por la Ley y, por lo tanto, no se ajusta a ninguno de los tipos establecidos[...]",[157] entonces podemos llegar a la conclusión de que atípico es aquel que no se encuentra dentro de una legislación ya regulada, ya tipificada la conducta criminal.

De igual manera, el Maestro Julio Téllez Valdés da su concepto atípico: *los delitos informáticos son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin.*

Se puede llegar a la conclusión de que es urgente y necesaria la realización de los tipos penales que se relacionan y tienen como fin y medio a la computadora, estableciendo así la realización de los delitos informáticos como un ente diferente y con características propias que los hacen formar parte de un capítulo especial.

3.4 Características esenciales

Son diversas las características de los delitos informáticos, las cuales veremos a continuación, para poder entender más aun la trascendencia de éstos y la necesidad clara, urgente y decidida de regular a la piratería de software o

[156] TÉLLEZ VALDÉS, Julio, *Op. Cit.*, pág.104.
[157] DE PINA, Rafael. DE PINA VARA Rafael. *Diccionario de Derecho*, vigésimo tercera edición. Porrúa. México, 1996, pág.188.

programas de computo; pasemos pues a ver estas características:

1.- Son conductas criminógenas de cuello blanco (*white collar crimes*), en tanto que sólo determinado número de personas, con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.[158] En cuanto a esto es necesario señalar, hacer hincapié, en que estas personas tienen conocimientos ciertamente técnicos, pero no todos, pues como ya lo señalé anteriormente, dichas conductas pueden ser realizadas por personas que tienen conocimientos "primarios" de computación, es decir de MS-DOS, de programación o bien de lenguajes de programación; este tipo de conocimientos, al que llamo primario, es el que se conoce en el medio como "lo básico para poder manejar y conocer a una computador". Estos conocimientos los adquieren en los primeros pasos y capítulos de estudio en la materia, ya sea como capturista –en algunos casos–, analista y principalmente cuando se estudia programación en sus diversas áreas, por lo cual no es necesario tener conocimientos amplios, concisos, profundos sobre la materia pues con lo anterior que acabo de señalar basta y sobra para poder accesar y tener un control de la máquina u ordenador. Otro grupo son aquellas personas que aprenden empíricamente, las cuales recibieron un "curso" para aprender por medio de rutinas, es decir, los pasos que se deben de realizar para llevar a cabo ciertas actividades por medio de las computadoras; estas actividades frecuentemente se aprenden fácilmente si el programa se encuentra en el idioma español, pues sólo tendrán que aprender bajo la práctica y apuntar en algunos casos.

---

[158] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pág.104.

2.- Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.[159] En un principio sí eran sólo ocupacionales, pero podemos ver que actualmente ya no es así, pues son tan grandes las ganancias que dejan estas conductas que los sujetos activos ya se dedican a este tipo de actos de lleno, como un trabajo con horario y sueldo. Así pues, podemos decir que independientemente de que sean acciones ocupacionales también son acciones de planta o de un fin cierto.

3.- Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.[160] Ciertamente son de oportunidad, pues los sujetos buscan los medios tecnológicos para realizar sus funciones –las armas o hardware mediante el cual se hará la piratería– y son económicos porque como ya se dijo anteriormente, estas actividades dejan muchos dividendos por lo cual no es imposible primeramente encontrar quien lo haga, en segunda quien lo compre pues es más barato que lo que se vende legalmente violando la legislación, particularmente la de derechos de autor.

4.- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.[161] Esto es una ratificación de lo anteriormente dicho y una característica singular pues estos beneficios son principalmente para los jefes o "patrones" dado que el pago a quienes lo hacen si bien no es malo tampoco es bueno, pues de acuerdo a las ganancias que genera esta conducta, el pago es "injusto".

---

[159] *Idem.*
[160] *Idem.*
[161] *Idem.*

5.- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.[162] Las facilidades de tiempo y espacio se traducen en que una persona puede realizar estos actos en un "tiempo corto, mínimo" –dependiendo del hardware y software que ocupe– y en un espacio físico que puede ser lo más sencillo e invisible para las autoridades, pues basta un pequeño cuarto para poder realizar dichas acciones. Por lo que respecta a la presencia física, ciertamente no es indispensable en la actualidad, pues es tanto el avance de las computadoras que con una sola vez que esté presente esta persona y deje las ordenes a la computadora, esta realizará a la perfección la tarea y sin errores, teniendo así la plena confianza de que no habrá retrasos ni perdidas en cuanto a la producción de materiales apócrifos.

6.- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.[163] En la actualidad siguen siendo muchos los casos y siguen aumentando, pero en cuanto a las denuncias sí es muy cierto que las autoridades fracasan en la investigación y castigo de estas conductas; es importante mencionar que las empresas han optado por realizar ellas mismas sus investigaciones, o también actúan como coadyuvantes del Ministerio Público y una vez que tienen las pruebas suficientes le dan conocimiento a éste de donde se realizan estas conductas y/o se ocupan dichos programas ilegales; una empresa que realiza esto y quizás la más conocida es Microsoft.

7.- Son muy sofisticados y relativamente frecuentes en el ámbito militar.[164] Verdaderamente deben de ser y

[162] *Idem.*
[163] *Idem.*
[164] *Idem.*

son sofisticados, pues para poder acceder a las computadoras o servidores militares pues se deben de crear programas especiales por técnicos o profesionales de la informática o ingenieros para que no sean descubiertos y sancionados; la frecuencia en este ámbito es quizá, como lo mencioné anteriormente, por querer dar a conocer y enseñar al gobierno que se puede primeramente acceder a su información y sacarla o simplemente destruirla; en segundo término el demostrarle que se le puede atacar sin ser visto –el enemigo– causándole grandes daños, inclusive molestias con otros países.

8.- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.[165] Estas dificultades no dejan de ser importantes, pues al momento de querer comprobar las conductas criminólogicas sólo tiene la autoridad y en algunos casos el medio por el cual se realizaban dichas conductas, pero no tiene pruebas de que el presunto delincuente haya sido el autor material o intelectual de ésta.

9.- En su mayoría son imprudenciales y no necesariamente se cometen con intención.[166] En cuanto a este punto no estoy de acuerdo, porque si bien es cierto que la persona que realiza esta conducta no sabe en algunos casos que está cometiendo una conducta ilícita, también es cierto –y lo comprobaré en el transcurso de este estudio– que la mayoría de los delincuentes informáticos saben y conocen la trascendencia de sus actos, pues los programas y el equipo que utilizan sólo se pueden utilizar para un fin, es decir, se crea para determinado y específico trabajo.

10.- Ofrecen facilidades para su comisión a los menores de edad.[167] Estas facilidades no son otra cosa que,

[165] *Loc. Cit.*
[166] *Ibidem*, pág.105.
[167] *Idem.*

a partir de los conocimientos ya sean científicos o empíricos que adquiere el menor por lo regular en su escuela, éste se pone primeramente a experimentar dichos conocimientos y posteriormente, conociendo sus límites y sabiduría, se presta a realizar actos que él sabe que son ilícitos pero que por ser menor de edad no será castigado. Es hasta cierto punto mentira que por ser menor no se entienda y sepa que lo que se realiza es ilícito, y por tanto deja de ser imputable dicha conducta del menor.

11.- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.[168] *La proliferación de que se habla es ya imparable pues la tecnología avanza a pasos agigantados, sólo queda que el derecho avance a la par de éste y de las posibles conductas ilícitas que se pudieran dar regulándolas y tipificando la conducta de los verdaderos responsables del inicio y creación de estos, es decir de los padres del software o hardware que se ocupa para la comisión de ellos.*

12.- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.[169] La impunidad de estos ilícitos es principalmente en cuanto a que los medios por los cuales se cometen son, como ya se dijo, rápidos y se realizan en lugares donde haya lo imprescindible para la utilización de éstos, es decir, luz, equipo de cómputo –uno o dos– con las características que se señalaron al principio y lo principal, mano de obra con la capacidad de poder manejar en lo más básico a este equipo.

3.5 Clasificación

Si bien autores como Sarzana mencionan que estos ilícitos pueden clasificarse en atención a que producen un prove-

[168] *Idem.*
[169] *Loc. Cit.*

cho para el autor y provocan un daño contra la computadora como entidad física, y que procuren un daño a un individuo o grupos, en su integridad física, honor o patrimonio, nosotros preferimos clasificarlos en atención a dos criterios: como instrumentos o medio (este ha sido adoptado comúnmente por la doctrina) y como fin u objetivo de la conducta ilícita. [170]

Dentro de la categoría como instrumento o medio tenemos a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computadora (tarjetas de crédito, cheques, etcétera).
b) Variación de los activos y pasivos en la situación contable de las empresas.
c) Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).
d) "Robo" de tiempo de computadora.
e) Lectura, sustracción o copiado de información confidencial.
f) Modificación de datos tanto en la entrada como en la salida.
g) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto es lo que se conoce en el medio como el método del "Caballo de Troya").
h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la "técnica de Salami".

[170] *cfr.* TÉLLEZ VALDÉS, Julio. *Op. Cit.* pág. 105

i) Uso no autorizado de programas de cómputo.
j) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios, tales como consulta a su distribución.
k) Alteración en el funcionamiento de los sistemas, a través de los cada vez más temibles virus informáticos.
l) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.
m) Acceso a áreas informatizadas en forma no autorizada.
n) Intervención en las líneas de comunicación de datos o teleproceso.[171]

En la categoría como fin u objeto se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunas de estas conductas son las siguientes:

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 (discos, cintas, terminales, etcétera).
e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

[171] *Ibidem.*, pp.105-106.

f) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje (pago de rescate, etcétera).[172]

Otro criterio de clasificación atiende a la fase de procesamiento y transmisión de datos en que se produce la conducta.

a) Fase de entrada de datos (Input): manipulación y transmisión de datos.
b) Fase de programación o procesamiento de datos (data processing): sustracción de programas, modificación de programas, instrucciones secretas de daños, etc.
c) Fase de salida de datos (Output): "robo" de información confidencial, lectura no autorizada, etc.
d) Comunicación de datos electrónicamente: alteración de información, apropiación de servicios, intercepción, sabotaje, etc.

Esta clasificación refleja las formas posibles de actuar sobre el ordenador con un criterio temporal, pero no vislumbra el verdadero sentido de la conducta que puede realizarse con finalidades muy diversas y tal vez vulnerando distintos bienes jurídicos, lo que lógicamente modificaría su tratamiento jurídico-penal [...].[173]

---

[172] *Idem.*

[173] CONTRERAS SALDIVAR, Gabriel. *El Derecho Penal ante el Crimen Informático.* Escuela Libre de Derecho. México, 1999, pág.17.

Sieber clasifica a este tipo de conductas atendiendo a los bienes jurídicos que se vulneran con su comisión:

a) De carácter económico o patrimonial:

- Fraude mediante manipulaciones contra los sistemas de procesamientos de datos.
- Espionaje informático y robo de software.
- Sabotaje informático.
- Apropiación de servicios.
- Acceso no autorizado a los sistemas informáticos.

b) Ofensas a los derechos individuales de la persona:

- Atentados contra la Seguridad Nacional.

c) Ataques a intereses supraindividuales.

- Atentados contra la Seguridad Nacional.
- Atentados contra la integridad de los procedimientos basados en la Informática y en los procesamientos de datos.
- Atentados contra la legitimación democrática de las decisiones parlamentarias vinculadas a los ordenadores.[174]

Este tipo de clasificación parece más acertado pues atiende a los bienes jurídicos que se vulneran, dando con ello más luz respecto de la naturaleza de cada uno de los "delitos". Sin embargo, descarta *a priori* la existencia

[174] *Idem.*

de un genero nuevo de delitos que proteja a bienes jurídicos distintos de los tradicionales, desconociendo que el fenómeno de la delincuencia informática ha estado condicionado por la aparición de nuevos valores económicos, como lo es el manejo de la información.

Como podemos ver esta clasificación es bastante amplia y sigue en aumento al propio paso de la tecnología, es por eso que es de suma importancia que se regulen en un apartado especial estos delitos, donde podamos encontrar aquellas conductas que son básicas para poder definir y establecer cuándo y cómo se dan estos delitos, ya que desde mi punto de vista sí hay las suficientes pruebas para realizar esta tipificación y en consecuencia, una reforma al código penal federal. Respecto a la anterior clasificación veremos en el capítulo cuarto más ampliamente las características de estas conductas, principalmente las que tienen singular importancia para nuestro estudio. A continuación analizaremos las conductas mas conocidas o mejor dicho a los sujetos activos y cómo es que ejecutan sus actos delictivos.

3.5.1 Sujetos Activos

En este apartado veremos los diversos sujetos que realizan las conductas delictivas anteriormente descritas; esto con el fin de poder diferenciarlos así como tener una visión de las características técnicas de cada uno y de su *modus operandi,* así como las posibles causas por las cuales se realiza el acto ilícito; así pues pasemos de lleno al estudio de las conductas de los sujetos en comento.

Hacker: La palabra deriva de hack, que significa hacha, y es el término que se usaba para describir la familiar forma en que los técnicos telefónicos arreglaban cajas defectuosas, el bueno y el viejo golpe seco, y a la persona

encargada de ejecutar esos golpes se le llamaba naturalmente un hacker; este tipo de persona no es considerado propiamente un delincuente, se asemeja mas bien a un bromista que disfruta entrando en sistemas informáticos privados y que toma esa actividad como un reto a sus conocimientos.[175] Ejemplo de estos se encuentra en el artículo escrito en la Revista Milenio por la reportera Laura G. De Rivera en el que se dice: "La mercantilización de la internet y los abusos del poder están en la mira de los Hacktivistas. [...], la más moderna forma de protestar, que tiene como una de sus primeras fuentes de inspiración la rebelión zapatista en la red. Entre sus víctimas están desde empresas como Yahoo.com, hasta el gobierno de México, la Casa Blanca y el Pentágono".[176]

El móvil: retar al poder utilizando las tecnologías de una forma creativa. Los actos hacktivistas son actuaciones colectivas puntuales que reúnen a personas geográficamente dispersas y se organizan a través de infraestructuras móviles y redes independientes.[177]

En el caso del activismo, el propósito de la protesta social, política y cultural completan la lista, guardando, en lo posible, las formas de lo legal. O anticipándose a ellas, como lo hizo el buscado grupo hacktivista mexicano X-Ploit, el cual, desde 1998, ha invadido varías veces los servidores del gobierno del entonces presidente Ernesto Zedillo [...]. Otra cualidad que define a las comunidades virtuales subversivas es la experimentación. Todas ellas apuestan por romper con lo establecido planteando nue-

[175] Instituto Nacional de Ciencias Penales. *Curso de Introducción a los delitos Informáticos*. México, 4 al 20 julio 2000.
[176] De Rivera ,Laura G. *Guía Básica del Hacktivismo. Los Guerreros de la Red*, en Revista Milenio, número 160, Octubre 2 de 2000, pág.35.
[177] *Idem.*

vas formas de comunicación, diseño y utilización de la internet.[178]

Es importante hacer mención de "El culto de la Vaca muerta" grupo de hackers formado en 1984, uno de los grupos más conocidos del mundo. Una de sus últimas y más populares creaciones es back Orificce 2000 (BO2K), una poderosa herramienta de administración remota diseñada para el sistema operativo Windows. Utilizando internet como "medio de transporte", BO2K puede instalarse silenciosamente en el sistema operativo del destinatario y realizar operaciones a través de la computadora abordada, como enviar y leer correo electrónico, comprar on-line, escribir documentos, copiar y borrar archivos. Y todo sin que el usuario se entere de nada. Desde cualquier parte del mundo, el invasor puede llegar así a cualquier máquina.[179]

La eficacia y gran accesibilidad de BO2K, disponible gratis en la red, la convierten en una arma muy peligrosa a los ojos de muchos. Sin embargo, según señala, "el culto" en su página de internet, "esta herramienta, como cualquier herramienta, puede emplearse de manera legítima o para hacer daño a las personas... Los hackers pueden utilizarla para hackear sistemas. Los administradores de sistemas pueden usarla para hacer su vida mucho más sencilla. Y aconseja: "Administradores, sean responsables. Usuarios finales, no se fíen de cualquiera en la red".[180]

Su autor es uno de los miembros del grupo DilDog, que tomó como punto de partida el programa original Back Orificce escrito por el programador Sir Dystic para Windows 95. BO2K no sólo está abierto a sucesivas

[178] *Idem.*
[179] *Ibidem*, pág.39.
[180] *Idem.*

mejoras y ampliaciones, sino que se invita a los programadores de todo el mundo a compartir sus conocimientos. Entre sus próximos objetivos está ampliar la versión para otros sistemas operativos, además de Windows.[181]

El espíritu subversivo de BO2K no sólo queda claro por ser freeware (cualquiera puede descargar el programa BO2K en su página web: RTMark.www.rtmark.com es la dirección en Internet que descarga información sobre Back Orificce 2000, producido por The Cult Of The Dead Cow-, completo cabe en un disco de 1.44 MB), ajeno a las leyes del mercado y en competencia directa con los programas comerciales. Va más allá con su reto a Microsoft, dejando al descubierto la vulnerabilidad del sistema operativo Windows, instalado en 80 por ciento de las computadoras del mundo.[182]

Así, las "travesuras" de hackers pueden traducirse en pérdidas de millones de dólares para algunos. Recordemos el berrinche que hicieron las autoridades estadounidenses, en febrero de 2000, cuando un grupo de "criminales" internautas colapsó las páginas de Yahho.com, eBay.com y Cnn.com, impidiendo su funcionamiento durante horas.[183]

Para ello se empleó un software programado por el hacker alemán Mister, el Tribal Flood Network, diseñado para ataques DdoS (Distributed Denial of Service). Meses después, a finales de abril, el gobierno canadiense detuvo en Montreal a Mafiaboy, un joven de 15 años acusado de ser el coordinador de estos ataques de "service denial" o denegación de servicio, en los que tomaron parte computadoras de diversas universidades estadounidenses.[184]

---

[181] *Idem.*
[182] *Loc. Cit.*
[183] *Ibidem,* pág.40.
[184] *Idem.*

En este tipo de ataque, los hackers o el grupo de internautas que "ataca" un blanco virtual específico como Yahoo.com, satura con peticiones falsas su servidor, hasta que lo sacan de operación.[185]

Como podemos ver, es verdaderamente grande y diversa la aplicación de los conocimientos de los programadores; este es un pequeño ejemplo de la peligrosidad del programador y como estos hay muchos más, de los cuales podemos deducir y señalar la necesidad de tipificar estas conductas.

Sigamos con los sujetos, pues la conducta antes mencionada se considera como la menos "dañina" y las siguientes como altamente destructivas, por lo cual sólo se darán sus características y una explicación pequeña.

Cracker: La significación deriva de la palabra en ingles crak, que significa romper. Este tipo de personas trae aparejada la firme intención de provocar un daño en los sistemas informativos de un tercero, lo cual constituye un auténtico peligro; su terminación (ER), connota al quebrador o persona que se dedica a dañar los sistemas informáticos, ya porque se le pagó o por motivos nocivos que bien pueden ser personales, (ejemplo un empleado vergonzosamente despedido, un competidor de los negocios o un enemigo personal del sujeto activo).[186]

Lammer: Connota a la persona cuya su especialidad radica en utilizar códigos fuentes de otros programadores para beneficio (una especie de plagio electrónico) propio sin hacer mención del copyright (Derechos de autor).[187]

---

[185] *Idem.*

[186] Instituto Nacional de Ciencias Penales. *Curso de Introducción a los delitos Informáticos.* México, 4 al 20 julio 2000.

[187] *Idem.*

Sniffer: Del ingles Sniff, que significa olfatear. Este tipo de personas navega por la línea internet de sistema en sistema, con la intención de descubrir todo tipo de errores que pudieran vender, o utilizar en su beneficio (robo de información, acceso a sistemas financieros, a secretos de patentes, el banco de información científica, etc., etc.).[188]

Graffitis: Deriva de la palabra gráfico, y su conducta esencial estriba en rayar los sistemas informáticos, al igual que en nuestra actualidad se rayan las paredes. Esos se dedican a decorar la pagina web (se le denomina así al servidor que sirve de conducto para leer información) con sus creaciones pintorescas.[189]

Fiberpan: Vandalismo electrónico. Destruir o dañar datos, soportes y programas, utiliza programas descifradores para poder entrar –por medio de Internet principalmente– a los discos duros de las computadoras u ordenadores y busca información principalmente, con el fin de destruirla.[190]

Otra figura y que debe formar parte de estos sujetos activos, ya que son parte de la propuesta a demostrar es aquella que lleva a cabo, ya sea la persona física o moral –inclusive Gobiernos a nivel Internacional– la realización de software ya sea para entrar en computadoras u ordenadores privados, para robar información, destruirla o sólo saber qué tiene, qué hace. Un ejemplo de estos lo tenemos aquí: "El hermano grande ya nos vigila. [...] los habitantes de este planeta hemos perdido totalmente la intimidad. Hoy el Big Brhoter se llama Echelon y es un programa dirigido por la ultrasecreta NSA (Agencia Nacional de Seguridad) de los Estados Unidos, en connvivencia con los gobiernos

[188] *Idem.*
[189] *Idem.*
[190] *Idem.*

de Australia, Canadá, Gran Bretaña y Nueva Zelanda, que mediante poderosos satélites escucha y lee conversaciones telefónicas, señales de radio, correo electrónico, navegaciones por internet, faxes y todo tipo de señal digital que se emita en cualquier lugar del mundo. Como si esto no bastara, empresas privadas ya comercializan a pedido, fotografías satelitales del lugar o la persona sobre la que se desean conocer detalles. Por último, un software espía que utilizan las empresas monitorea cada una de las acciones que se realicen con la computadora, ya sea que se escriba una carta o se visite algún sitio en la Web. [...]".[191]

En lo concerniente a los software, existen espías (spyware) que llegan y se instalan en nuestras computadoras sin que nos enteremos, ya sea al navegar por Internet, bajar de la Red algún programa gratuito o de prueba o instalar uno, en apariencia, inocente programa educativo infantil. Esta última instancia no se encuentra en las cookies, archivos que también curiosean en nuestras máquinas, pero que únicamente se alojan en ellas cuando navegamos por la Red.[192]

Estos programas intrusos que están ocultos en más de 500 programas comerciales o shareware (pruébelo y pague después) y en otros tantos sites de Internet, ingresan a nuestras máquinas con el total conocimiento de las empresas que los diseñan, quienes alegan que incorporan el spyware a sus software exclusivamente por razones de marketing. Según los especialistas en seguridad informática, hay más de 20 millones de computadoras que tienen, sin saberlo, un spyware en su disco rígido.[193]

---

[191] MONZÓN, Enrique. "El Hermano Grande nos Vigila", en Periódico *Tiempos del Mundo*, año 2 / número 43 / (206), semana del 26 al 2 de Noviembre del 2000, pág.B37.
[192] *Idem.*
[193] *Idem.*

Estos archivos espías tienen la habilidad de enviar y recibir datos por Internet cada vez que navegamos por la Red. Como la información que extraen de nuestra máquina está encriptada por el archivo espía, es imposible saber qué datos de los que sacaron de nuestro disco rígido llegan a manos de personas que desconocemos. Entre ellos pueden estar los sites que visitamos al conectarnos, los e-mails (correos electrónicos) que recibimos y mandamos, y las compras que realizamos on line. Mas allá de los propósitos comerciales que alegan las empresas, la privacidad de nuestros datos y nuestras costumbres debe considerarse sagrada y debe ser preservada. [...].[194]

Después de haber analizado lo antes expuesto, podemos deducir y señalar claramente que sí hay y tienen una gran responsabilidad primeramente los dueños de empresas creadoras de software y hardware conjuntamente con sus programadores, así como aquellos programadores que son independientes, pues tiene en sus manos, por así decirlo, el destino de los que utilizamos en nuestra vida diaria una computadora sin llegar a preocuparnos por estos "pequeños detalles" que son fatales y en algunos casos hasta se nos puede culpar de falta de cuidado, precaución, e inclusive de participar como cómplice en estos delitos, aun sin saber cómo fue que pasó; es por eso que desde mi punto de vista se les debe responsabilizar y tipificar penalmente su conducta.

3.6 Formas de control preventivo y correctivo

Como podemos inferir, este tipo de ilícitos requieren de un necesario control, y éste, al no encontrar en la actualidad

[194] *Loc. Cit.*

un adecuado entorno jurídico, ha tenido que manifestarse, en su función preventiva, a través de diversas formas de carácter administrativo, normativo y técnico, de entre las que se cuentan las siguientes:

- Elaboración de un examen psicométrico previo al ingreso al área de sistemas en las empresas.
- Introducción de cláusulas especiales, en los contratos de trabajo con el personal informático que por el tipo de labores a realizar así lo requiera.
- Establecimiento de un código ético de carácter interno en las empresas.
- Adoptar estrictas medidas en el acceso y control de las áreas informáticas de trabajo.
- Capacitación adecuada del personal informático, a efecto de evitar actitudes negligentes u omisivas por falta de los conocimientos necesarios e imprescindibles.
- Rotación en el uso de claves de acceso al sistema (password).[195]

Estas formas son quizás las más utilizadas y se consideran las idóneas, pero esto no basta pues cuando el sujeto activo desea realizar el acto ilícito éste se allega de los medios técnicos necesarios e información de la seguridad del lugar a ser atacado con el fin de tener, como se dijo anteriormente, los medios y en este caso el software idóneo para librar todos los obstáculos que se le presenten. Estos son por lo regular, passwords (claves de acceso), identificadores personales y en el último de los casos, los

[195] TÉLLEZ VALDÉS, Julio, *Op. Cit.*, pág.106.

códigos para abrir un programa o software; estos son mejor conocidos como código fuente y código objeto, los cuales se verán más a fondo posteriormente.

Por otra parte, en cuanto concierne al control correctivo, éste podrá darse en la medida en que se introduzcan un conjunto de disposiciones jurídicas específicas en los códigos penales sustantivos, ya que en caso de considerar este tipo de ilícitos como figuras análogas ya existentes, se corre el riesgo de alterar de manera flagrante el principio de legalidad de las penas.[196]

Cabe hacer mención que una adecuada legislación al respecto traería consigo efectos no sólo correctivos sino eventualmente preventivos, de tal forma que se reducirían en buen número este tipo de acciones que tanto daño causaran a los intereses individuales y sociales y actualmente también a los intereses gubernamentales a nivel mundial.[197]

Por cuanto toca a nuestro país, este tipo de ilícitos no están actualmente contemplados ni por asomo en nuestros códigos penales respectivos. Si bien es cierto que el nivel de informatización nacional no es tan pronunciado como en otros países, al menos es suficiente como para un adecuado análisis y tratamiento por la vía del Derecho.[198]

"[...] la utilización de tipos penales generales por vía de extensión a este tipo de acciones puede provocar enormes errores de apreciación y, por ende de punitividad. Así entonces, situaciones tales como el robo de tiempo de sistemas no podrían ser encuadradas bajo las consideraciones de un robo convencional, esto en función de las complejidades que reviste el factor tiempo o aún otras cuestiones como sería la misma información".[199]

---

[196] *Ibidem*, pág.107.
[197] *Idem.*
[198] *Idem.*
[199] *Loc. Cit.*

Habría que considerar, asimismo, que nuestro actual Código Penal sustantivo, que data de 1931, no se ajusta de ninguna manera a este tipo de manifestaciones tecnológicas, además de que el se atiende a un criterio preponderantemente subjetivo, y tal vez sería conveniente considerar la necesidad de contemplar o dar cabida a criterios más propiamente objetivos; esto en atención a la gran importancia que adquieren cada vez con más fuerza este tipo de instrumentos tecnológicos, como es la computación.[200]

Así pues, podemos darnos cuenta una vez más del grado de necesidad que hay en la actualidad de que se tipifiquen no sólo las conductas ilícitas informáticas, sino también el de crear un apartado especialmente dedicado a ellos. Un ejemplo de esto es España, que a fines de mayo de 2000, realizó reformas en su código penal dando un especial atención a estos delitos, llamándolos delitos Telemáticos.[201]

3.6.1 Formas técnicas (Software)

Por lo que respecta a este tipo de formas (preventiva y correctiva) y a los dos sucesivos temas, daré las que desde mi punto de vista son las necesarias, las idóneas para erradicar al máximo la piratería de software. Después de esta pequeña aclaración, pasemos a explicar y analizar dichas formas. Preventivamente y desde el inicio de una empresa o área gubernativa se deben de tomar en cuenta y a la vez realizar los pasos que se señalaron en el capítulo anterior. Estos son la base para poder tener un control ético, profe-

[200] *Loc. Cit.*

[201] *Cfr.* Instituto Nacional de Ciencias Penales. *Curso de Introducción a los delitos Informáticos.* México, 4 al 20 julio 2000.

sional y veraz sobre los usuarios de las computadoras, siguiendo así con formas quizás más técnicas pero que no dejan de pertenecer a este rubro.

Otra forma de prevenir puede ser el tener presente por categoría a los usuarios, es decir, hacer una división de éstos por medio de sus conocimientos técnicos y antigüedad; técnicos por que al personal mejor capacitado se le puede influir para que omita actuar de forma ilícita, ya sea por medio de principios éticos, profesionales e incluso sociales –esto no quiere decir que aquellos que no tengan conocimientos no se les deba o pueda persuadir, o no conozcan y sepan cómo realizar estos actos ilícitos, pero es y debe ser diferente la forma de prevenir y persuadir para cada uno– y antigüedad, porque si bien estos sujetos no tienen conocimientos técnicos, por su propio tiempo de trabajo conocen las formas de realizar dichos actos, los cuales pueden aprender empíricamente en un principio y posteriormente manejan con cierta técnica –que desde mi punto de vista no es técnica sino un conocimiento mecánico que por el tiempo de trabajo conocen y aplican para realizar dichas conductas–.Como vuelvo a repetir, por su antigüedad saben y conocen el manejo del equipo y los programas, pues por las características propias del software para realizar ciertos procesos se necesitan hacer pasos y/o movimientos que siempre serán iguales para dichos procesos, y por lo cual un individuo que no tiene conocimientos técnicos puede aprender a realizarlos con un poco de experiencia –empírica– y práctica continua sobre el software, no importando el idioma en que se encuentre.

Esta categorización es con el fin de tener presente quien o quienes pudieran realizar en un momento dado procesos que significan actos ilícitos; así son variadas las formas preventivas que se pueden llevar a cabo, pero sólo la empresa o gobierno puede elegir las que mejor le con-

vengan de acuerdo a sus intereses y los medios que tenga para llevarlo a cabo.

Por otro lado, tenemos a los particulares mejor conocidos como piratas, los cuales han sido hasta el momento la pesadilla de empresas nacionales e internacionales. Estos sujetos por sus características especiales, *modus operandi y modus vivendi,* son difícil primeramente de ubicar y posteriormente de aplicarles una sanción si no se encuadran correctamente los elementos de la conducta ilícita, la cual actualmente está tipificada y sancionada dentro de los derechos de autor. Esta equiparación, a mi parecer es válida pero incorrecta para este tipo de conductas, pues regularmente las empresas piden la reparación de daños y al hacerlo el delincuente, la empresa se desiste de toda acción en su contra, pues ésta lo que quiere como fin es rescatar un pago y no el encarcelamiento del sujeto pues esto le trae como consecuencia gastos que no son recuperables y por lo contrario, al obtener una indemnización, recupera parte de lo perdido. Así el pirata sale libre y sigue delinquiendo, por lo que en mi opinión se debe de tipificar esta y la propuesta que hago, en el Código Penal Federal como delito grave y sin derecho a fianza. Por lo anteriormente dicho creo que preventivamente no hay mucho por hacer sino que debe de ser totalmente correctivo el procedimiento para obtener un buen resultado.

Dentro de la forma correctiva que propongo, podemos crear un conjunto legislativo dentro del Código Penal Federal, en el cual se tipifiquen primeramente las conductas de los fabricantes o creadores de software, los cuales están debidamente registrados como tales ante la autoridad correspondiente, para el caso de que si éstos no toman las medidas necesarias para la protección de su software creado o inventado u omita protegerlo, se le sancione, esto con el fin de obligar a la persona física o moral a realizar

dicha protección sin alegar posteriormente algún error o eximiente de culpabilidad por no haberla concretado.

Es así como una forma de controlar técnicamente el software y siguiendo los pasos de un programador, primeramente se debe de tener un control total de los códigos fuente y objeto, es decir, el programador como "padre" de un programa debe saber –y de hecho lo sabe– dónde están los lugares por donde se puede atacar, dañar e inclusive modificar a su programa, por lo cual si no tiene un control sobre estos códigos es un cien por ciento negligente, y en consecuencia culpable. Por otro lado si un programador tuvo la capacidad para crear un programa, tiene la capacidad de protegerlo, es decir puede dejar un programa adjunto que al momento de que se trate de realizar algún acto ilícito sobre éste, se active e inclusive se destruya el propio programa original, realizando al mismo tiempo un daño irreversible en el equipo donde se trató de realizar el acto ilícito.

Ahora bien analicemos lo anteriormente expuesto más detenidamente: primeramente, no se trata de limitar el desarrollo de la tecnología ni limitar a los empresarios en su desarrollo y el de la propia tecnológica e industria, ni mucho menos la inventiva e ideas nuevas, en este caso de los inventores o creadores de nuevos equipos o programas, sino el de tener el medio legal y eficaz para detener y en su caso extinguir la piratería de los programas mejor conocidos como software. Se preguntarán por que tipificar esta conducta; pues bien, estos sujetos ya sean personas físicas o morales tienen los conocimientos técnicos para poder proteger sus producciones, inventos y/o creaciones, pero el caso es que no lo hacen, siendo diversas las causas: en el caso de grandes corporaciones como Microsoft, no los protegen para después realizar campañas de regularización mediante las cuales identifican a quienes tienen sus productos sin licencia y posteriormente les cobran cierta

cantidad por esta regulación, recabando así sumas considerables de dinero que en un momento dado lo habrían perdido y de hecho lo está. ¿Pero cómo se pueden piratear sus programas? fácilmente, sólo basta esperar y actuar en el momento y lugar idóneo. Otro caso puede ser qué sus programas o software tienen ocultos "virus" conocidos como programas destructores, los cuales tienen órdenes predefinidas, como destruir información, bases dc datos y en casos extremos el daño físico de la computadora; estos programas ocultos son con el fin de que posteriormente el usuario final, al encontrar estos "virus" o programas destructores no sabe que hacer y solicita la ayuda de "personal experto", que tiene la "vacuna", la cual curiosamente fue creada-inventada por la misma compañía que creó primeramente el software y dentro de éste el virus, y el único que tuvo que pagar o ver mermado su patrimonio es el usuario final. Un ejemplo palpable es el reportaje realizado por Enrique Monzón llamado "¡Socorro, hay un espía en mi PC!, además de los Virus debemos proteger a nuestra PC de otros intrusos".[202]

Un último caso que quizás es el más importante, es que estos sujetos señalan que la autoridad está obligada jurídicamente a proteger sus derechos de propiedad sobre sus programas, pues ellos cumplen con sus obligaciones fiscales, administrativas y llevan a cabo el registro de sus productos ante el IMPI (Instituto Mexicano de la Propiedad Intelectual). Ciertamente, la autoridad tiene la obligación jurídica de proteger al máximo sus derechos sobre todas las cosas y conjuntamente sancionar al que infringa estos; pero vuelvo a repetir la pregunta central, medular de este estudio ¿dónde queda su responsabilidad como creadores tanto de software y hardware que sirven para dar vida a las conduc-

[202] Ver *Supra.*, pág.58.

tas ilícitas mencionadas anteriormente? ¿acaso ellos no tienen también obligaciones?, y si no las tienen el Estado está obligado a aplicárselas, dentro de estas obligaciones es de donde tomo el pilar para tipificar estas conductas, pues al realizar dicha tipificación, lograremos primeramente que las empresas –ya sea persona física o moral– protejan sus programas y en consecuencia, se reduzca la piratería, lo cual aumentaría el nivel de venta de estos los productos originales.

Una forma de protección que existía en un principio –y que a mi parecer sigue siendo la más apropiada, y que ocupaban tiempo atrás los programadores o técnicos mexicanos en su mayoría y en el extranjero– se llegó a opinar que los programas mexicanos eran los más seguros, pues al momento que se les quería violentar alguna clave de seguridad de éstos (programa objeto y/o programa fuente), éste se destruía automáticamente, no siendo el caso en los demás programas, especialmente los norteamericanos, pues estos primeramente no estaban protegidos y los que lo estaban tenían y tienen una protección muy débil que cualquier persona con conocimientos básicos de programación podía invalidar, independientemente de que estos preferían que se pirateara su programa a que se destruyera la información, y aún es así, con algunas modificaciones pues ahora ocupan códigos que se obtienen mediante una llamada al centro de servicio y sólo sirven una vez. Esto lo podemos constatar en el reportaje hecho por Jorge Taboada del periódico Reforma, en el cual nos explica lo siguiente: "En Estados Unidos, Microsoft tiene implementado un programa piloto para evitar la piratería. El consumidor adquiere un producto y para instalarlo deberá solicitar un número de acceso por teléfono que funcionará sólo en una ocasión".[203] Como lo señala, es un

[203] http://www.reforma.com/negocios_y_dinero/artículo/009049/.

programa piloto pero, ¿por que no se ha puesto en marcha en los países donde tienen mayor piratería de software? quizás por que les conviene que permanezca esta situación.

Así pues, esta puede ser una forma de protección que practiquen las personas físicas o morales, y hasta con mejoras, pues pueden inclusive hacer que al momento de que se quiera violentar el programa fuente u objeto, o hacer una copia ilegal de estos, se destruya el original; seguidamente, dañe el material donde se iba a realizar y por último dañe o cause daños severos al equipo donde se pensaba realizar la conducta ilícita, y si se diera el caso de que se lograra hacer una copia ilegal, incluir programas ocultos que destruyan "todo" lo que encuentre a su paso en la instalación del mismo. Una vez hecho esto, la autoridad más fácilmente puede identificar y sancionar a los que realizan este tipo de conductas porque primeramente, no cualquier persona puede o tiene los conocimientos técnicos científicos para invalidar códigos de seguridad y los que lo tienen no arriesgarían su libertad por unos cuantos pesos, pues su nivel de estudio-conocimiento generalmente les da varias oportunidades de obtener un buen empleo y sin realizar conductas criminógenas. Por ende, la autoridad atraparía e identificaría en corto tiempo el quién, cómo y dónde se realizaran estos actos ilegales, disminuyendo así el delito de piratería en su modalidad de copia ilegal de software.

Lo anterior no implica relevar de su responsabilidad al Estado, pero tampoco implica que éste deba realizar todo el trabajo y menos por las características de la conducta ilícita, pues se necesita de la participación total y sin condiciones de los empresarios, técnicos y profesionistas para poder erradicar este mal informático, pues si seguimos actuando de la misma forma sólo se logrará que los

sujetos activos se trasladen a otros lugares a seguir con su "trabajo", sin poder tener un fin cierto y preciso relativo a la extinción de estas conductas.

3.6.2 Formas sociales

Por lo que respecta a este tipo y partiendo de la palabra sociales, hemos de ubicar a ésta dentro de las acciones que se realizan conjuntamente con la sociedad, como un ente con principios éticos, profesionales y morales. Así pues, la sociedad es un punto importante dentro del aumento de esta conducta –especialmente de aquella parte de esta que ocupa diariamente una computadora–, pues es más barato comprar un programa pirata que uno original con su respectiva licencia, garantía y servicios al cliente, pues el precio se duplicaría o triplicaría ya que estos programas son muy caros. Por lo que respecta al costo, los empresarios una vez que protegieran a sus programas y la autoridad actuara como anteriormente lo señalé, podrían disminuir esta conducta pues tendrían más ventas –podrían bajar sus precios– pues al saber el usuario final que los programas están protegidos y si utilizan una copia ilegal, su equipo se puede dañar e inclusive perder, éste optaría por comprar un original con su licencia respectiva y derechos adicionales a ésta, independientemente de las acciones legales a que estaría sujeto como coparticipe de la conducta ilícita. Pero actualmente no es así, una copia ilegal es tan económica que con el pago del costo de un programa original se pueden comprar hasta ocho programas sin licencia; utilizando la lógica, se pueden deducir las ganancias de los piratas, el ahorro del usuario final y las pérdidas que sufre el dueño original de estos programas, por la no protección de los mismos antes de salir al mercado mundial.

Por otro lado, mencioné los principios éticos, profesionales y morales porque toda persona que los tiene ciertamente piensa no dos ni tres veces que está cometiendo una conducta ilícita, pero, el caso es que usualmente prefiere realizar una compra pirata a hacer un gasto excesivo, pues se consigue más económico; con esto quiero decir que no es que se olvide de sus principios sino que ante la actual situación económica no se puede esperar mucho de la respuesta de la sociedad para con la disminución de los delitos, y en este caso de la piratería. Estos se podrían elevar y valorizar más una vez que se realizara lo anteriormente señalado, pues al ver la sociedad que se preocupa el empresario, persona física o moral por proteger sus creaciones y darle una seguridad como usuario final, y que el Estado a la vez otorga una seguridad jurídica en general, la sociedad pondría en la balanza sus principios contra la realización de una conducta ilícita.

Es muy importante señalar también que no se trata en ningún momento de violentar la garantía individual que consagra nuestra Constitución Política en su artículo quinto, en su párrafo primero, el cual señala que "A ninguna persona podrá impedirse que se dedique a la profesión, industria, comercio o trabajo que le acomode, siendo lícitos. El ejercicio de esta libertad sólo podrá vedarse por determinación judicial, cuando se ataquen los derechos de tercero, o por resolución gubernativa, dictada en los términos que marque la ley, cuando se ofendan los derechos de la sociedad. [...]"[204] Pues consideramos que al seguir dejando a estas personas con las "manos libres" en un tiempo corto no sólo les bastará con la protección de sus intereses sino también esperaran tener el control total de los diver-

[204] Constitución Política de los Estados Unidos Mexicanos. Secretaría de Gobernación. Febrero de 2001, pág.14.

sos medios de producción informática en todas sus áreas, a nivel mundial y sin que el Estado los vigile o controle, pues como es sabido la informática sigue actualmente en franco desarrollo y su tendencia es estar de la mano con el desarrollo humano y regular, si no en todas las actividades diarias del ser humano, sí en la mayoría de éstas.

3.6.3 Formas Científicas (Hardware)

Como forma preventiva proponemos que se haga un registro de las personas que saben utilizar y/o manejar estos equipos para poder tenerlos vigilados y en un caso determinado, investigarlos directamente, pues si no fuera así la autoridad tendría que investigar no a unos cuantos si a toda la empresa o en su caso a los posibles técnicos o profesionistas, o también a aquellos que lo aprendieron a utilizar empíricamente, teniendo como consecuencia que a la autoridad le tome tiempo en tener resultados acertados y en algunos casos sea muy tarde para actuar contra estos sujetos, pues se mueven continuamente con sus equipos y con sus centros de "trabajo" a otros lados, ya sea del Distrito Federal e inclusive en el interior del país; pero no siendo tema central de nuestro estudio, pasemos pues a la forma correctiva en el ámbito científico.

Por lo que respecta al rubro correctivo, es especialmente importante señalar que siendo parte intrínsica de mi propuesta al igual que en la forma técnica (software), aquí hemos de tipificar también la conducta de los fabricantes o creadores de (hardware), –esta es la diferencia esencial con la primer forma– que no los protejan o diseñen con seguridad especial, pues estos equipos se ocupan en ciertos actos que se consideran delitos o conductas ilícitas.

De esta forma pasemos a analizar más ampliamente la conducta anteriormente expuesta: en primer tér-

mino y en un inicio, los expertos ciertamente crean un equipo con características especiales y para un fin cierto y concreto; hasta ahí esta bien, pero ¿qué pasa cuando este equipo sale a la venta sin regulación alguna y puede ser adquirido por casi cualquier persona?, vuelvo a repetir, no se trata de limitar el desarrollo científico e industrial ni mucho menos, sólo de garantizar tanto a los empresarios como a los usuarios finales, que se lucha contra la piratería por todos los medios eficaces e idóneos para proteger su trabajo y patrimonio principalmente; es con esta compraventa discriminatoria con la que se inician los actos de piratería, pues aquellos personas que obtienen estos productos iniciarán los actos ilícitos sin que la autoridad tenga un antecedente de quién los compró, para qué empresa en su caso trabaja, con qué fin lo usa y si es experto, profesional o empírico en el uso de este equipo, o lo utilizarán sus trabajadores en el caso de empresarios.

Es por eso que al tipificar la conducta de los que los crean se podrá primeramente garantizar que no cualquier persona pueda manejarlos, sólo aquellas con conocimientos técnicos o profesionales y mediante autorización o permiso y registro de éstos, de su área o empresa donde trabaja, fin que se dará al equipo y, en su caso, permiso del dueño de la propiedad del software o programa para realizar la copia de éste.

Es así como se puede disminuir y me atrevo a decir que extinguir la piratería, pues al tener identificados a quienes tienen los medios idóneos y necesarios para la posible creación de copias ilegales, la autoridad no pensaría dos veces en actuar en una investigación, obteniendo resultados satisfactorios, logrando la disminución de piratería y consecuentemente el costo de programas originales, resultando así que el usuario final compre productos directos de fabrica, primeramente por su bajo costo y en su

caso, por la garantía del producto tanto en el servicio como en las actualizaciones del mismo, que son gratuitas en su mayoría.

En general y a mi parecer, no se deben de utilizar medios preventivos sino sólo correctivos, pues al tipificar la creación de software o hardware, así como la utilización de los mismos en una forma ilegal o con el fin de realizar actos de piratería, se tiene, se da a la autoridad pauta y armas para actuar con todo el peso de la ley para aplicarla de una forma total y flagrante, pues al tratarlo como delito grave, los sujetos activos y aquellos que quieran realizar estas conductas lo pensarán varias veces antes de iniciar o reincidir dichas conductas; esto último lo podemos utilizar como medio quizás preventivo.

La tipificación que se pide y se propone es porque hay ciertos sujetos que se dedican a crear software y hardware con el fin de realizar actos de piratería y actos diversos que también son ilícitos. Es por eso que al tipificarlos se les sancionará no sólo como a aquellos que lo utilizaron sino también como autores intelectuales, tipificándolo como delito grave y en consecuencia sin derecho a libertad bajo caución, pues actualmente sólo se sanciona a quienes los utilizan (hardware o software) como medio o fines del delito pero no la creación de software y de hardware para la culminación de estos delitos satisfactoriamente; ejemplo de esto lo tenemos aquí: "[...] en febrero de 2000, un grupo de "criminales" internautas colapsó las páginas de Yahoo.com, eBay.com y Cnn.com, impidiendo su funcionamiento durante horas. Para ello se empleó un software programado por el hacker alemán Mister, el Tribal Flood Network, diseñado para ataques DdoS (Distributed Denial of Service). Meses después, a finales de abril, el gobierno canadiense detuvo en Montreal a Mafiaboy, un joven de 15 años acusado de ser

el coordinador de estos ataques de "service denial" o "denegación de servicio", en los que tomaron parte computadoras de diversas universidades estadounidenses".[205] Como podemos ver sólo se detuvo a quien lo utilizó pero no a quien lo creó, no se detuvo al autor intelectual del medio del que se sirvió el sujeto activo para realizar el acto ilícito, ejemplo claro de la tipificación que se propone.

3.7 Regulación en el ámbito nacional

En nuestro país, este tipo de conductas no están actualmente contempladas como tales en los códigos penales –salvo el estado de Sinaloa–. Si bien es cierto que el nivel de informatización nacional no es tan pronunciado como en otros países, al menos es suficiente como para un adecuado análisis y tratamiento por la vía del Derecho.

Como mencionábamos antes, la utilización de tipos penales generales por vía de extensión a este tipo de acciones puede provocar enormes errores de apreciación y, por ende, de punibilidad. Así entonces, situaciones tales como el robo de tiempo de sistema no podrían ser encuadradas bajo las consideraciones de un robo convencional, esto en función de las complejidades que reviste el factor tiempo o aún otras cuestiones como sería la misma información.

Habría que considerar, asimismo, que nuestro Código Penal sustantivo, que data de 1931, no se ajusta de ninguna manera a este tipo de manifestaciones tecnológicas, además de que en él se atiende a un criterio preponderantemente subjetivo, y tal vez sería conveniente considerar la necesidad de contemplar o dar cabida a criterios más propiamente objetivos.

[205] En Revista Milenio, *Op. Cit.*, pág.40.

Esto en atención a la gran importancia que adquieren cada vez con más fuerza los instrumentos tecnológicos, tales como la computación.

Con las últimas reformas al Código Penal de fecha 17 de mayo de 1999, así como la denominación del título noveno y sus respectivos capítulos, se regulan sólo las conductas ilícitas dentro del rubro de la informática pero se deja mucho por hacer, pues se concretan estas reformas a tipificar sólo la "Revelación de secretos y acceso ilícito a sistemas y equipos de informática"; dejan las otras conductas fuera de este titulo, es decir las siguen tratando como conductas equiparadas a otros tipos penales.

Por otro lado, los empresarios (ya sean personas físicas o morales) y/o mediante sus representantes legales, han realizado acciones por su lado con el fin de disminuir estas conductas y las pérdidas millonarias a que están sujetos. Un ejemplo de esto son las denuncias que hacen ante la autoridad correspondiente de la utilización de software sin licencia en determinadas empresas, negocios pequeños, así como la creación de páginas en Internet donde se da información sobre acciones contra los piratas y actualizaciones de licencias "por un bajo costo", claro que implica otras exigencias, pues estos grupos han tenido éxito ya que con sus denuncias logran que empresarios sean castigados y obligados a pagar el daño y en algunos casos a actualizar y legalizar sus licencias, pero no pasa lo mismo con la piratería y uso informal de programas pues como ya se mencionó anteriormente, por su forma de operar y vivir es difícil que la misma autoridad los ubique, y si lo hace, cuando actúa es mínimo el resultado obtenido pues los sujetos activos tuvieron el tiempo necesarios para salvaguardar sus intereses materiales y económicos.

Un ejemplo claro de esto es el reportaje hecho por Jorge Taboada del periódico Reforma en donde seña-

la quien ataca la piratería en México, independientemente de las acciones de la autoridad, el cual es el siguiente: ¿Quién ataca la piratería en México? *A través de programas y acciones diversas instituciones combaten la copia ilegal de softwares*. México.–La BSA, integrada por varias empresas desarrolladoras de software (Microsoft, Autodesk, Adobe, Symantec, Corel, Macromedia y Network Associates) es una asociación internacional cuya labor principal es la de informar en qué consiste la piratería, además de que denuncia ante las instancias de cada país cualquier irregularidad en la venta y distribución de sus productos. Así, en México la BSA se apoya en el IMPI (Instituto Mexicano para la Propiedad Intelectual) para el usuario final y en la Procuraduría General de la República en los operativos legales.

Como organización internacional, la BSA también se acerca a los gobiernos de cada país con el objetivo de promover leyes en pro de la defensa de la propiedad intelectual. Las legislaciones que protegen al software en nuestro país son la Ley de Derechos de Autor y Propiedad Intelectual y la Ley de la Propiedad Industrial.

Además de promociones para adquirir el software a precios más bajos (los estudiantes, por ejemplo, pueden obtener precios especiales acreditándose como tales), la BSA encabezó en meses pasados una tregua para legalizar el software empresarial y ahora difunde una campaña de vacunación. Ambas llevan la finalidad de entregar a las empresas todas las facilidades de tiempo y precios, para regularizar el software instalado en sus compañías.

Siguiendo el reportaje, también nos señala que "México no es tan pirata", pues los resultados del estudio practicado por PriceWaterhouseCoopers para la BSA muestran que México está por debajo del promedio en los índices de piratería de Latinoamérica. La lista de los países

más piratas se conforma de la siguiente manera. Los resultados que aparecen representan el porcentaje de software pirata instalado.

Bolivia	87
El Salvador	87
Paraguay	85
Guatemala	85
Ecuador	73
Rep. Dominicana	73
Costa Rica	72
Jamaica	72
Trinidad y Tobago	72
Uruguay	72
Panamá	70
Perú	64
Argentina	62
Venezuela	62
Brasil	61
Colombia	60
México	59
Chile	53
Puerto Rico	49

También nos señala, ¿Qué se puede denunciar? Vendedores de software ilegal, empresas que operen con el mismo, además de que podrá recibir información sobre los productos y programas de la BSA y sus acciones para erradicar la piratería.[206]

Quizás estas acciones sean hasta el momento las que han tenido más respuestas satisfactorias, pero aún así

[206] http://www.reforma.com/negocios_y_dinero/artículo/009049/.

siguen cometiéndose estas conductas y están aumentando conforme se desarrolla la tecnológica informática.

3.7.1 Regulación en el ámbito internacional

La rápida expansión transnacional a gran escala de las redes computacionales y la facilidad de acceso a diversos sistemas a través de líneas de teléfono, ha incrementado la vulnerabilidad de los sistemas y la oportunidad de que se presenten abusos o conductas criminales. Las consecuencias de estas actividades pueden tener serios costos, tanto económicos como en materia de seguridad. Cuando esta cuestión es elevada al plano internacional, los problemas pueden cobrar enormes dimensiones. Es por esta razón que ha existido preocupación por organismos internacionales por entender los problemas que presenta esta nueva forma de crimen transnacional.

En este contexto, la Organización para la Cooperación Económica y el Desarrollo (OCDE), el Consejo de Europa, la Mancomunidad Británica, la Organización de las Naciones Unidas, la INTERPOL, la Asociación Internacional de Derecho Penal y la Cámara de Comercio Internacional han abordado esta problemática.

A. Organización para la Cooperación Económica y el Desarrollo (OCDE)

El primer esfuerzo internacional para tratar los problemas de los delitos informáticos fue iniciado por la OCDE (Organización para la Cooperación Económica y el Desarrollo). En 1983 esta organización encargó a un grupo de expertos el estudio de la posibilidad de una armonización internacional de las leyes penales, para hacer frente a los delitos informáticos (computer crime). Como resultado, en

1985 el grupo de expertos recomendó a los Estados miembros considerar extender sus leyes penales para penalizar a quienes dolosamente cometan actos de abuso en el campo de las computadoras.

En 1986 la OCDE publicó un estudio llamado "Delitos Relacionados con computadoras: Análisis de la Política Legal". Este reporte analiza las leyes existentes y las reformas propuestas en algunos Estados miembros. Tras el análisis, se recomendó a los Estados miembros prohibir y tipificar en sus leyes penales una lista mínima de conductas relacionadas con el abuso a las computadoras. A saber:

1. El ingreso, alteración y/o supresión de datos computarizados y/o programas informáticos con la intención de transferir ilegalmente fondos u otras cosas de valor.

2. El ingreso, alteración y/o supresión de datos computarizados y/o programas informáticos con la intención de falsificar documentos.

3. El ingreso, alteración y/o supresión de datos computarizados y/o programas informáticos, o cualquier otra interferencia con equipos informáticos con la intención de impedir el funcionamiento de equipos informáticos o de telecomunicaciones.

4. La infracción a los derechos exclusivos del propietario de programas informáticos protegidos, con la intención de explotar comercialmente el programa y ponerlo en el mercado.

5. El acceso o intercepción a equipos de cómputo o de telecomunicaciones a sabiendas y sin autorización de la persona responsable del sistema, ya sea por la infracción de medidas de seguridad o por cualquier otra intención deshonesta o dañosa.

La mayoría de los miembros del Comité de Política sobre Información, Computarización y Comunicaciones, también recomendaron que las leyes penales deberían considerar otros tipos de abuso con computadoras, incluyendo el robo de secretos y el acceso o uso no autorizado de computadoras.

En 1990 el Comité de Política sobre Información, Computarización y Comunicaciones encomendó a un grupo de expertos la creación de lineamientos guía para la seguridad en los sistemas de información. Este grupo se conformó por delegados de los gobiernos, académicos en los campos del Derecho, las Matemáticas y la Computación, así como representantes del sector privado, incluyendo a proveedores y usuarios de servicios de computación y comunicaciones.

El 24 de noviembre de 1992 los Estados miembros de la OCDE adoptaron los "Lineamientos Guía para la Seguridad en los Sistemas de Información".

Por lo que hace a las sanciones que deben adoptarse para hacer frente a estas nuevas conductas abusivas, los lineamientos establecen que:

"Las sanciones por abuso sobre sistemas de informática son un medio importante en la protección de los intereses de aquellos que tienen confianza en los mismos, respecto de los daños que puedan resultar de los ataques a la disponibilidad, confidencialidad e integridad de los sistemas de información y de sus componentes. Ejemplos de esos ataques incluyen daños o interrupciones a los sistemas informáticos por la introducción de virus, alteraciones a los datos computarizados, acceso ilegal, fraude o falsificación por computadora y reproducción ilegal de programas informáticos. En el combate a tales peligros, los Estados han escogido responder a estos actos en diversas formas. **Existe un creciente consenso internacional de que es-**

tos abusos a las computadoras deberían ser cubiertos por las leyes penales nacionales.[207]

B. Consejo de Europa

De 1985 a 1989 el Comité de expertos sobre Delitos Relacionados con Computadoras del Consejo de Europa elaboró un estudio sobre el fenómeno de los delitos informáticos, con el objeto de apoyar a los legisladores en la determinación de las conductas que deberían ser contempladas por las leyes penales, y cómo deberían de lograrse estos en relación con el conflicto de intereses entre las libertades civiles y la necesidad de protección.

El Comité elaboró la Recomendación No. R(89)9 que contiene lineamientos para las legislaturas nacionales, misma que fue adoptada por el Consejo de Europa el 13 de septiembre de 1989. Este documento contiene una lista mínima, que rebasa considerablemente a la de la OCDE, y que refleja el consenso general del Comité respecto de las conductas que deberían considerar las leyes penales, así como una lista opcional de conductas que ya han sido penalizadas en algunos países, pero respecto de las cuales no se logró consenso en relación con su penalización, por parte del propio Comité.

Actos que el Consejo de Europa considera que deben ser penalizados:

1.- **Fraude por computadora.** El ingreso, alteración o supresión de datos computarizados o programas informáticos, cualquier otra interferencia durante el procesamiento de datos, que provoque como resultado pérdidas

[207] CONTRERAS SALDIVAR, Gabriel. *Op. Cit.*, pp.24-27.

económicas o de posesiones de otra persona con el propósito de obtener una ganancia económica ilícita para sí o para otra persona.

2.- **Falsificación por computadora.** El ingreso, alteración o supresión de datos computarizados o de programas informáticos, o cualquier otra interferencia durante el procesamiento de datos realizada de tal forma o bajo condiciones tales que constituyan un delito de falsificación, cuando sea sometido respecto de un objeto tradicional de ese delito.

3.- **Daños a datos computarizados o programas informáticos.** El daño, deterioro o supresión de datos computarizados o programas informáticos sin derecho a hacerlo.

4.- **Sabotaje informático.** El ingreso, alteración o supresión de datos computarizados o programas informáticos, o cualquier otra interferencia en los sistemas informáticos con la intención de impedir el funcionamiento del sistema informático o de telecomunicaciones .

5.- **Acceso no autorizado.** Acceso sin autorización a un sistema informático o red, infringiendo medidas de seguridad.

6.- **Intercepción sin autorización.** La intercepción, efectuada sin derecho y por medios técnicos de comunicaciones transmitidas, recibidas o que se encuentren dentro de un sistema informático o red.

7.- ***Reproducción no autorizada de programas informáticos protegidos.*** La reproducción, distribución o comunicación al público, sin derecho, de un programa informático protegido por la ley.

8.- **Reproducción no autorizada de topografías.** La reproducción sin derecho de topografías protegidas por la ley, de un producto semiconductor o la explotación comercial o importación con ese propósito, efectuada sin de-

recho, de una topografía o de un semiconductor fabricado usando la topografía.

La lista opcional contiene las siguientes conductas:

1.- *Alteración sin derecho, de datos computarizados o programas informáticos.*

2.- *Espionaje informático.* La adquisición por medios impropios o la revelación, transferencia o uso de secretos comerciales sin autorización o cualquier otra justificación leal, con la intención de causar pérdidas económicas al titular del secreto o de obtener una ventaja económica ilícita para sí o para una tercera persona.

3.- *Uso no autorizado de una computadora.* El uso sin derecho de un sistema informático o de una red que se realice: (I) con la aceptación de un riesgo significativo de pérdida, causando a la persona facultada al uso del sistema, o de daño al sistema o a su funcionamiento; (II) o con la intención de causar perjuicio a la persona facultada para usar el sistema, o dañar el sistema o funcionamiento; (III) o causar pérdidas a la persona facultada para utilizar el sistema o daño al sistema o a su funcionamiento.

4.- ***Uso no autorizado de programas informáticos*** protegidos por la ley que han sido reproducidos sin derecho a hacerlo, con la intención de obtener una ganancia económica ilícita para sí o para otra persona o para causar un daño al titular del derecho.

C. Organización de las Naciones Unidas

Siguiendo al séptimo Congreso de las Naciones Unidas sobre la Prevención del Crimen y el Tratamiento de los Delincuentes, que tuvo lugar en 1985, la Secretaría Gene-

ral preparó un documento titulado "Propuestas para una Acción Internacional Concertada contra las Formas del Crimen identificadas en Plan de Acción Milán". El crimen informático forma parte de este documento.

Durante la preparación del Octavo Congreso de la Naciones Unidas sobre la Prevención del Crimen y el Tratamiento de los Delincuentes, Asia y algunos países del Pacifico manifestaron su preocupación respecto de los efectos de los avances tecnológicos, como es el caso del crimen informático.

En el Octavo Congreso se adoptó, a propuesta de Canadá, una resolución que llama a los Estados miembros a intensificar sus esfuerzos en el combate al crimen informático, considerando, de ser necesario, la adopción de medidas para: "La modernización de las leyes penales nacionales y los procedimientos", incluyendo medidas para:

- Asegurar que los tipos penales existentes y las leyes relativas a la investigación y admisibilidad de pruebas en los procedimientos judiciales se aplican adecuadamente y, de ser necesario, efectuar los cambios pertinentes.
- Ante la ausencia de leyes que se apliquen adecuadamente, crear tipos penales y procedimientos de investigación para hacer frente a esta novedosa y sofisticada forma de crimen..."

En la citada resolución, el Congreso recomendó al Comité sobre el Control y Prevención del Crimen la promoción de esfuerzos internacionales en el desarrollo y difusión de un extenso marco de guías y estándares, que apoyen a los Estados miembros en la lucha contra el crimen relacionado con computadoras.

Asimismo, recomendaron que este asunto debería ser considerado por un grupo de expertos *ad hoc* y que requirieron a la Secretaría General la consideración de una publicación de carácter técnico sobre la prevención y persecución de los crímenes relacionados con computadoras.

En este contexto, la ONU publicó un documento titulado "Revisión Internacional de Política Criminal-Manual de la Naciones Unidas sobre la Prevención y Control del Crimen Relacionado con Computadoras".

En este documento se analiza la problemática relacionada con el crimen por computadora y se emiten recomendaciones internacionales en aras de la armonización de las leyes en materias como: derecho sustantivo en materia de privacidad y protección de la información, leyes procesales, prevención del delito y cooperación internacional.

El manual de la ONU reconoce como delitos informáticos a las siguientes conductas:

1.- *Fraude por manipulación.* En la actualidad, los negocios están reemplazando las operaciones en efectivo por depósitos en sistemas informáticos, lo que crea un enorme potencial para el mal uso de las computadoras.

El fraude informático mediante el ingreso de datos (Input) es el tipo más común de los delitos informáticos, ya que es fácil cometerlo y difícil su detección. En cambio, la manipulación a los programas informáticos requiere de conocimientos específicos por parte del sujeto activo.

Las técnicas más comunes son las siguientes:

- "Caballo de Troya" a través del cual se colocan instrucciones encubiertas dentro de un programa informático para que ejecute sus

funciones durante el funcionamiento normal del programa.

- Manipulación en la salida de la información, cuyo ejemplo clásico es el "fraude" a los cajeros automáticos mediante la falsificación de instrucciones.
- "Técnica salami" que apoya en la repetición automática de los procesos informáticos, donde se programa a la computadora para que transfiera repetitivamente pequeñas cantidades de dinero de una cuenta a otra.

2.- *Falsificación informática.* Consiste en la alteración de datos de documentos almacenados en la computadora, así como en el uso de la computadora como instrumento para cometer el delito de falsificación.

3.- *Daños o modificaciones a datos computarizados o a programas informáticos.* Esta categoría incluye el acceso de virus o de bombas lógicas. Esta actividad es frecuentemente conocida como sabotaje informático y puede ser el medio para lograr ventajas económicas sobre los competidores.

4.- *Acceso no autorizado a sistemas informáticos y servicios.* El injustificado y doloso acceso por una persona no autorizada por los propietarios u operadores del sistema, puede generalmente constituir una conducta criminal. El acceso no autorizado da la oportunidad de causar daños adicionales o impedir su uso a los legítimos propietarios.

Los modernos sistemas de telecomunicaciones son igualmente vulnerables a esta nueva forma de crimen y al igual que las computadoras, son susceptibles de conductas abusivas por acceso remoto.

5.- *Reproducción no autorizada de programas protegidos legalmente.*

Como puede apreciarse, existe consenso en considerar a estas conductas como delictivas por parte de la UNO, OCDE y el Consejo de Europa; pero nunca se menciona a los autores, diseñadores, creadores de estos programas como posibles coparticipes de estas conductas o en su mejor acepción facilitadores de los medios tanto de hardware y software para la realización de actos ilícitos, sin un medio legal que hasta el momento les regule esta forma de actuar tan libre en cuanto a la creación de software y hardware para "satisfacer sus necesidades tecnológicas".

D. Asociación Internacional de Derecho Penal

Con el objeto de tratar esta nueva forma de crimen, la Asociación Internacional de Derecho Penal se reunió en Würzburg, en octubre de 1992. Como resultado de esta reunión, se elaboró un proyecto de recomendaciones en el área; entre las más importantes para el objeto de nuestro estudio se encuentran las siguientes:

"5. Con el objeto de evitar la excesiva criminalización debe considerase el alcance de la ampliación de los tipos penales en esta área... esta ampliación requiere de un cuidadoso examen y justificación. Un criterio importante en la definición de estos tipos penales es que deben limitarse primordialmente a actos intencionales."

"7. [...] se recomienda a los Estados que, de acuerdo con sus tradición legal y sus leyes aplicables, tipifiquen como delitos las conductas descritas en la lista opcional (del Consejo de Europa), especialmente la alteración de datos computarizados y el espionaje informático."

En septiembre de 1994 se celebró el XV Congreso Internacional de Derecho Penal en Río de Janeiro,

Brasil, el cual dedicó una parte del mismo al tema de los "Delitos Informáticos y Otros Cometidos contra la Tecnología Informática."

Para Juan José Ríos Estavillo, este XV Congreso fue de suma importancia, ya que recogió los avances que hasta ese momento se habían logrado por parte de la OCDE (Organización para la Cooperación Económica y el Desarrollo), el Consejo Europeo, la Comunidad Europea, la Mancomunidad Británica, las Naciones Unidas, INTERPOL y la Cámara de Comercio Internacional. Y señala que en medidas de prevención no penales, el aspecto primordial gira en recordar que el derecho penal debe ser una última medida cuando han fallado o fueron insuficientes las sanciones civiles o administrativas. Se deben implantar, en primer lugar, medidas de seguridad por parte de los usuarios; dictar medidas disciplinarias en la industria del proceso de datos –y no sólo de datos sino también en la creación de software y hardware– dentro de una práctica de patrones profesionales; elaborar políticas de usos informáticos por parte de los gobiernos; promocionar la cooperación entre las víctimas, el entrenamiento y educación del personal en los sistemas de investigación, prosecución y judiciales.[208]

En cuanto al derecho penal sustantivo, se mencionó que, agotadas las posibilidades no penales, sería necesario considerar la adopción de nuevas leyes penales o reforma de las existentes, toda vez que hay o puede haber un bien jurídico afectado que debería tutelarse a través del derecho.[209]

---

[208] RÍOS ESTAVILLO, Juan José. *Op. Cit.*, pág.119.

[209] Al igual que Juan J. Ríos Estavillo, nosotros afirmamos que algunas conductas informáticas pueden adecuarse a los tipos existentes en la legislación, pero es posible que el *modus operandi* escape a las formas tradicionales o que se requieran nuevos tipos para proteger intereses no tutelados hasta ahora.

Dentro del proyecto de recomendaciones emitido por la Asociación, se encuentran los siguientes puntos relevantes:

"3. El abuso de la tecnología informática afecta los intereses de carácter económico relacionados a la informática, cuanto a los orientados hacia la intimidad, abarcando situaciones en que el proceso y sus componentes sólo se utilizan como herramientas para infringir los valores tradicionales, así como cuando son objeto de una conducta delictiva".

"4. [...] el desarrollo de la tecnología informática exterioriza la emergencia de nuevos tipos de intereses que requieren protección legal, especialmente la integridad de los sistemas informáticos y datos incidentes, así como la disponibilidad exclusiva de ciertos datos (seguridad de datos y protección de datos)".

"5. En la medida en que el Derecho Penal es insuficiente, y en el caso que otras medidas también lo sean, debe respaldarse la modificación de la legislación existente o la definición de nuevos delitos..."

"12. Debe reconocerse que, en la constantemente mutante era de la informática, es importante proteger los intereses de la intimidad contra los nuevos cambios que provoca la tecnología informática."

Se debe considerar a este Congreso como de gran importancia, pues por primera vez se trata el problema del crimen informático con criterios jurídicos basados en el bien jurídico que se vulnera con este tipo de conductas. Según el proyecto, los bienes vulnerables son tanto los económicos como la intimidad, así como "nuevos tipos de intereses" como la integridad y disponibilidad exclusiva de ciertos datos –así como la disponibilidad de tiempo, es decir, el robo de tiempo real dentro de un área de trabajo o en su domicilio particular, al detener o "bombardear" con basu-

ra informática su sitio o cuenta en internet–. Esto es por una parte, pero por otra volvemos al cuestionamiento principal ¿dónde queda la responsabilidad de los programadores o creadores de software o hardware, por la creación de estos medios que facilitan las conductas delictivas?.

Por otro lado en lo que respecta a la regulación de estas conductas internacionalmente, tenemos que se han llevado a cabo varias acciones ya sea por parte de un solo país al legislar para el mismo así como se han realizado tratados internacionales y convenios para luchar contra estos actos ilícitos conjuntamente todos los países, aunque a este nivel no están reconocidos como delitos informáticos, pues cada Estado le da el nombre o tipifica de acuerdo a su experiencia.[210]

En cuanto a la comunidad europea tenemos que esta se rige principalmente por la "L.O.R.T.A.D."[211] (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter Personal), la cual actualmente es la legislación que ha prevalecido para regular, recomendar y tipificar a estas conductas dentro de la mayor parte de Europa, y por medio de la cual varios países de esta comunidad se han adherido a la misma, como una forma de garantizar seguridad jurídica.[212]

---

[210] RIESTRA GAYTAN, Emma. *Op. Cit.*

[211] Para tener una visón más amplia y profunda sobre el alcance de ésta Ley, recomendamos la lectura del análisis hecho a la misma con el título "La L.O.R.T.A.D. y su futuro. La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal", por Manuel Heredero Higueras, Exjefe del Gabinete de la Agencia de Protección de Datos. Consultor de Derecho Informático, en Informática y Derecho, Revista Iberoamericana de Derecho Informático. Jornadas: Marco Legal y Deontológico de la Informática, actas Volumen I, UNED. Centro Regional de Extremadura. Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura-Mérida. 1998, pág.463.

[212] RIESTRA GAYTAN, Emma. Op. Cit.

CAPÍTULO CUARTO

PROTECCIÓN JURÍDICA DEL SOFTWARE NACIONAL E INTERNACIONALMENTE

4.1 Antecedentes

Como ya ha sido expresado antes, la comercialización de las computadoras se inició propiamente en la década de los sesenta. Pues bien, en un principio el 70 % del capital destinado al desarrollo de la industria informática se empleaba en el área de componentes físicos (hardware), en tanto que el 30% o restante se canalizaba al área de soporte lógico (software).[213]

Posteriormente, la producción de equipos requirió menos inversiones. Sin embargo, la creación de programas se ha tornado más compleja y, por ende, más costosa, en virtud de que son precisamente los programas de cómputo los que soportan en buena medida el adecuado comportamiento y carácter efectivo de las computadoras. Todo ello, aunado a la falta de una estandarización de los programas, ha motivado que las cifras se inviertan, por lo que la industria de programación absorbe en la actualidad el 70% de los costos, cantidad difícilmente amortizable, entre otras cosas, por la falta de un adecuado régimen regulador que impida o limite las continuas actividades de apoderamiento ilícito en detrimiento de los creadores y usuarios.[214]

---

[213] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pág.85.
[214] Idem.

Es así como actualmente el desarrollo del software tiene un auge sin precedentes; hay todo tipo de programas y para cada necesidad, pues se puede encontrar desde un pequeño juego hasta un complejo programa para evadir seguridad dentro de los servidores de Internet y sacar información o destruirla, o "simplemente molestar". Se puede deducir que el mismo avance de la tecnología y en especial la informática favorecieron el desarrollo más complejo y dedicado del software, pues las necesidades de los ingenieros, de los inventores, de los empresarios fueron, en un determinado momento, tan apremiantes que el software pasó de ser un complemento para la computadora a ser el elemento indispensable para ella, pues actualmente no nos podemos imaginar a una computadora sin un instrumento software que dirija sus operaciones, pues sería en este caso un ser sin importancia, sin valor.

El software tiene un valor imprescindible para todo programador así como para cualquier usuario final, pues el programador como padre del software lo crea, sabe donde están sus puntos vulnerables, dónde se puede atacar en un momento dado, cómo destruirlo en un santiamén. Como ejemplo de esto tenemos cuando uno o varios "hackers" lograron accesar a los servidores centrales de Microsoft, en donde se mantiene el código fuente de varios productos clave, incluyendo el sistema operativo Windows y de la suite de aplicación de Office. De acuerdo con expertos en informática, las consecuencias de la intrusión pueden ser muy graves para Microsoft, aunque la magnitud no se sabrá hasta que quede claro exactamente qué hicieron los intrusos. Si lograron hacerse con el código fuente de las nuevas versiones de Windows y Office, éstas podrían ser usadas para detectar fallas de seguridad, lo cual comprometería a los sistemas que usen esos programas; también podrían distribuirse por Internet, de modo

que uno de los secretos mejor protegidos en el mundo informático quedaría develado.[215] –Este ejemplo lo pongo con el fin de que nos demos cuenta de la falta de protección y seguridad que tienen los empresarios por parte de sus programadores o personal encargado de cuidar sus secretos.– ¿No sería mucho mejor que se destruyera la información antes de que se permitiera el acceso a sujetos o equipos extraños a los servidores?

De hecho al tener, el código fuente al igual que, en un caso determinado, el código objeto, puede modificarse totalmente hasta llegar al grado de mejorarlo, motivando así otra versión más cara por ser nueva y mejorada, con el fin de realizar una tarea precisa y después de haber pasado las pruebas necesarias sin errores. Así, posteriormente se pone a la venta y esta es su carta de mayor presentación, no sólo ante un grupo de su profesión sino ante todo el que use su programa. En un principio y como experiencia personal, el realizar o crear programas era parte intrínseca del trabajo de toda aquella persona que supiera manejar una computadora, pues cuando se le enseñaba a usarla no sólo era para manejar un sencillo procesador de textos o realizar mantenimientos sencillos. Pues como había muy pocos programas, para ponerse a escoger el mejor o el más sencillo tenía que aprender a manejarlos a la perfección o de lo contrario podía realizar acciones que le costaran la pérdida de información e incluso del equipo. Los programas que existían venían en el idioma inglés y muy pocas personas los podían manejar así como modificar –lo que se conoce actualmente como macros–. A donde quiero llegar es que si en un principio la conducta ilícita de piratería o copia ilegal de software

[215] CHÁVEZ, José Antonio. Periódico *Reforma, "Hackean" a Microsoft.* Sección A, *Interfase.* Lunes 30 de octubre de 2000., pág.1

era escasa fue por estas razones, no siendo igual en la actualidad pues la propia tecnología informática ha otorgado las facilidades para que toda persona que tenga los conocimientos necesarios pueda realizar dichas conductas dado que basta tener una computadora y un programa especialmente hecho para esta conducta y es todo, no es necesario de tomar clases, asistir a escuelas o pedir ayuda, pues el propio programa señala cómo hacerlo, y si está en el idioma español mucho mejor pues sólo se siguen los pasos, pero si está en inglés a lo mucho lo que se tiene que hacer es acudir con otra persona que sepa hacerlo y listo, podrá utilizarlo con tan sólo unas cuantas horas de experiencia en la computadora, una experiencia totalmente empírica pero que cumple su fin: saber realizar actos o conductas ilícitas.

Por lo que respecta al usuario final, es de la misma forma imprescindible pero no para realizar conductas ilícitas –aunque no está exento de poder realizar éstas–. Este sujeto los utiliza ya sea para sus labores diarias, para su casa, para realizar transacciones bancarias, para navegar, para divertirse, para muchas y múltiples cosas, pues como ya lo dijimos anteriormente hay un sin número de programas o software los cuales en su mayoría están registrados y otros no, como es el caso de los que se hacen con el fin de realizar actos ilícitos, virus e inclusive aquellos que si bien están registrados tienen en sus adentros programas "espías", los cuales también están violando derechos, aun a sabiendas de los empresarios o programadores. Estas conductas no están actualmente reguladas, pero es importante su regulación pues hasta el momento no hay poder humano y legal que los obligue proteger sus programas totalmente sin errores u omisiones, señalando éstos que la autoridad es la que debe proteger sus derechos.

Es preciso señalar como conclusión y de la misma forma que Julio Téllez Valdés, que el problema que se

está tratando –protección de los programas– no es estrictamente jurídico, como lo señalamos anteriormente, sino que implica la presencia de otros elementos fundamentales como el técnico y el económico para que de manera global se puedan obtener resultados halagadores y palpables.

4.1.1 Evolución

Por lo que respecta a esta evolución podemos empezar diciendo que el propio avance de la tecnología es el encargado de la misma; primeramente de la creación del software y en segundo lugar del problema de la protección del mismo. Así pues ha ido evolucionando quizás no tan rápido y de la misma manera que los avances tecnológicos del Derecho, tratando de proteger tanto los derechos de los creadores sobre sus inventos u obras como de castigar las conductas que se realizan en perjuicio de éstos. Como se vio anteriormente se han dado y creado diversos actos tendiente a dicha protección, los cuales han sido en su momento correctos y con buenos resultados, pero al pasar el tiempo dejan de ser los idoneos para dicha protección, pues en lo concerniente al orden tecnológico los avances son diarios e innovadores por lo que se vuelven obsoletos. En el orden jurídico tenemos que también se han llevado a cabo acciones tendientes a la protección de estos programas o softwares, pero se siguen realizando conductas ilícitas mediante las cuales se transgeden los derechos de empresarios y/o particulares al realizar copias ilegales del software debidamente registrado por ellos.

Así pues el Derecho ha evolucionado a pasos agigantados para ponerse al nivel de las necesidades de la tecnología y en particular el Derecho Informático, para poder regular las diversas conductas ilegales ya mencionadas. En lo que respecta a nivel interno de cada país, és-

tos primeramente no les daban la importancia que merecían pues las consideraban como faltas leves e incluso "pasajeras", pero al ir pasando el tiempo se dieron cuenta que no era así pués estas conductas ilícitas ya habían tomado grandes dimensiones; fue así que decidieron tomar medidas jurídicas y regularon estas conductas desde su punto de vista y experiencia. En un país los tratarían como delitos graves y en otros como delitos simples y en algunos ni siquiera eso, pues el grado de industrialización y tecnología informática no era lo suficientemente bueno y deseable como para que se dieran estas conductas, y si las había era y es fácil de evadir la acción de la justicia.

En lo que respecta a nivel internacional, se han tomado acciones tendientes a reducir estas conductas pues jurídicamente se ha tratado de atacar este problema realizando legislaciones que tengan una uniformidad para todos los países, logrando así que se pueda tipificar y castigar a los delincuentes independientemente del lugar donde se realice la conducta ilícita. De igual forma varias organizaciones y comunidades internacionales han creado legislaciones que aplican dentro de sus territorios, independientemente de los acuerdos, tratados o convenios que hayan suscrito y firmado a nivel internacional.

Como podemos ver, el Derecho ha tratado de estar a la vanguardia de los cambios tecnológicos pero, aun así estos lo rebasan, primordialmente porque la tecnología responde a los intereses de los empresarios y de los ingenieros y no ve el daño que se pueda causar por crear ya sea software o hardware con características especiales, las cuales pueden ocupar sujetos diversos para realizar conductas ilícitas, y como consecuencia el Derecho actúa en tiempo posterior a estas conductas, ya no como medio previsor del delito sino como medio coercitivo del mismo.

Es así como ha evolucionado la protección del software, con grandes aciertos así como desaciertos. A continuación veremos cómo los países han tratado de regular estas conductas tanto en sus códigos a nivel nacional como a nivel internacional, el punto de vista por medio del cual lo han tipificado, cómo los caracterizan, por qué los han regulado penalmente y no en autoría como nuestra legislación actual, por qué proliferan en algunos países más que en otros, y por qué ha dado mejores resultados en unos países que en otros, o son escasos los resultados. Pasemos pues al estudio de la protección que se aplica al software a nivel nacional e internacional.

4.2 Aspectos fundamentales

En lo que respecta a éstos, consideramos que el problema de la protección de los programas o software no es estrictamente jurídico sino, como ya se mencionó en capítulos anteriores, aparecen tanto los elementos técnicos como los económicos, es decir la interrelación de la que ya hemos hablado entre tecnología y Derecho, en este caso entre informática y Derecho, y como consecuencia el orden económico tanto a nivel nacional como internacional, pues actualmente el Derecho necesita de los profesionistas de la cibernética e informática para poder regular debida y correctamente la conductas que se consideran ilícitas, para saber y conocer el cómo, el cuándo y el porqué sólo se las puede dar y explicar una persona que está en el medio, que utiliza a diario estos instrumentos informáticos (software y hardware).

Por otra parte pero también relacionado, aparece el aspecto económico, el cual tiene una gran importancia dentro del desarrollo de todo país que se considere avan-

zado tecnológica y socialmente pues al causar daños a esta área por las conductas ilícitas que se mencionan, no sólo se daña la economía de los empresarios o particulares que tienen el legítimo derecho sobre sus obras, sino que también se daña la economía del país pues al saber estas personas que pierden mucho económicamente hablando, optan por retirarse o por disminuir su producción dando como resultado que se produzca una crisis ya sea de producción tanto como de empleos seguros, por lo que el legislador deberá de prever las consecuencias económicas que se pueden dar si no se tipifican esta conductas, si no se regulan correctamente y si no se toman en cuenta los comentarios de los profesionistas de estas áreas para la debida legislación a crear o modificar.

A continuación veremos más ampliamente estos aspectos con sus características e implicaciones.

4.2.1 Aspectos técnicos

Los programas de cómputo se pueden considerar como el conjunto de procedimientos o reglas que integran el soporte lógico de las máquinas y permiten la consecución del proceso de tratamiento de la información.[216]

En la práctica podemos distinguir dos tipos de programas: el programa fuente y el programa objeto.

Los programas fuente (conocidos también como sistemas operativos o de exploración) están ligados al funcionamiento mismo de la máquina, guardando una estrecha relación con las memorias centrales y auxiliares de la computadora a través de dispositivos como los compiladores, traductores, intérpretes, editores, etcétera, que

[216] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pág.86.

permiten el adecuado enlace entre la máquina y los trabajos del usuario.[217]

Por otra parte tenemos los programas objeto, que son aquellos que se realizan para satisfacer las necesidades más variadas de los usuarios y permiten el tratamiento de datos definidos concretamente, siendo disociables de la máquina. En este tipo de programas tenemos los que resuelven las necesidades de un número elevado de usuarios y aquellos que "sobre medida" responden a necesidades específicas de determinados usuarios.[218]

Es evidente que los programas están relacionados de manera estrecha con los llamados lenguajes de programación, los cuales, sea del nivel de que se traten, fungen como medio de enlace entre el lenguaje natural y el lenguaje de la máquina.[219] Este aspecto técnico es el punto medular de donde se desprende nuestra propuesta, pues los códigos fuente y objeto son los cuales hay que proteger –principalmente el fuente– ya sea por medio del empresario o particular, por su propia voluntad u obligándolo a hacerlo jurídicamente; adentrémonos un poco a lo que son estos programas.

Iniciemos con el programa fuente, dando la definición de éste: es la versión del programa de computadora escrita en uno de los diferentes lenguajes de programación usualmente utilizados para escribirlo, y que permite su lectura por cualquier profesional programador.[220]

De esta definición se puede desprender la importancia del mismo, el cual se puede considerar como la base, el pilar de todo programa, sólo el programador, el creador

---

[217] *Idem.*
[218] *Idem.*
[219] *Loc. Cit.*
[220] RIESTRA GAYTAN, Emma. *Op. Cit.*

de un programa sabe como abrir el sistema de seguridad hacia éste, sabe cómo acceder al código fuente, si alguna otra persona llegáse a tener en sus manos este código puede hacer y deshacer el mismo, inclusive mejorarlo o destruirlo totalmente. Así pues, al obligar tanto al empresario o particular a proteger toda creación de programas así como el acceso a los códigos de éstos sin excusa ni pretexto, se está dando seguridad jurídica no sólo a ellos sino también al usuario final, porque el tipo de seguridad que se impondrá debe ser actual –y debe de actualizarse conforme al avance de la propia tecnología–, preciso, sin omisiones u errores de ningún tipo, y debe destruirse al momento que se quiera hacer uso ilegal de algún programa o software, por cualquier forma, o medio, logrando con esto que haya consecuentemente por parte del usuario final una confianza plena en sus productos y decida comprar éstos y no el pirata, el cual implicaría riesgos tanto económicos, técnicos y finalmente penales, beneficiándose así ellos, e inclusive si no se bajan los precios de sus productos éstos no subirán de precio, nivelando la economía de las empresas y particulares, es decir del usuario final.

En lo que respecta al código objeto, se puede definir como la versión del programa accesible únicamente a la máquina, es decir, el lenguaje comprendido por la computadora para llevar a cabo las diferentes etapas del programa.

Como podemos ver, estos códigos realizan funciones independientes pero forman dentro del programa un solo ente, son intrínsecamente uno, pues por una parte el código fuente, siendo el principal, tiene la función de comunicar a la computadora –entendida ésta como la realización de una tarea precisa– con el usuario, es decir, entablar un diálogo comprensible entre ambos, el cual una vez hecho, es codificado por la computadora hacia el có-

digo objeto, el cual tiene como fin el ordenar y realizar mediante varios procesos las tareas encomendadas por el usuario.

Es así como estos se unen, se fusionan, formándose uno solo; es por lo anterior que para la propuesta estos códigos son importantes, son la parte medular para poder disminuir y en su caso terminar con la piratería de software, pues si los programadores, inventores, creadores, ya sean personas físicas o morales los protegieran totalmente, sin objetar causa alguna o excusa, se podría extinguir este tipo de ilícitos y particularmente el de software.

Con lo anteriormente expuesto podemos ver y concluir que es vital la protección a ellos; de hecho la hay pero es insuficiente, no es garantizable, confiable, ni segura– Aquí cabría la pregunta ¿por qué? si hay los medios y técnicas suficientes e idóneas para ello, quizá como ya dijimos anteriormente hay otros intereses de por medio, más fuertes, que no permiten el realizar lo que proponemos, siendo que en particular al realizar la protección de estos códigos que es donde se puede, debe y es posible de facto instalar la seguridad contra la piratería, la protección para evitar su violación y por ende la creación de copias ilícitas ya sea en su totalidad o parcialidad del software; teniendo como resultado la disminución de las conductas ilícitas que se relacionan con éstos, y no sólo el de piratería.

4.2.2 Aspecto económico

Hemos expresado la importancia económica que reviste actualmente los bienes informáticos. Los programas de cómputo, como una de las máximas manifestaciones del producto-información, han provocado un apuntalamiento de la industria de programación, lo cual ha traído consigo que los problemas en torno al software rebasen la esfera

puramente técnica, para alcanzar niveles económicos y, por ende, jurídicos.[221]

El contenido económico indiscutible de los programas ha suscitado, entre otras cosas, que dichos bienes se constituyan en objeto de inversiones muy altas, así como de acciones ilícitas de apoderamiento, lo cual ha privado a la búsqueda de soluciones a dichos problemas, primeramente encuadradas bajo la misma perspectiva técnica y económica; estos son variados y un ejemplo de ello es lo siguiente: [222]

La misma falta de protección ha provocado que las empresas creadoras de software destinen, las más de las veces, sumas considerables de dinero para desarrollar programas similares (si no es que iguales) a los de sus propios competidores, lo cual redunda en un ofrecimiento desmedido de programas para determinadas áreas en detrimento de otras tantas, así como un precio elevado del producto. Estas dos consecuencias van en menoscabo de los intereses de los usuarios informáticos; a esta forma se le considera como un despilfarro.[223]

La lucha continúa por dominar el mercado de programación en la industria informática por parte de las empresas especializadas, y aún por los propios intereses de los particulares, genera un sinnúmero de acciones que tienden hacia un apoderamiento dentro de los "términos" más técnicos posibles, esto a través de métodos directos o indirectos, sofisticados o no, de mala o aún buena fe por manifestaciones tales como el robo, espionaje industrial, chantajes físicos o morales, etcétera, lo cual ha propiciado una búsqueda desesperada de soluciones por parte de los mismos creadores de programas. Estas se han dado bajo la

---

[221] *Idem.*
[222] *Ibidem*, pág.87.
[223] *Idem.*

forma de resguardo bajo secreto de los programas, así como dispositivos más sofisticados como la criptografía (la cual veremos más detenidamente en el capítulo posterior) o aún los temibles "virus informáticos", utilizando códigos indescifrables o introducción de instrucciones que impiden el copiado de programas, con lo cual se llega hasta el bloqueo o destrucción total de los mismos, todos ellos muy onerosos, a la vez que transitorios no obstante su relativa eficacia durante su corta existencia, ya que al estar fundamentados sobre bases técnicas, es evidente su superación por la misma técnica. De esta forma, el problema queda aún sin solución, por lo que surge la necesidad de volver los ojos hacia instituciones aparentemente más resolutorias como es el caso del derecho.[224]

4.3 Derecho Civil

En primer término, bajo la égida de esta vía tenemos a los contratos, es decir, al conjunto de cláusulas introducidas en el contrato y alusivas a la seguridad y protección de los programas, consignando el eventual acceso a los mismos por personas no autorizadas, uso inadecuado, modificaciones no pactadas, destrucción de información, etcétera. Todo ello implica un régimen de confidencialidad y resguardo bajo secreto. En la actualidad ya son varios los proveedores de software que han recurrido a este recurso contractual, sin embargo, es necesario decir que por circunstancias tales como la alta tecnicidad, desequilibrio entre las partes, problemas en la prueba, etcétera, esta figura se presenta como insuficiente frente al problema.[225]

---

[224] *Idem.*
[225] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pág.88.

En el caso anterior, consideramos que es de muy poca efectividad la vía civil para aplicar un castigo a las conductas ilícitas en comento y en particular la piratería, pues en estos casos les importa muy poco a los sujetos activos el que haya o no un contrato de por medio, si bien es un medio de protección al actuar por la vía de enriquecimiento sin causa –la cual veremos posteriormente–, esto trae aparejadas ciertas características y circunstancias que hacen de poca efectividad esta vía para poder castigar a los culpables y recuperar el patrimonio económico.

Haciendo un paréntesis, es necesario mencionar en este apartado la relación que puede tener la materia mercantil, ya que considero que este es el lugar idóneo para hacerlo, pues el realizar un apartado especial para el estudio de las conductas en análisis traería como consecuencia un desvío del presente análisis, pero como mencioné anteriormente, es menester hacer un pequeño comentario, así pues, tenemos que es más propiamente asimilable en el ámbito mercantil con la figura de la competencia desleal, como aquella que reprime las acciones deshonestas entre agentes de comercio y que operaría bajo las consideraciones de una apropiación o "sustracción" dolosa de secretos (en este caso programas) de un competidor, a fin de explotarlo comercialmente. Esto sin embargo, y muy a pesar de que por momentos se consideró, sobre todo en Estados Unidos, como solución al problema, no llega a resolver satisfactoriamente la cuestión en función de que sólo se da entre comerciantes, por lo que los particulares escaparían a dicha acción, la cual supone un comportamiento desleal que atenta contra los intereses comerciales de un competidor y que genera un desvío de clientela (lo cual ofrece serios problemas a nivel de prueba), por lo que al final se le asimila como igualmente insuficiente respecto a la situación.

[...] siguiendo la vía civil, tenemos a la figura del enriquecimiento sin causa, derivada de un principio general de equidad según el cual está prohibido enriquecerse en detrimento de otro –dicha figura la encontramos en el Libro Cuarto. De las obligaciones. Primera parte, de las obligaciones en general. Título primero. Fuentes de las obligaciones y capítulo tercero, del enriquecimiento ilícito, artículo 1882 que a la letra dice: El que sin causa se enriquece en detrimento de otro, está obligado a indemnizarlo de su empobrecimiento en la medida que él se ha enriquecido–.[226] Dicha acción requiere comprobar el enriquecimiento de uno a costa del empobrecimiento de otro, lo cual, como puede inferirse, ofrece serios problemas a nivel probatorio y aun en el caso de ser aplicada frente al problema, bien podrían desencadenarse abusos a nivel de invocarse falsas por parte de particulares o empresas en el sentido de verse perjudicados (entendiéndose empobrecidos) por una inapropiada utilización de algún programa, lo cual, lejos de ser real, bien pudiera fincarse sobre bases ampliamente sobreestimadas, por lo que el vacío subsiste.[227]

Efectivamente hay un vacío, y dentro de esté podemos incluir y señalar a las conductas que estudian como ilícitas así como también las conductas que se proponen; es decir, la de aquel productor o creador de software, ya sea persona física o moral, que no proteja su producto antes de sacarlo al mercado, así como aquellos individuos que inventan o crean algún software o hardware que les facilite el realizar actos ilícitos –piratería–. No siendo esta rama tema principal de nuestro estudio, sólo podemos señalar que quizás en algún futuro el legislador atienda con

[226] TÉLLEZ VALDÉS, Julio. *Op. Cit*, pp.88-89.
[227] *Código Civil para el Distrito Federal*, 68ª Edición. Porrúa. 2000, pág.338.

más cuidado estas conductas en la materia civil, creando un capítulo dentro del código en comento, para poder así tener más "armas", más medios jurídicos para poder castigar a quienes cometan estas conductas.

En lo concerniente al orden internacional, podemos señalar que la mayoría de los países, los cuales han considerado a este tipo de conductas como verdaderos actos que significan un peligro latente y progresivo para su estabilidad económica, política e industrial, han optado por dos vías, principalmente: la autoral y la penal, así como se han adherido ya sea a convenios, tratados o acuerdos mediante los cuales tratan de mantener reguladas estas conductas tanto en el interior de su país como en el extranjero uniformemente, para poder así castigar conjuntamente a los sujetos activos de estas conductas. Así pues, pasemos al estudio de estas conductas iniciando por el Derecho penal.

4.4 Derecho Penal

Siendo esta la rama por medio de la cual se pretende tipificar y castigar a las conductas propuestas anteriormente, haremos su análisis de forma que podamos visualizar el tratamiento que se le ha dado en varios países, primeramente por experiencia propia y posteriormente a nivel internacional con la llamada cooperación internacional, así como mediante reuniones internacionales con el fin de regular estos actos o delitos derivados de la informática, por lo que expondremos el siguiente estudio de una forma en la cual no perdamos el fin del mismo y de la propuesta y su justificación: iniciaremos con los países que han tenido mayores problemas con estos delitos y, en consecuencia, han tenido que llevar a cabo reformas a sus diversos siste-

mas legales, particularmente al penal. Como punto final de este capítulo analizaremos a nuestro país, los actos y medidas que ha tomado para prevenir y contrarrestar estos delitos, tanto nacional como internacionalmente

Francia[228]

Demos inicio con los antecedentes legislativos dentro de este país, recordando que en materia penal se fueron dando reformas o cambios en diversas etapas:

Primera etapa. Hasta 1970 la informática sólo la ocupaban empresas, eran las especialistas y hasta cierto punto su uso era elitista. Consecuentemente, no había la necesidad de legislar en este rubro. A partir de esta fecha es cuando el Estado se empieza a preocupar por esta área elaborando un Estatuto Informático (penal), instituido por iniciativa de los Poderes y el Parlamento el 6 de enero de 1978. Ya dentro de una segunda etapa se da el desarrollo comercial en la informática (segunda parte de los 70's). Las computadoras personales invaden las empresas y al gobierno, y se toma más en cuenta a este fenómeno, se da entonces una consolidación tanto penal como legislativa pero sólo se castigaba el comportamiento informático que atentara contra las personas, en el Derecho francés aún no existía pena para la delincuencia informática pues los tipos penales de éste se aplicaban en una forma equiparada, por ejemplo: robo, daño, etc., particularmente en

[228] El presente análisis es la parte más importante del análisis presentado por el Doctor BRUNO NEDELEC, Charles, en el Instituto Nacional de Ciencias Penales, llamado en éste punto de estudio: *Curso de Introducción a los delitos Informáticos. La Experiencia Francesa.* Realizado en la Ciudad de México, del 4 al 20 julio 2000, en el caso de que se haga mención de otros textos o medios de información, haremos la anotación correspondiente.

lo que respecta al software, abuso de confianza en cuanto a las tarjetas de crédito, modificaciones de datos personales. Dentro de este Derecho también nos encontramos con problemas y particularmente cuando se considera la informática como inmaterial, pues en el Derecho francés no se puede primeramente comprobar y finalmente castigar lo inmaterial, es decir, no se puede robar información, no existe esta figura como tal, consecuentemente no se puede robar software, ni ningún tipo de información. Para ejemplificar lo anterior más claramente hagamos de cuenta que un empleado roba información en un disquete de una compañía donde trabaja, será condenado no por el robo de datos sino por el del disco.

En la tercera etapa, la cual se da diez años más tarde (1988) con la creación de la "Ley Relativa a la Información, Ficheros y Libertades", se consolida el estatuto legislativo en el área penal, concluyendo este tercer momento a fines de los ochenta cuando se pone en práctica la legislación penal. Esta ley contiene 48 artículos y no sólo se limita a la informática, pues también se aplica a los ficheros manuales; por lo anterior mencionaremos sólo sus características que son de importancia para el presente estudio.

Dentro del capítulo segundo, en su artículo segundo y tercero, se reconocen dos principios fundamentales: la institución pública y privada no puede tomar decisiones sobre el comportamiento humano mediante un ordenador, "se prohíbe el gobierno por las máquinas", la evaluación de una persona física no puede ser realizada por una computadora personal. El segundo principio se da con la creación de la Comisión Nacional de Informática y Libertades, autoridad administrativa independiente que ha servido de modelo para organizaciones importantes y está compuesta por 17 miembros parlamentarios, juristas y

expositores de informática que demuestran capacidad y experiencia. Esta comisión tiene un reglamento propio y su función principal es aplicar la ley en la materia y dar a conocer al público sus derechos sobre la informática en general. Por otro lado, esta comisión tiene poder de decisión, puede crear y reglamentar en todo tipo de áreas para garantizar la seguridad informática, este poder es inclusive más importante que el de los ministros y autoridades administrativas. Dentro de estas decisiones están: realizar propuestas, modificar el sistema jurídico en cuanto a la informática, realizar avisos y recomendaciones publicadas en un boletín, así como posiciones teóricas de la comisión e inclusive dar avisos de cuáles son ficheros sensibles, sobre su constitución, esto con el fin de que no se alegue posteriormente desconocimiento o error alguno si se llegare a dar el caso de que se entrara ilícitamente a estos ficheros; de igual forma recibe peticiones y resuelve investigaciones mediante la ayuda de jueces, señala y otorga concesiones o permisos para "violar" garantías de sistemas informáticos con el fin de investigar posibles delitos, realiza también cada año un informe de trabajo para el Presidente y Parlamento, y por último organiza diversos mecanismos de protección para actos informáticos. Lo anteriormente expuesto está regulado por el artículo 45 de la ley en comento.

Iniciamos la cuarta etapa en este punto, para tener una mejor comprensión de la evolución del derecho en la informática en Francia y no causar al lector alguna confusión con la redacción de los anteriores textos y esta etapa a analizar. Así pues, esta cuarta etapa se inicia con la era del Internet –dentro de la cual se inicia un fenómeno tecnológico, social y económico, no sólo en este país sino a nivel mundial– mejor conocida como la era de la informática; paralelamente en 1993 se garantizan los derechos

o garantías individuales frente a las computadoras, según el estatuto o carta magna (lo cual es dictado por un juez). Esta carta magna es un código y actualmente está vigente y es obligatoria. En Europa muchos países se inspiraron en este modelo francés; es importante mencionar que este estatuto lo ocupa mucho la Unión Europea en sus últimas sentencias y lo pueden invocar los perjudicados directamente ante el juez.

Es de interés mencionar que en las cumbres mundiales se ha llegado al común acuerdo de que actualmente hay un exceso de normas y que se debe de aplicar el Derecho actual. Así pues y continuando en esta etapa, tenemos el Código Penal de marzo de 1993 –nuevo en esta fecha–, en su Capitulo III "Ataques sobre sistemas de Procesamiento Automatizado de Datos" tipifica la siguientes conductas:

Artículo 323-1. El acto de ingresar o mantenerse fraudulentamente en todo o en parte de un sistema de procesamiento automatizado de datos es punible con prisión que no exceda de un año y con multa de 100, 000 francos.

Cuando de esta conducta resulte la supresión o modificación de los datos contenidos en el sistema, o en la alteración del funcionamiento del mismo, el acto es punible con prisión no mayor de dos años y con multa de 200,000 francos.

Artículo 323-2. El acto de obstaculizar o distorsionar el funcionamiento de un sistema de procesamiento automatizado de datos es punible con prisión que no exceda de tres años y con multa de 300, 000 francos.

Artículo 323-3. El acto de introducir o suprimir fraudulentamente información en un sistema de procesamiento automatizado de datos es punible con prisión que no exceda de tres años y con multa de 300,000 francos.

Como podemos ver su código penal trata de regular las conductas más realizadas pero como veremos más adelante esto no ha servido de mucho –hubo reformas en 1994 las cuales veremos posteriormente–, pues hasta ahora se ha aplicado la frase: "Negociación más que represión informática".[229]

Por lo que respecta a las disposiciones penales en la Ley de Informática, Ficheros y Libertades, en su capítulo quinto y los artículos 41, 42, 43 y 44, se señala que en caso del fracaso del dispositivo de prevención se aplicará ésta en las disposiciones anteriores, estos se encuentran en una ley especial y no en el código penal. Por lo que respecta al nuevo código (1994), la situación se modifica pues con la de 1978 se suprimen y se incluyen en el código penal para tener en un solo documento estos delitos, la mayoría se traducen sin cambios importantes (sólo cambió el texto).

Ahora bien se han reconocido siete delitos relacionados con la materia informática regulados en el artículo 226 y sus fracciones, los cuales son:

- Creación de fichero clandestino.
- Falta de preservación de la información.
- Tratamiento de información.
- Conservación de datos sensibles.
- Conservación de ficheros informáticos.
- Desvió de información recolectada, regularmente datos.
- Proteger las libertades individuales, divulgación voluntaria o involuntaria de la vida personal.

[229] BRUNO NEDELEC, Charles. Instituto Nacional de Ciencias Penales. *Curso de Introducción a los delitos Informáticos. La Experiencia Francesa.* México, 4 al 20 julio 2000.

Teniendo un antecedente más claro del largo camino que ha recorrido Francia para realizar una legislación acorde con los cambios tecnológicos que proteja los intereses tanto de las personas morales y físicas, ahora veremos qué tanta eficacia han tenido, si han resultado sus diversas reformas legales como se tenía proyectado en sus inicios.

Así pues los poderes públicos actuaron en un principio a petición de la sociedad, pues se consideraba como un riesgo para la misma en diferentes puntos, por lo que se creó la "CREL" la cual a contribuido en 20 años al desarrollo armonioso de la computadora personal y las empresas y ha servido también como modelo para crear autoridades administrativas. Es importante mencionar que los derechos de las personas informatizadas son esenciales en Francia y en toda Europa, es decir en la Comunidad Europea –hasta octubre de1995 eran 15 países– dentro de la cual se regula sobre la protección de las personas físicas, en cuanto a la protección de datos, definiendo la legalidad, el tratamiento de datos, los derechos especiales de las personas, crea autoridades nacionales para proteger a las personas físicas y sus datos. Como características de la "CREL" tenemos que: es un producto de exportación en toda Europa, pues toda la economía francesa se rige por la "CREL" , tanto administrativa como penalmente, su mecanismo legal es complejo administrativamente, la compilación penal de la "CREL" es un fracaso pues es una institución con vocación moral que trata de una solución sin castigo penal, utilizando "la fórmula de advertencia solemne"; en 20 años sólo tres veces se ha actuado ante el Ministerio Público, aunque esto es una violación a la legislación pues debe de actuar e imponer justicia penal.

En cuanto a la competencia de la "CREL" tenemos que es: denunciar ante el juez para que éste imponga

la sanción penal, pero esta los excluye unilateralmente, por lo que se ha perdido el carácter disuasivo de la parte penal. No hay colaboración entre las dos instituciones, sólo hay una guerra por mantener el poder en los delitos o actos informáticos; es así como el sujeto dañado puede actuar ante el tribunal sin pasar por el Procurador.

A partir de 1994 se realizaron reformas al Código Penal Francés, tipificando los delitos contra los sistemas automatizados, introduciendo cuatro tipos de infracciones:

1.- Introducción fraudulenta en los sistemas.

a) Enunciada en el artículo 323 del Código Penal Federal, sin acceso y mantenerse fraudulentamente. La Ley no difiere la forma de acceso o penetración, pero están todas las posibles.
b) Falta de autorización para acceso, no tiene derecho a permiso o no se respeta la voluntad del titular, del administrador del sistema. Aquí debemos de mencionar que la seguridad es más elevada que en Alemania, esto porque más adelante veremos las características legislativas y penales de este país para con los delitos informáticos.

I).- Mantenerse en el sistema informático.

a) No debe quedarse más del tiempo permitido.
b) Que el autor no esté conciente que la conducta a realizar es un delito, en caso de ignorancia, el móvil es el hecho delictuoso y que el autor del hecho haya actuado con algún fin inclusive didáctico.

Puede haber aumento de sanciones al doble si:

a) Modifica o suprime datos.
b) Altera el funcionamiento del sistema.

En cuanto al acceso a un sistema sin realizar acto ilícito alguno dentro de éste, en el Código no existe tipo penal alguno. Esto tiene mucho de importancia pues hay algunos países en los cuales si lo tienen penado e inclusive, mandan un mensaje vía internet dando a conocer el delito y su castigo, por lo cual el intruso no puede alegar error alguno al momento de que se castigue.

2.- Obstaculizar el funcionamiento del sistema, artículo 323.

- Para destruir información.
- Virus.
- Bomba lógica.
- Bloqueo de acceso.
- Cambio de password, aquí hay dos excepciones: en caso de huelga y rotura de un contrato de abastecimiento.

3.- Acción fraudulenta de datos.

Introducción en modo de datos contenidos en sistemas informáticos, puede ser en vía de elaboración (pero es la copia de datos en diskette), esto es, pueden ser datos en forma de programas, virus, pero voluntariamente en servidor por medio de un cliente el cual también tiene o se determinará su responsabilidad un ejemplo de esto es el Caballo de Troya: aquí existe un dolo general, pues el fin es perjudicar el lugar o computadora donde se instale.

4.- Malhechores informáticos.

- Se les conoce como malhechores informáticos a quienes intervienen cuando la infracción informática es realizada por más de un infractor informático.
- El legislador actúa consecuentemente contra los clubes, asociaciones y piratas.
- Sólo sanciona la complicidad y no a quien lo hizo.
- La ley no define a la asociación así pues esta puede ser física o moral, no importa qué tan pequeño o grande sea el grupo.

Como podemos ver, dentro de esta descripción hay una característica que es importante para nuestro estudio y es el punto tres: sólo se sanciona la complicidad y no a quien lo hizo. Esto quiere decir que la ley considera sólo como delito aquel que se cometa en grupo, pero no sanciona al autor material –quizás desde mi punto de vista es una forma de proteger a la ciencia o a los "genios"–; esto tiene algo de similitud con Estados Unidos, pues ellos no consideran piratería aquella conducta mediante la cual se realicen copias ilegales siempre y cuando no sobrepase "un límite" que ellos tienen reglamentado, el cual lo veremos en su tema correspondiente.

Por otro lado, Francia tiene la Ley Godfra, la cual en sus inicios tenía como fin tipificar la falsificación de documentos informáticos, pero al haber cambios tan radicales en el avance de la tecnología se reformó para dejar de existir el delito de falsificación informática, la cual quedó ahora sólo como falsificación. Puede castigarse la alteración fraudulenta en un escrito u otro soporte, que tiene por efecto comprobar un hecho de consecuencias jurídicas.

Respecto a la represión –castigos– que se utiliza en Francia para estas conductas tenemos que las sanciones no son sólo simbólicas, estas son diversas:

- Un año de prisión y multa si hay daño de datos, pero si daña un sistema será la pena de tres años de prisión y multa.
- Asociación criminal. Por las acciones principales del grupo.
- *Las personas morales pueden ser condenadas (últimas reformas). Ya sea que la infracción la cometa por su interés y para sí mismo o sea cometida por tercera persona, el castigo es independiente del que se imponga a la persona física que lo realizó.*[230]
- Contempla también la situación de la víctima respecto del castigo al sujeto activo.

Como conclusión podemos decir que las incriminaciones escritas en el Código Penal parecen completas pero es difícil comprobar la propiedad, pues los tribunales protegen al sistema y la información que contienen; en consecuencia, los jueces sólo castigan por introducción ilícita al sistema y no por violar los derechos de autor.

Los jueces (justicia penal) no tienen el filtro de la "CREL", ya que argumentan: dificultad para obtener pruebas, aplicar sanciones penales, por lo que esto no conduce a un fin cierto y no castigan al delincuente.

---

[230] Este punto es importante para nuestro estudio, pues como podemos ver Francia ya regula la conducta de las personas morales por su responsabilidad en la comisión de delitos informáticos –aunque no por la conducta propuesta– y la pena por esto es diferente a la del sujeto que lo comete bajo sus ordenes o alentado por el.

"Hay una hipocresía de los poderes públicos, pues critican a la telemática pero no adoptan medios reales para atacar a estos delitos, pues estos propusieron leyes pero no las adoptaron por las anteriores "justificaciones" de los jueces".

A nivel internacional es muy complejo tanto la persecución, el castigo, y aplicar una pena finalmente.

Es difícil la cooperación internacional, especialmente con Estados Unidos, pues es diferente la regulación del derecho de libertad de expresión en este país, y otra causa es que Estados Unidos rechaza la ayuda en delitos constituidos en Europa, pues en éste no existen como tales, por lo cual no existe cooperación internacional. Respecto a ésta tenemos que también se oponen Estados Unidos y Canadá en cuanto a la responsabilidad de los proveedores, ya señalada anteriormente.

No hay penas específicas para los delitos informáticos.

España

Por lo que respecta a este país, analizaremos su desarrollo legislativo dentro de la informática, la forma en que han ido dando protección a las áreas diversas que utilizan diariamente la computadora u ordenador, como mejor se le conoce en este país, así como la forma en que fueron dándole la importancia debida y necesaria a este problema y fenómeno derivado del avance tecnológico mundial, hasta nuestros días.

Iniciemos con su Constitución del año de 1978, la cual en sus artículos 9, 18, 20 y 24, establecía regulaciones en cuanto a los delitos informáticos –los cuales en éste país se conocen como telemáticos– sólo que se trataban de forma muy general, y específicamente en el apartado cua-

tro, señalaba: "La Ley Garantizará el uso de la informática". Así pues el legislador, a partir de la Constitución de 1978 y hasta 1995, no se ocupa de reformar, legislar en el tema de la informática, dándose así un vacío legal en cuanto a estos delitos, por lo cual se puede inferir que la regulación española es joven en esta materia; pero para ellos es un gran paso de actualización y tratamiento de este problema que con el paso del tiempo se va haciendo más complicado por el propio avance de la tecnología a nivel mundial.

Analicemos a la delincuencia informática; esta inicia con la era cibernética, la cual cambia la estructura de la sociedad, su mentalidad y sus hábitos. De lo anterior surgen problemas, los cuales hay que prevenir, regular, tipificar y castigar como última instancia, estos son:

1.- El problema que surge dentro de la era informática hace referencia a la necesidad de garantizar la intimidad, derecho fundamental dentro de los derechos humanos (compras en internet, datos personales protegidos). La pregunta es ¿cómo garantizar esto?.

2.- El mundo de Internet necesita una regulación pormenorizada de las conductas que se susciten dentro de él.

3.- Hay necesidad de regular jurídicamente los actos ilícitos que pueden vulnerar a los bienes protegidos o tutelados por el Estado, ya sean ilícitos, administrativos o penales. En este punto es donde nosotros hemos de analizar la forma en que han legislado y por ende regulado las diversas conductas ilícitas que se han ido dando dentro de su país, así como en la Comunidad Europea.

Desde el punto de vista doctrinal, la realidad de la criminalidad informática se da en dos grupos:

1.- Grupo de delitos que recaen sobre objetos pertenecientes al ámbito de la informática: sustracción de programas, reproducción de datos, etc.

2.- Grupo integrado por la comisión de los delitos más tradicionales: Derecho de Propiedad Industrial, Derechos de Autor y Derechos de Propiedad Intelectual.

Uniendo a estos dos grupos podemos definir a la Criminalidad Informática como: la realización de un tipo de actividades que reúnen los elementos del delito, sean llevadas a cabo utilizando un elemento telemático, o sean llevadas a cabo vulnerando el derecho del titular del elemento o programa; aquí el elemento informático no es el medio sino el fin.

Así pues no se ataca a los objetos de la informática, pero estos son el medio para llevar a cabo en este tipo de delitos y por ende hay que regularlos.

Al mismo tiempo se hacían varias preguntas relativas a la criminalidad informática dentro de su sistema legal, las cuales son:

- ¿Qué tratamiento recibe la criminalidad informática en el Código Penal Español? (esto era novedoso en este momento, era real y palpante el regular esta conducta)
- ¿El Código Penal no los menciona materialmente?
- ¿Dependen de la informática todos los medios?
- ¿Todos los delitos informáticos se cometen por medio de un ordenador?.

Es así como la mayoría legislativa dice que hoy no puede hablarse de delito informático como concepto,

como un solo tipo, pues intervienen diversos sectores así como en particular el Derecho Penal, concluyendo que:

1.- No existe un delito informático; existe una realidad compleja que liga a las nuevas tecnologías de la informática, pues por su diversidad no puede haber un solo tipo de delito informático.

2.- Las parcelas –áreas– más afectadas son tres:

a) Todos los atentados contra la intimidad, artículo 197.
b) Los atentados contra los intereses de contenido económico, artículos 248.2, 256, 254.2 y 278.
c) Falsedades documentales, artículo 26.

Consecuentemente la criminalidad informática se relaciona no sólo con lo informático de manera específica, se incluye todo lo que se pueda realizar por medios informáticos, por ejemplo; blanqueo de dinero, pero hay delitos que ya son "tradicionales", es decir ya están tipificados, sólo que no se excluye a los que se puedan realizar por medios informáticos; sin embargo, antes de llegar al castigo penal, se trata de "atacar" a estas conductas ilícitas por otras vías tanto jurídicas como administrativas, particularmente por la vía preventiva, es decir, se trata de prevenir la realización de estas conductas.

Así pues, en el Código Penal Español se hacen reformas con el fin de regular las conductas diversas que se dan con los nuevos avances tecnológicos y a los cuales se les conoce como delitos telemáticos, regulados en el capítulo quinto del código en comento. Dentro del articulado de este capítulo hay diversas conductas tipificadas, las cuales mencionaremos pero sólo para tener presente el

nivel de la reformas que se llevaron a cabo en España y haremos especial mención en aquellas que están relacionadas con nuestro tema.

Por lo que se refiere a delitos contra el patrimonio y orden sociológico, los cuales son una novedad en cuanto a la reforma, estos se regulan en dos grupos:

1.- Infracciones patrimoniales cometidas por medios informáticos: estafa, tarjetas electromagnéticas y robo.

2.- Utilización ilícita de tarjetas electromagnéticas, al delito de robo con violencia.

En cuanto al tipo de robo, la reforma que realizó al código penal hizo especial énfasis en los artículos 238 y 239. Respecto al artículo 238 se hace mención del uso de "llaves falsas", y en específico el articulo 239 señala y define a estos tipos de llaves, las cuales son magnéticas o perforadas y los mandos o instrumentos de apertura a distancia, e inclusive se considera en este rubro a la tarjeta de crédito, pues hasta antes de las reformas de 1995 quedaba impune la conducta ilícita realizada por medio de este tipo de llaves.

La estafa informática se encuentra regulada en el artículo 248.1, el cual sufrió las reformas necesarias, pues la estafa tradicional no se establecía en la informática, como lo podemos ver a continuación en el artículo 248.1: Comenten estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. Con la reforma podemos ver cómo se trata de regular este tipo de acciones con los medios informáticos inmersos en la propia conducta, ya sea como medio o fin de ésta, artículo 248.2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante, consignan la transferen-

cia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Como podemos ver es nuevo el medio por el cual se regula la conducta, pues de igual forma es nueva la manipulación de datos informatizados en el código penal y desaparecen requisitos del tipo penal tradicional de estafa; aquí los legisladores opinan en forma común su acuerdo relativa a la reforma, señalando que es oportuna y válida.

El intruismo se define, según el código penal español, como: el que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses, artículo 256.

El sabotaje, el cual se encuentra regulado por el artículo 274.2, se define como: [...] Las mismas penas se impondrán a quien, a sabiendas, posea para su comercialización o ponga en el comercio productos o servicios con signos distintivos que, de acuerdo con el apartado 1 de este capítulo, suponen una infracción de los derechos exclusivos del titular de los mismos, aun cuando se trate de productos importados del extranjero.

El espionaje informático se regula en el artículo 278.1, el cual lo define como: El que para descubrir un secreto de empresa se apodere por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses [...]. Respecto a este tipo, el legislador hace referencia al espionaje informático aunque no le puedan ser aplicadas las reglas o tipos sobre la propiedad intelectual contempladas en el artículo 270, el cual lo veremos a con-

tinuación más ampliamente por ser el que contiene la conducta de reproducción ilícita de programas o software, objetivo del presente estudio.

Es así como llegamos al capítulo XI. De los Delitos relativos a la Propiedad Intelectual e Industrial, al Mercado y a los Consumidores. Sección 1ª. De los Delitos relativos a la Propiedad Intelectual. Artículo 270. Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.[231]

La misma pena se impondrá a quien intencionalmente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

---

[231] El artículo 17 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizado, aclarando y armonizando las disposiciones legales vigentes sobre la materia, sostiene: Corresponde al autor del ejercicio exclusivo de los derechos de explotación de su obra en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser realizados sin su autorización, salvo en los casos previstos en la presente Ley.

Artículo 271. Se impondrá la pena de prisión de un año a cuatro años, multa de ocho a veinticuatro meses, e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando concurra alguna de las siguientes circunstancias:

a) Que el beneficio obtenido posea especial trascendencia económica.
b) Que el daño causado revista especial gravedad.

En tales casos, el Juez o Tribunal podrá, asimismo, decretar el cierre temporal o definitivo de la industria o establecimiento del condenado. El cierre temporal no podrá exceder de cinco años.

Como podemos ver, España ya tiene tipificada la posible conducta del empresario o profesionista que fabrique, ponga en circulación o tenencia cualquier medio que facilite la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador, y por otro lado también señala que el juez podrá decretar el cierre temporal o definitivo de la industria o establecimiento del condenado. Como podemos ver España trata de proteger al máximo la propiedad intelectual dentro de su territorio, pero ¿qué pasa cuando estos medios son creados o diseñados en el extranjero o inclusive en su propio territorio? Es claro que también sus legisladores se han abocado, como en la mayoría de los demás países a regular la conducta de los sujetos activos que utilizan como medio o fin las diversas herramientas tanto de software como de hardware para cometer dichas conductas.

Respecto de la facultad que se otorga al juez para poder decretar ya sea el cierre temporal o definitivo de la

industria que infringe la ley, consideramos que es una medida totalmente aceptable y tomada a tiempo, pues de otra manera seguirá proliferando de forma indiscriminada la producción de estos medios que facilitan la comisión de los delitos informáticos, en su modalidad de piratería.

Respecto a lo anteriormente dicho, creemos que este tipo de legislación indudablemente pone un freno a la creación de dichos medios por los cuales se cometen las diversas conductas ilícitas, pero aun así deja algunas preguntas y a la vez lagunas, pues por una parte sanciona la creación de medios por los cuales se realicen dichos actos, principalmente en su territorio, pero por otro vemos que hasta el momento no sanciona o dirige sus líneas legislativas para con la responsabilidad del empresario o creador de dichos medios por no otorgar la seguridad debida, idónea y necesaria para que una vez que sus productos salgan al mercado, no puedan ser copiados ilegalmente. Con esto quiero decir que estos sujetos tienen una responsabilidad por otorgar o facilitar los medios por los cuales se cometen las conductas ilícitas, un ejemplo claro en contrario sensu de esto es la creación de programas para copiado de CDs, con la capacidad de violar o traspasar sistemas de seguridad en diversos programas originales, especialmente el programa llamado "Nero", pues si los empresarios pueden crear un programa que logre traspasar un sistema de seguridad anticopias, pueden entonces crear a la vez un programa que proteja a sus creaciones contra cualquier acto de piratería, por lo que se puede deducir la responsabilidad penal que tienen y por la cual se debe tipificar su conducta.

Artículo 272.1. La extensión de la responsabilidad civil derivada de los delitos tipificados en los dos artículos anteriores se regirá por las disposiciones de la Ley de Propiedad Intelectual relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios.

Las auditorías informáticas previenen, es la represión que a ellos mejor les ha resultado. Las medidas que España toma son:

– Ley Orgánica de Protección de Datos de 1999, la cual aplica sanciones administrativas.
– Promover la cooperación internacional, colaboración judicial y policial.

Hay acciones muy comunes por lo cual es mejor crear una legislación telemática y no utilizar la analogía, equiparar con delitos tradicionales; en México no hay analogía pero sí se equiparan con otros tipos penales las conductas realizadas por delincuentes informáticos.

En cuanto a los delitos tradicionales, como ya se habló anteriormente de ellos, hacen que no se creen nuevas figuras si es que no es necesario, pero si es, entonces sí se crean tipos acorde con las necesidades del propio avance del Derecho y la tecnología. Así pues también tenemos que en los delitos informáticos hay atenuantes y agravantes por lo que la autoridad toma ciertos elementos para ello; algunos de estos son:

1.- Que bienes jurídicos tutelados se transgedan, así como en algunos casos los Derechos Humanos.
2.- Que demuestre arrepentimiento.
3.- Que haya reincidencia

Por último, hay dentro del Código Penal Español una característica que no debemos omitir y es aquella que se encuentra en el artículo 197.4, que a la letra dice: "Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos,

archivos o registros, se impondrá la pena de prisión de tres a cinco años, [...]". Como podemos ver, el legislador tiene ya una visión clara de lo que puede hacer una persona capacitada y/o con los conocimientos necesarios para poder operar una computadora así como todos sus accesorios y programas en perjuicio de los derechos de otros. Esto es muy importante para nuestro país pues es cada día más claro que personas con conocimientos en informática realizan las conductas ilícitas y, sin embargo, si se les logra fincar alguna responsabilidad ésta no es agravada por ningún elemento característico de su conducta. Por otro lado, también es agravada la conducta de los servidores públicos que teniendo estudios técnicos o profesionales realicen conductas ilícitas, sin justificación alguna, artículo 198.

Estados Unidos de América

Dada la frecuencia con que se han presentado estas conductas, directamente relacionadas con su nivel de desarrollo, es importante conocer la respuesta que en este país se ha dado al fenómeno del *computer crime* (crimen informático o computacional).

En este sentido, Gutiérrez Francés resalta la importancia de estas conductas en Estados Unidos al señalar que "el alto nivel de desarrollo económico y tecnológico de los Estado Unidos ha propiciado una *computer dependency* superior a la de otros países de nuestro entorno, favoreciendo a la vez, como contrapunto, una experiencia precoz en materia de criminalidad mediante ordenador.[232]

[232] CONTRERAS SALDIVAR, Gabriel. *Op. Cit.*, pág.42.

El Derecho Penal estadounidense, basado inicialmente en el *common law* (*case law*, derecho basado en precedentes), ha venido a fundamentarse actualmente en los estatutos legislativos. Cada Estado tiene sus propios estatutos penales, en tanto que el gobierno federal, en ejercicio de su competencia, ha regulado a los delitos informáticos sólo en cuanto conciernen a las materias federales.[233]

En el Código de Estados Unidos, la Sección 1030 considera como delitos:

(1) El que a sabiendas accese a una computadora sin autorización o más allá de lo autorizado para obtener información determinada por el Gobierno de los Estados Unidos como información que requiere protección contra la revelación no autorizada, por razones de defensa nacional o de relaciones internacionales...

(2) El que intencionalmente accese a una computadora sin autorización o más allá de lo autorizado y como consecuencia obtenga:

A. Información contenida en registros financieros de instituciones financieras o contenida en el expediente de un cliente de una agencia de información sobre clientes, en los términos en que los define la Ley sobre Reporte de Créditos;

B. Información de cualquier computadora protegida, si la conducta involucra comunicaciones entre los Estados o hacia el exterior.

C. Información de cualquier computadora protegida, si la conducta involucra comunicaciones entre los Estados o hacia el exterior.

---

[233] *Ibidem*, pág.43.

(3) El que a sabiendas y con la intención de defraudar accese sin autorización o más allá de lo autorizado a computadoras protegidas y por ese medio obtenga cualquier valor, a menos que el objeto del fraude y la cosa obtenida consistan sólo en el uso de la computadora y el valor de tal uso no sea mayor de $5,000.00 durante el periodo de un año.

(4) Quien a sabiendas cause la transmisión de un programa, información, código o comando, y como consecuencia de esa conducta intencionalmente y sin autorización, cause daño a una computadora protegida; o intencionalmente y sin autorización accese a una computadora protegida y cause daños...[234]

Como ejemplo de una Ley Local puede citarse al Código Penal del Estado de Texas. Estas conductas están previstas en el Título 7 "Faltas en contra del Patrimonio", Capítulo 33, "Delitos Computacionales" (1994).

"Violación de los Sistemas de Seguridad de Computadoras".

A. Comete un delito, quien con conocimiento, accese a una computadora, red de computadoras o sistema de computadoras sin el consentimiento de su propietario o de la persona legalmente autorizada.

B. Comete un delito, quien intencionalmente o conscientemente, dé a otra persona la clave de ingreso, código de identificación, identificación personal, número de tarjeta de débito, número de cuenta bancaria, o cualquier otra información confidencial sobre el sistema de seguridad de una computadora, sin el consentimiento de quien utiliza el sistema de seguridad, para restringir el

[234] *Ibidem*, pp.43-44.

acceso a la computadora, red, sistema computacional o datos.

C. Estas faltas son consideradas como delitos menores, salvo que la intención del delincuente sea obtener un beneficio, defraudar o dañar a otro, en tal caso se considerará:

a) Un crimen que merece prisión estatal, es el caso de que la pérdida o daño sea menor de $20,000.00 dólares o
b) Un crimen grave, si el valor del beneficio o el monto de la pérdida o daño es mayor a $20,000.00 dólares.[235]

Como puede apreciarse, en los cuatro ordenamientos citados se sanciona el acceso y obtención de información, lo que puede ser indicativo de que el bien jurídico protegido, tal vez entre otros, es la información o el derecho de su titular sobre la misma. A este respecto cabe señalar que no son pocos los países que sancionan el simple acceso no autorizado a sistemas informáticos, entre otros: Australia, Dinamarca, Finlandia, Grecia, Irlanda, Israel, Italia, Países Bajos, Noruega, Suecia y Suiza.

Se puede apreciar la línea que se sigue o mejor dicho qué países se han decidido por regular estas conductas ilícitas, pues en la gran mayoría se trata de Estados con un gran poder económico, político, social y cultural, dentro de los cuales no veremos por un largo tiempo a otros países, inclusive a México. Podría ser por varios elementos el que no estén en esta lista, pero a estos elementos o causas no le importará al crimen cibernético pues al contrario son una gran atracción para ello, pues con sus siste-

[235] *Ibidem*, pp.44-45.

mas vulnerables –por pequeños que sean– ante cualquier ataque o violación por parte de los diversos sujetos activos ya vistos anteriormente, no habrá acto o delito que no se pueda realizar dentro y fuera de estos países, y si a esto le agregamos que no tienen una legislación que contemple estas conductas, podemos imaginarnos los problemas que tienen actualmente así como los que se generarán en un futuro próximo.

Por otra parte, veamos ahora el punto de vista de un experto en el área del crimen informático o cibernético, el cual no sólo nos dará su opinión como parte del sistema gubernamental encargado de la investigación y persecución de estos delitos sino acerca de la forma en que se ha tratado el problema jurídicamente, principalmente por la vía penal. Empecemos por analizar la frase que utilizó el Dr. Rodolfo Orjales[236] que señala: "Para nosotros (Estados Unidos de Norteamérica), México no le da aún la importancia debida a este problema, quizás por que aún no ha tenido grandes persecuciones o no ha llegado en gran dimensión a su país, e influye en esto el que no tiene una actualidad informática vanguardista, pero pronto lo será".[237]

Ciertamente estamos en circunstancias tecnológicas diferentes y en clara desventaja con relación al país más poderoso en el continente americano y quizás del mundo, por lo que nosotros vemos hasta cierto punto con un grado de indiferencia los problemas tanto legales como

[236] Instituto Nacional de Ciencias Penales. *Curso Introducción a los Delitos Informáticos. La Experiencia Estadounidense.* Computer Crime Intellectual Property Seccion (CCIPS). U. S. Dept. Justice. Washington D.C. 4 al 20 julio del 2000.

[237] Apartir de éste párrafo, la fuente del diverso material que se encuentra en el presente apartado en comento, es en su mayoría parte del Curso Introducción a los Delitos Informáticos. La Experiencia Estadounidense, expuesto por el Doctor Rodolfo Orjales dependiente de: Computer Crime Intellectual Property Seccion (CCIPS). U. S. Dept. Justice. Washington D.C., en aquellos casos donde sea diferente la fuente se hará la mención necesaria.

tecnológicos que se presentarán en un futuro próximo, si no es que ya los tenemos y muy serios por cierto[238]. De esta experiencia debemos tomar lo que nos hace falta, tanto para prevenir las conductas ilícitas que ya se conocen como aquellas que si aún no llegan a nuestro país como tales, muy pronto las tendremos, por lo cual el legislador debe tomar medidas tanto para regular y corregir el presente problema como los que llegarán con la tecnología de punta que se desarrolla a pasos acelerados mundialmente.

Así pues, analicemos algunas de las instituciones creadas, así como las acciones y medidas que han tomado para legislar, prevenir y castigar las conductas ilícitas que se comenten por medio de la informática o bien como el medio para cometer dicho acto.

Una institución creada para la lucha contra los delitos cibernéticos es "The Computer Crime Intellectual Property Seccion (CCIPS), la cual se especializa en delitos en propiedad intelectual, derechos de autor, marcas, delitos cibernéticos; fue fundada en 1991 y sus características principales son:

- Inicialmente empezó con 20 abogados, doblando esta cantidad en tamaño cada 3 años.
- Su misión es combatir el crimen cibernético.
- Se analizan los alcances del crimen cibernético y los problemas que se desprenden de éste, tanto a nivel nacional como internacional.
- Coordina los esfuerzos tanto de aplicación de castigos como de la propia aplicación de la ley.

[238] Ver *Supra* Capítulo III.

- Entrena a los agentes para la persecución de los delitos cibernéticos y para la formación de fiscales en la materia.
- Coordina los esfuerzos intelectuales semejantes, ya sea a nivel nacional o internacional, así como con otras instituciones locales y federales.
- Propone reformas y hace comentarios sobre legislaciones afines al crimen cibernético, tanto local como federal.

Ahora bien, el crimen cibernético es tomado o definido como: aquellas personas u objetos que son víctimas de ataque por algún medio informático o inclusive como fin del ataque el equipo informático. Por otro lado, al igual que en nuestro código penal, se señala que el delito puede ser instantáneo, permanente o contínuo y continuado, así como se puede presentar la figura del cómplice para poder realizar estos actos ilícitos; de lo anterior podemos concluir que hay tres reglas que consideran y toman como discretas (*three discrete roles*), estas son:

1.- Sin víctima u objeto de algún ataque; esto se da cuando la computadora, cualquier tipo de ella, sufre algún ataque, el sujeto que realiza el daño o ataque tiene el deseo de obtener información.

El ataque puede ser a una información sensible o clasificada (*sensitive information*); ésta puede ser militar, comercial, clasificada, de inteligencia, secretos comerciales internacionales, datos personales, números de tarjeta de crédito, documentos financieros.

2.- Se inicia con ellos un ataque, mejor conocido como daño al sistema (*Damage to System*), realizado por el sujeto activo conocido como "Hacker" ya estudiado y

analizado su conducta dentro del ambiente informático anteriormente. Dentro de las características que tiene en sistema norteamericano están las siguientes:

- Destrozar, dañar el sistema computacional y otros propósitos dentro del sistema (*breaking in for other purposes*).
- Realizar ataques de vandalismo en la "WEB".
- Dañar ventanas dentro de la "WEB".
- Traspasar llaves de seguridad.
- Destruir propiedades (possesions).
- Virus Melissa y otros.

3.- Se da la figura del cómplice.

Como mero antecedente y para tener presente el avance del crimen informático, en Estados Unidos tenemos el informe de la "Nation Information Protección Central", Central de Información Nacional de Protección (NIPC), por sus siglas en ingles, en el cual se ve como en un solo año ha crecido en dimensiones extremadamente peligrosas el crimen cibernético, pues en 1998 fue de 547 casos en concreto y en 1999 fue de 1154 un poco más del doble.

Así pues, la "Inspección de seguridad contra el crimen de computadora" rindió un informe donde señala las conductas más realizadas:

- Hubo un 98% detectado en el quebrantamiento de seguridad.
- El robo de información privada.
- La defraudación financiera.
- Aumentó el sistema de penetración por forasteros o intrusos.

- Se sabotea más continuamente la red de datos.
- Se crea la figura –y se utiliza principalmente en la "WEB"– o tipo de negativa de servicio.

Más específicamente podemos señalar a quien ataca a las computadoras de una forma contínua o con intereses muy poderosos, que utilizan todos los medios que están a su alcance tanto económicos como tecnológicos, siendo estos últimos los empleados de personas o empresas, los entrometidos o intrusos –hackers, ckrakers–, los agentes industriales de espionaje y los operativos extranjeros de inteligencia.

Hay otros grupos, pero su actuación está regida por motivos de tipo político, religioso o económico; algunos de ellos son: Hack-Tevisión (Por motivos políticos entran a la Web para manifestar su descontento), Virus Writers (entran a los sistemas informáticos y dejan virus para que destruyan ya sea información, bases de datos, programas o simplemente destruir todo), grupos criminales, terrorismo, grupos de inteligencia, alternativa de guerra (*Information Warfare*).

Por lo que respecta a las herramientas de la computadora y cuando ésta es utilizada para atacar, es decir como medio para realizar el delito, podemos señalar como conductas principales de este tipo: el crimen tradicional conectado –conexión a internet–, la defraudación, el juego, la pornografía infantil, la piratería y el acosamiento. Podemos resumir que los medios por los cuales se cometen el o los crímenes de computadora son principalmente los hackers; si se regula el delito de y para las computadoras esta regulación puede ser el arma contra otras computadoras, –por lo que se refiere a nivel local–. Este tipo de

delitos o crímenes cibernéticos son relativamente nuevos; aunque se pueden regular en base a los delitos tradicionales no es suficiente en la actualidad, ni en el futuro ya próximo.

Por otra lado, tenemos también la regulación en el marco internacional. Los principios a considerar en cuanto a la Organización de Estados Americanos (OEA) y el Informe sobre Delitos Cibernéticos.

Este trabajo se llevó a cabo en Lima, Perú, en marzo de 1999, con tres principales temas a tratar.

1.- Condiciones de Cárceles
2.- Extradición.
3.- Delitos cibernéticos.

Por lo que respectá este informe, nos hemos de colocar en el punto tres, tema central de nuestro estudio.

Los puntos principales de esta reunión fueron:

- Crear un grupo especial de Ministros de Justicia con el fin de que éstos sean especialistas en los crímenes cibernéticos, desde sus generalidades hasta sus formas específicas de acción.
- Organizar un grupo de expertos para delitos cibernéticos, en octubre realizar un reporte a los Ministros de Justicia en el cual se emitirán diez recomendaciones.
- Analizar el tipo de necesidades y equipos técnicos que tiene cada país, para poder dirigir correctamente la capacitación de su grupo de expertos.
- Que sea un grupo de contacto. Es decir que se conozcan para trabajar directa y correcta-

mente a nivel internacional, pues si no se trabaja así, se pierde mucho tiempo en buscar y contactar a la persona encargada en cada país en situaciones urgentes de investigación.

Los ministros aceptaron estas consideraciones así como los siguientes principios de Acuerdo –recomendaciones, mencionaremos sólo las que se relacionan directamente con nuestra área de estudio–:

Se acepta:

a).- Los delitos cibernéticos no tienen fronteras, por lo que si hay un país que no legisle esta conducta; estamos todos los países desprotegidos de estas conductas ilícitas.

b).- Hay la necesidad de armonizar leyes para mejorar la cooperación internacional.

c).- Se afirma la importancia de mantener la integridad, disponibilidad y confiabilidad de los sistemas.

d).- Implementar una respuesta a delitos que sea adecuada y rápida.

e).- Criminalizar y castigar amenazas, balancear intereses policiales con derechos fundamentales (privacidad).

Por lo que respecta a las Definiciones Comunes (una sola para todos los países) tenemos que:

I.- Sistema computadora: cualquier aparato o conexión de aparatos que, de acuerdo con un programa, ejecuta un proceso automático de datos.

II.- Dato de computadora: cualquier representación de hechos, infracción o conceptos en una forma que puede ser procesada.

III.- Datos de suscriptor: cualquier información retenida por un servidor (ISP) necesario para identificar y determinar la dirección e identidad de un usuario/cliente.

IV.- Cualquier información: lo asociado con tal usuario o cliente retenido por el servidor (ISP) para identificar el lugar de un sistema.

En cuanto a la legislación que se propone crear a nivel internacional están: leyes sustantivas, en las cuales se habrá de definir a los actos contra la integridad, disponibilidad y confidencialidad de sistemas, acceso ilegal, interceptación ilegal, daño al sistema, daño a datos (virus), aparatos ilegales (con el fin de causar daños).

Actos Contra la Integridad, Disponibilidad y Confidencialidad de Sistemas.

- Se propone penalizar el acceso ilegal, sin autorización y con mala intención, invadir medidas de seguridad o para obtener datos del sistema (mediante un ataque).
- Protección de Integridad y Confidencialidad.
- Penalizar la intercepción ilegal, sin autorización y con mala intención.
- Usar maneras técnicas para cometer ilícitos.
- Interceptar las transmisiones de datos de cualquier sistema.
- Penalizar el daño a datos: sin autoridad.
- Penalizar el daño al sistema: sin autoridad y con mala intención; impide la normal función de un sistema, transmitiendo programas que añadan, perjudiquen, anulen o supriman datos de un sistema.
- Penalizar los aparatos ilegales: crear, proveer, vender, usar y distribuir, con el fin de realizar algún daño.

- Penalizar el fraude; es una persona con intención de causar pérdida u obtener un beneficio sin derecho, por medio de cualquier entrada, alteración o supresión de datos de un sistema. Puede ser cualquier interferencia con el normal funcionamiento de un sistema.
- Penalizar la falsificación; quien crea, altera o extingue datos de un sistema, resultando en la creación de datos falsos con la intención de que sean considerados o aceptados como legalmente auténticos.

En lo concerniente a las ofensas relacionadas con derechos de autor tenemos que se hace la recomendación de penalizar el uso de un sistema para la reproducción y distribución de obras protegidas por las leyes de derecho de autor.

Esta última recomendación es importante pues es parte fundamental de nuestra propuesta, la diferencia es que sólo se limita a penalizar "el uso de un sistema para la producción y distribución de obras protegidas por las leyes de derecho de autor", sin mencionar a los responsables de la creación de estos sistemas o equipos, así como del software que se ocupa ya sea como complemento o base de esta conducta, aunque por comentarios del Dr. Rodolfo Orjales, desde el punto de vista filosófico sí se puede castigar a estos sujetos ya sean personas físicas o morales, aunque no este tipificada la conducta como tal; por otro lado señala que Alemania no considera aún a estos sujetos como responsables de algún delito, pues ellos creen –y es razonable pero hasta cierto punto– que es responsabilidad total del gobierno proteger los derechos del pueblo en general.

Ahora bien, a nivel mundial tenemos que se pide la tipificación de esta conducta si cubre los siguientes requisitos: que sea cometido a nivel comercial y si es así entonces se castigará. Estados Unidos, para el efecto, señala que para ser delito deben de ser más de diez copias en un periodo de 180 días y cuyo valor es o sea mayor de 2,500 dólares y en software un valor de 500 dólares. Como podemos ver Estados Unidos, independientemente de las acciones que pudieran tomar las demás naciones, optó por regular la piratería conforme a su experiencia, y en la mayor parte es buena desde mi punto de vista pues, al regular al máximo de copias a nueve ata a los piratas de manos, pues tendría que ocuparse un sinnúmero de gente para no violentar esta disposición legal, y por si fuera poco, hay todavía niveles económicos que se deben de respetar.

Por ende, la tecnología y el delincuente pueden actuar a cualquier hora y tiempo, es casi imposible su identificación dentro de este tipo de acciones, pero la autoridad no necesita permisos, así como los jueces, fiscales, etc.[239]

En cuanto a las leyes procesales, también se recomienda a los países que deben permitir a sus autoridades: realizar una investigación dentro de los sistemas de su país para recolectar y conducir investigaciones de delitos en cualquier tiempo, es decir, tener a la mano un expediente o base de datos con informes precisos y actuales para poder llevar a cabo las investigaciones de una forma pronta y expedita; se recomienda también a los países que permitan a sus autoridades realizar la búsqueda y colecta

[239] Respecto a este comentario y en particular al que señala "la autoridad no necesita permisos", es importante señalar que es comentario exclusivo del Dr. Rodolfo Orjales, quizás lo señalo así por las características de su procedimiento de investigación, así como las facultades que tienen sus autoridades tanto policiales como judiciales para investigar y castigar las conductas ilícitas. Particularmente considero que se están violentado las garantías de los presuntos delincuentes con este tipo de investigación, pero no profundicemos en este tema y sigamos adelante.

de datos en otros países y dentro del propio. Respecto a esta última recomendación, considero que esta es parte de los "pequeños problemas" que tiene el poder regular a nivel internacional estos delitos, pues se daña la soberanía de los países y, consecuentemente, la mayoría no está dispuesta aún a dejar que otro país la violente y mucho menos Estados Unidos.

Sin embargo proponen la manera de colectar datos, mediante las siguientes sugerencias:

- Hacer y retener una copia de datos (para probanza válida y plena, que la policía entre a una computadora y haga una copia que sea considerara como evidencial.
- Mantener en custodia el sistema mediante cuerpos de policía, que resguarden el equipo del delito, así como rendir y/o bloquear el sistema (la policía puede actuar como mejor le parezca, es decir, apagar la computadora, investigar dentro de sus ejecutivos, etc.).

Estas dos anteriores propuestas son válidas –en lo que respecta a la materia local– siempre y cuando no las quieran aplicar a otros países unilateralmente, pues como ya mencionamos anteriormente, los demás no dejarán tan fácilmente que llegue otro país, y particularmente Estados Unidos a organizar su forma de investigar por muchos convenios, acuerdos o tratados internacionales que hayan firmado, no lo harán tan fácilmente.

Respecto del texto anterior, también se menciona a la jurisdicción señalando que los países deben establecer jurisdicción cuando un delito cibernético es cometido:

- Dentro de su territorio o de un barco o avión bajo su bandera.
- Por uno de sus ciudadanos, si este delito es cometido dentro de su país o fuera de éste.

Dentro del rubro de la a cooperación internacional, tenemos que también hubo recomendaciones; las más importantes son las siguientes:

Extradiciones:

- Incluir las ofensas cibernéticas en los tratados.
- Si no se realiza la extradición, por ejemplo: un delito cometido en México o que ocurrió en México con efectos en un país extranjero, iniciar un juicio dentro del país del delincuente por dicho delito.

Asistencia Mutua:

En circunstancias de emergencia, la rápida actuación de ambas partes es importante para lograr buenos resultados; así pues se recomienda:

- Aceptar y responder inmediatamente al llamado de ayuda de otro país y dejar para posteriores acciones la confirmación formal, y ordenar al gobierno o compañía la preservación de la información que servirá como prueba dentro un proceso.

Cada país debe previamente:
- Identificar a la autoridad responsable.

- Las autoridades deben mantenerse en contacto.
- Compartir teléfonos y direcciones del personal propio que está a cargo de estas áreas.

Para realizar una petición para preservación de datos, un país debe identificar:

- La autoridad que hace la demanda, el delito y los acontecimientos.
- La información que se busca y no toda la información de un sitio.
- En caso de que sea necesario preservar la información, debe expresar, decir el por qué, de esta preservación.

Al realizar el trámite anterior se pierde tempo vital para poder actuar contra algún delito que se realizó dentro de algún país con efectos en otro, por esto se hace la recomendación anterior; así mientras la autoridad actúa por un lado administrativamente, por otro se puede inclusive identificar a los responsables del ilícito y hasta llegar a su detención.

Por último, nos permitimos citar a Jerome Roaché, quien justifica la creación de nuevos tipos penales al considerar que "mientras algunos de estos estatutos son deficientes en diversas áreas, sus diseños muestran al menos el reconocimiento del crimen informático y el intento de combatirlo. Deberán legislarse ordenamientos más efectivos y fuertes para impedir esta actividad. Aunque tome tiempo desarrollar ordenamientos que se adecuen a este problema, es mejor tener ordenamientos que traten el problema a no tener ninguno".[240]

[240] CONTRERAS SALDIVAR, Gabriel. *Op. Cit.*, pág.45.

Alemania

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

Código penal. Sección 202ª. Espionaje informático.

A cualquier persona que obtenga sin autorización, para sí o para otro, información que no esté destinada para él y que esté protegida contra accesos no autorizados, se le impondrá prisión por un término que no exceda de tres años o multa.

- Espionaje de datos (202ª).
- Estafa Informática (263ª).
- Falsificación de datos probatorios (269), junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de comentos falsos (270, 271, 273).

Sección 303a. Alteración de datos. Es ilícito cancelar, inutilizar o alterar datos; inclusive la tentativa es punible:

A cualquier persona que ilícitamente borre, suprima o altere información (la que se refiere en la sección 202ª) se le impondrá prisión por un término no mayor de dos años o multa.

Sección 303b. Sabotaje informático. Destrucción de elaboración de datos de especial significado por medio

de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa:

Se impondrá prisión que no exceda de dos años o multa a cualquier persona que interfiera con el procesamiento de datos que sea de esencial importancia para otro negocio, empresa o autoridad administrativa mediante:

1.- La comisión de un delito previsto en la Sección 300(1), o

2.- La destrucción, daño, remoción o alteración de un sistema informático o portador de información.[241]

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 terror y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la 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, a través de una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los Países Escandinavos y en Austria. En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a

[241] *Ibidem*, pp.41-42.

tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

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

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

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas. En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate de daño a sistemas informáticos. El tipo

de daños protege corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

Como podemos ver, Alemania ha recurrido a la regulación de ciertas conductas, quizás las que más se han presentado en este tiempo, pero también podemos ver que no tipifica la conducta de los sujetos, ya sean personas físicas o morales, –productores– que crean o inventan y en consecuencia sacan al mercado software y hardware también, como armas o medios potenciales para cometer un ilícito. Un elemento importante que refuerza a nuestra afirmación es que Alemania señala y considera que el Gobierno tiene la obligación de proteger los derechos de ellos, terceras personas y consecuentemente la estabilidad económica, social y política del país y no tiene ninguna obligación de realizar esto, la iniciativa privada principalmente.[242] Pero como ya mencioné anteriormente, no se trata de quitarle obligaciones al Estado o gobierno, sino de mantener por cualquier medio la seguridad jurídica, la estabilidad económica y social, el bien común en sentido general y si es necesario –que desde mi punto de vista lo es– que se regule y participe a la vez la iniciativa privada, llámese persona física o moral, sin articular objeción alguna.

Argentina

Hago particular mención de este país porque es uno más –Latinoaméricano en especial– que ha tomado la decisión de regular y tipificar los delitos informáticos como tales, un claro ejemplo de esto es la siguiente reforma que llevo a cabo Argentina –esta reforma se realiza a la vieja Ley

[242] ORJALES, Rodolfo. *Op. Cit.*

11.723 de Propiedad Científica, Literaria y Artística– que hemos de analizar, la cual se denomina SOFTWARE: REFORMA A LA LEY DE PROPIEDAD INTELECTUAL. A. LEY 25.036. PROTECCIÓN PENAL DEL SOFTWARE,[243]

Así pues, tenemos que Argentina tomó la decisión de llevar a cabo esta reforma en el mes de noviembre del año de 1998, modificando el art.1° de la ley 11.723, incorpora el inciso d) al art.4° de la ley 11.723, incorpora un segundo párrafo al art.9° de la ley 11.723, incorpora el art.55 bis a la ley 11.723 y se incorpora como art.57° in fine de la ley 11.723;[244] para su mejor comprensión se ha realizado un cuadro comparativo entre los textos anteriores a la reforma y los que se agregaron a ésta:

[243] CUADERNOS DE DOCTRINA Y JURISPRUDENCIA PENAL. *Software: Reforma a la Ley de Propiedad Intelectual. A. LEY 25.036. PROTECCIÓN PENAL DEL SOFTWARE.* Año, 5, número 8 C, ADHOC-Buenos Aires, 1998, pág. 631.

[244] *Ibidem*, pp. 631-632.

TEXTO ANTERIOR	TEXTO VIGENTE
Articulo 1°: A los efectos de la presente ley, las obras científicas, literarias y artísticas, comprenden los escritos de toda naturaleza y extensión; las obras dramáticas, composiciones musicales, dramático-musicales; las cinematográficas, coreográficas y pantomímicas; las obras de dibujo, pintura, escultura, arquitectura; modelos y obras de arte o ciencia aplicadas al comercio o a la industria los impresos, planos y mapas; los plásticos, fotografías, grabados y fonogramas; en fin, toda producción científica, sea cual fuere el procedimiento de reproducción.	Artículo 1°: A los efectos de la presente ley, las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, *entre ellos los programas de computación fuente y objeto: las compilaciones de datos o de otros materiales;* las obras dramáticas, composiciones musicales, dramático-musicales; las cinematográficas, coreográficas y pantomímicas; las obras de dibujo, pintura, escultura, arquitectura; modelos y obras de arte o ciencias aplicadas al comercio o a la industria; los impresos, planos y mapas; los plásticos, fonografías, grabados y fonogramas; en fin, toda producción científica, literaria, artística o didáctica, sea cual fuere el procedimiento de reproducción. *La protección del derecho de autor abarcará la*

	expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos pero no esas ideas, procedimientos, métodos y conceptos en sí.
Art. 4°: Son titulares del derecho de propiedad intelectual: a) El autor de la obra; b) Sus herederos o derechohabientes; c) Los que con permiso del autor la traducen, refunden, adaptan, modifican o transportan sobre la nueva obra intelectual resultante;	Art. 4°: Son titulares del derecho de propiedad intelectual: a) El autor de la obra; b) Sus herederos o derechohabientes; c) Los que con permiso del autor la traducen, refunden, adaptan, modifican o transportan sobre la nueva obra intelectual resultante; *d) Las personas físicas o jurídicas cuyos dependientes contratados para elaborar un programa de computación hubiesen producido un programa de computación en el desempeño de sus funciones laborales, salvo estipulación en contrario.*
Art. 9°: Nadie tiene derecho a publicar, sin permiso de los auto-	Art. 9°: Nadie tiene derecho a publicar, sin permiso de los

res o de sus derechoahabientes, una producción científica, literaria, artística o musical que se haya anotado o copiado durante su lectura, ejecución o exposición pública o privada.	autores o de sus derechohabientes, una producción científica, literaria, artística o musical que se haya anotado o copiado durante su lectura, ejecución o exposición pública o privada. *Quien haya recibido de los autores o de sus derechohabientes de un programa de computación una licencia para usarlo, podrá reproducir una única copia de salvaguarda de los ejemplares originales del mismo. Dicha copia deberá estar debidamente identificada , con indicación del licenciado que realizó la copia y la fecha de la misma. La copia de salvaguarda no podrá ser utilizada para otra finalidad que la de reemplazar el ejemplar original del programa de computación licenciado si ese original se pierde o deviene inútil para su utilización.*

	Articulo 55 bis: La explotación de la propiedad intelectual sobre los programas de computación incluirá entre otras formas los contratos de licencia para su uso o reproducción.
Art. 57: En el Registro Nacional de Propiedad Intelectual deberá depositar el editor de las obras comprendidas en el art.1° tres ejemplares completos de toda obra publicada, dentro de los tres meses siguientes a su aparición. Si la edición fuera de lujo o no excediera de 10 ejemplares, bastará con depositar un ejemplar. El mismo término y condiciones regirán para las obras impresas en país extranjero, que tuvieren editor en la República y se contará desde el primer día de proponerse en	Art. 57: En el Registro Nacional de Propiedad Intelectual deberá depositar el editor de las obras comprendidas en el art.1° tres ejemplares completos de toda obra publicada, dentro de los tres meses siguientes a su aparición. Si la edición fuera de lujo o no excediera de 10 ejemplares, bastará con depositar un ejemplar. El mismo término y condiciones regirán para las obras impresas en país extranjero, que tuvieren editor en la República y se contará desde el primer día de proponerse en

venta en territorio argentino. Para las pinturas, arquitecturas, esculturas, etcétera, consistirá en deposito de un croquis o fotografía del original, con las indicaciones suplementarias que permitan identificarlas. Para las películas cinematográficas, el depósito consistirá en una relación del argumento, diálogos, fotografías y escenarios de sus principales escenas.	venta en territorio argentino. Para las pinturas, arquitecturas, esculturas, etcétera, consistirá en deposito de un croquis o fotografía del original, con las indicaciones suplementarias que permitan identificarlas. Para las películas cinematográficas, el depósito consistirá en una relación del argumento, diálogos, fotografías y escenarios de sus principales escenas. Para los programas de computación consistirá el deposito de los elementos y documentos que determine la reglamentación.

Recientemente, nos encontramos con la producción de una novedad de importancia, la Ley 25.036, cuyo comentario no podía soslayarse. En efecto, habida cuenta del grado de oscuridad y discusión que enmarcaba el tema. [...] pero es oportuno recordar que habíamos concluido que en lo que toca concretamente al software, su protección desde el punto de vista penal sólo podría viabilizarse la normatividad vigente propiciando su incorporación por medio de la ley que específicamente adecue el texto vigente [...].[245]

Con la sanción de la Ley 5.036, como hemos indicado en el título de este comentario, se cierra en modo definitivo y por la afirmativa la discusión respecto de si en nuestro derecho el software tiene protección penal. La directriz de política criminal que malamente se quiso imponer [...], es reafirmada y concretada técnicamente en modo adecuado con el nuevo texto legal. Ello no quiere decir que la ley ahora sancionada no fuere perfectible o que carece de toda objeción, sino simplemente que al modificarse la Ley 11.723 por la ley 25.036, se introduce la protección penal del software en modo respetuoso de las exigencias del principio de legalidad. [...] en materia de responsabilidad penal importa como condición esencial la existencia de una regla jurídica que formule la descripción del hecho criminal y de la pena que se le imputa al autor, que debe ser previa temporalmente al hecho que se califica por ella como criminal, único modo en que se garantiza la certidumbre de su contenido y su difusión para el acabado conocimiento y compresión de éste por todos los habitantes. Sólo ahora, ante la claridad que a la cuestión provee la reforma de la Ley de Propiedad Intelectual, puede considerarse satisfecho el principio de legalidad, lo que sin duda no sucedía

[245] MARCELO A. Riquert. *Ley 25.036: Análisis de sus cláusulas sobre protección penal del software.* Cuadernos de Doctrina y Jurisprudencia Penal. *Op. Cit.*, pág.638.

por vía de la interpretación que pretendía sortear el "bache punitivo" [...].[246]

Así ya sin ninguna duda, puede afirmarse que aquellas conductas descritas en los art. 71 y ss. de la Ley de Propiedad Intelectual, realizadas respecto de "...los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales..." y desplegadas a partir del mes de noviembre de 1998, configuran delitos para el Derecho Penal Nacional. Se ha concretado entonces un supuesto de nueva incriminación [...].[247]

[...] algunas de las previsiones no penales son de particular interés al momento de ponderar la posible tipicidad de una conducta. Así, deben destacarse los nuevos párrafos segundo y tercero del art.9°, que si bien consagran el principio de que a una máquina le corresponde una licencia (1 máquina = 1 licencia), lo que desde la perspectiva del usuario empresario importa un costo que es ciertamente significativo, han solucionado en adecuado modo la cuestión de la famosa "copia de resguardo" o "copia de respaldo",[248] cuya atipicidad era resistida por algunos sectores.[249]

Quienes se manifiestan contrarios a este tipo de previsiones suelen argumentar que se favorece la actividad de copiado y se afecta el derecho del titular de propiedad intelectual, que esta actividad "hormiga" individualmente considerada no parece importante pero que por su extensión, si se le considera en conjunto, adquiere un vo-

---

[246] *Ibidem*, pp.639-640.

[247] *Ibidem*, pág.640.

[248] La consagración de la "copia de salvaguarda", es acorde a la directiva 250 del 14 de mayo de 1991 del Consejo de las Comunidades Europeas, cuyo art.5.2. dice "La realización de una copia de salvaguarda por parte de una persona con derecho a utilizar el programa no podrá impedirse por contrato en tanto en cuanto resulte necesaria para dicha utilización [...].

[249] *Ibidem*, pp.650-651.

lumen no despreciable. Si se actualizan u discriminan algunos de los datos que ya hemos ido destacando con anterioridad, surge con mayor claridad que la previsión comentada ha sido una decisión correcta. Price-Waterhouse ha indicado que conforme el revelamiento de datos correspondientes a 1997 en nuestro país, el mercado de software legal llegó a unos 559 millones de dólares, estimándose en términos ideales que las pérdidas del sector habrían sido unos 1.300 millones de la misma moneda. La cifra inicial puede descomponerse del siguiente modo: 267 millones fueron adquiridos por grandes empresas, 261 por medianas y pequeñas empresas, mientras que el consumo hogareño fue de sólo 31 millones. En el primer sector se estima que se cuenta con alrededor de un 70 a 80% de software legal, que baja a un 40 a 50 % en el segundo sector y es prácticamente nulo en el tercero. Es evidente que por volumen, necesidad, capacidad adquisitiva y rentabilidad, entre otros factores, son los dos primeros sectores los que tienen verdadero interés en el desarrollo de la industria del Software. Correlativamente, sólo respecto de ellos tiene algún sentido la protección penal, porque son los clientes naturales a gran escala del pirata del software. Incluso, debe tenerse siempre presente que es a este último a quien está dirigida la actuación punitiva: no hay penas para quien compra software ilegal, sino para quien lo edite, venda o reproduzca ilegalmente.[250]

Respecto al anterior texto, es importante señalar que en nuestro país sí están tipificadas es tas conductas y por lo tanto tienen una pena, pero por otro lado podemos constatar una vez más que al legislar sobre el tema, el legislador se olvida o no considera importante el regular la conducta del fabricante o creador de programas como su-

[250] *Ibidem*, pp.651-652.

jeto de obligaciones y responsabilidades ante la autoridad como creador tanto de programas o software que sirven para realizar copias ilegales como de diseñar, inventar o armar equipos o hardware especiales como complemento de estos programas, pues al ser "independientes" uno de otro, también es cierto que esta independencia es sólo exterior pues interiormente, es decir a nivel procesador o computadora personal, no pueden "vivir" por separado éstos si no existe uno u otro.

Por otra parte [...] la doctrina ha hecho notar la falta de una adecuada compensación al inventor, máxime cuando la explotación produce beneficios muy superiores a la renumeración del trabajador.[251] Lo anterior lo podemos comprobar con lo que ya habíamos señalado previamente, pues esta puede ser una forma de disminuir tanto la creación de programas dañinos -virus- como la creación o invento de programas o software y hardware con fines de realizar copias ilegales u otro tipo de conductas indebidas, pues se estimularía a estos con una buena paga y por ende no tratarían de hacer algún daño sino al contrario protegerían al máximo tanto su trabajo como su empresa.

Podemos concluir que este país tomó la decisión de tipificar en concreto las conductas más comunes dentro de los llamados delitos informáticos y particularmente desprendiéndose de lo anteriormente analizado a la protección del software por la vía penal, esto quiere decir, a mi parecer, que es actualmente un área hacia lo que se han dirigido los esfuerzos de la mayoría de los países, con el fin de poder detener estas conductas ilícitas tanto nacional como internacionalmente; es así también como tenemos una fuente y base más para nuestra propuesta ya mencionada anteriormente.

---

[251] *Ibidem*, pág.653.

México

Se ha llegado a considerar que figuras tales como el robo, fraude, abuso de confianza o los llamados secretos comerciales (figura americana) y secretos de fabricación (figura europea), se presentan como medios de solución frente al problema; sin embargo, dichas instancias parecen no estar integradas por elementos tales que permitan atribuir una cabal asimilación.

Así por ejemplo, en el robo se requiere del apoderamiento físico de una cosa mueble, la cual, en los términos de la información como un "algo" indiscutiblemente intangible o inmaterial, no configura de manera convincente el supuesto. Por otra parte, en el abuso de confianza se requiere de la disposición de una cosa ajena mueble, lo cual representa igualmente problemas a nivel de la carga de la prueba. En el fraude se requiere un engaño o aprovechamiento de un error que permita hacerse de manera ilícita de alguna cosa (no se especifica de qué tipo) o alcanzar un lucro indebido, lo cual, si bien pudiera ser aplicable a final de cuentas, por su misma abstracción frente al problema, ofrece serias inconveniencias en la práctica.

Ahora bien, por cuanto concierne a los secretos comerciales y de fabricación (si bien no utilizados en nuestro país), en ellos se implica una divulgación intencional (o aun fortuita) de alguna información, en este caso referida o contenida en un programa de cómputo; dichas figuras, si bien apropiadas en apariencia (sobre todo porque son castigadas penalmente), revisten asimismo dificultades a nivel probatorio en cuanto al apoderamiento y difusión de la información.

Entrando al estudio de nuestra área y como un caso especial que existe en nuestro país haremos referencia al Estado de Sinaloa, el cual es el único Estado de la República que ha tipificado penalmente el delito informático como tal,

ubicándolo dentro del Código Penal y de Procedimientos Penales para el Estado de Sinaloa, en el Título Décimo. Delitos contra el patrimonio. Capítulo quinto. Delitos Informáticos, artículo 217, en el que se describe como sigue: Comete delito informático, la persona que dolosamente y sin derecho:

I.- Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o

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

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.[252]

Como podemos ver, primeramente se ubica el tipo dentro de aquellos que son cometidos en contra del patrimonio, pues es donde estos delitos regular y generalmente causan perjuicio, y en segundo caso sólo se señala a las conductas de aquellos sujetos que utilicen a las computadoras como medio o fin del delito, así como otras características más, pero es el caso que en particular que dejan una vez más no se considera y por ende no se regula la conducta del fabricante, ya sea persona física o moral.

Consideramos que se ubica al delito informático bajo esta clasificación dada la naturaleza de los derechos

[252] *Código Penal y de Procedimientos Penales para el Estado de Sinaloa*, Porrúa, tercera edición, 1997, pág.68.

que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad.

Resulta ilimitada la cantidad de conductas que pueden considerarse como delitos informáticos, de tal suerte que sólo analizaremos aquellas conductas que se han considerado como las más representativas de este "genero". Para este efecto seguiremos el orden previsto por el Manual de las Naciones Unidas sobre la Prevención y Control de Crimen Relacionado con Computadoras,[253] es decir:

- Fraude Informático.
- Falsificación Informática.
- Daños o modificaciones a datos computarizados o a programas informáticos.
- Acceso no autorizado a sistemas informáticos y servicios.
- Reproducción no autorizada de programas protegidos legalmente.

Fraude Informático

Siguiendo la definición del Consejo de Europa, este delito consiste en "el ingreso, alteración o supresión de datos computarizados o programas informáticos, o cualquier otra interferencia durante le procesamiento de datos, que provoque como resultado pérdidas económicas o de posesiones de otras persona, con el propósito de obtener una ganancia económica ilícita para sí o para otra persona.[254]

[253] Ver *Supra*, pág.73.
[254] CONTRERAS SALDIVAR, Gabriel. *Op. Cit.*, pág. 47

Como elemento distintivo de este tipo de fraude, Ma. De la Luz Lima señala que "han aumentado los fraudes utilizando el llamado dinero electrónico, que es el dinero representado en signos electrónicos o patrones magnéticos, como las tarjetas de crédito (dinero de plástico); el cual es almacenado y procesado en computadoras y transmitido a través de líneas telefónicas.[255]

Se trata de una conducta directamente relacionada con la manipulación de los datos almacenados en una computadora, que provoca transferencias de fondos o de otros valores. Para numerosos analistas, en el empleo de los medios informáticos en la planeación y ejecución de delitos de fraude financiero en el espacio binario, el engaño se hace a la máquina.

En este sentido Arteaga Sánchez, refiriéndose a la legislación venezolana, que por su contenido es aplicable a nuestra legislación, señala que "ciertamente nuestra figura delictiva de estafa, a la letra, parecería excluir el engaño a la máquina y su consiguiente error que motiva la disposición perjudicial. Nuestro Código, inspirado en legislaciones que no se plantearon los retos de la revolución, sólo pensó en la estafa y el engaño de hombre a hombre.[256]

Frente a este planteamiento del que dimana la atipicidad del llamado fraude informático, algunos autores norteamericanos consideran que la introducción de datos falsos en una computadora equivale el engaño sobre un ser humano. Nimmer señala que "conforme al uso actual de los sistemas computarizados, encargados de ejecutar transacciones directamente, esta equiparación (engaño a un ser humano y engaño a una máquina) es necesaria y conceptualmente justificada para asegurar la represión pe-

[255] *Idem.*
[256] *Ibidem*, pág. 48.

nal del fraude moderno. No hay diferencia ni de facto ni legal, entre engaño utilizado para apoderarse de propiedad ajena a través de una máquina y aquél dirigido a la persona con idéntica intención.[257]Este argumento cuenta con detractores en la propia literatura norteamericana, pero como señala Gutiérrez Francés , tratándose de un sistema de "common law", al estar respaldado por una importante línea jurisprudencial, su peso específico es notable, lo cual se propicia en algunos Estados por la propia ley: así el estatuto de Alaska establece expresamente que cuando la ley exija la presencia del elemento engaño (deception), no servirá como defensa que el demandado haya engañado, o intentado engañar, una máquina, incluido el ordenador.

Siguiendo estas posturas, el engaño se realiza directamente sobre la máquina, por lo que esta conducta no encuadraría en el tipo penal de fraude, toda vez que éste requiere que el sujeto pasivo sea engañado o se encuentre bajo error, de conformidad con le artículo 386 del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal:

"Artículo 386.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que estese halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido".[258]

Así pues, consideramos que el pago de una suma de dinero, producto de una transferencia ilícita de fondos por medio de equipos computacionales, encuadraría en el tipo penal del fraude genérico, pues esta conducta implicaría un engaño al titular del sistema, que es el titular del

[257] *Idem.*

[258] *Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la República en Materia de Fuero Federal.* Sista, 2000, pág.123.

bien jurídico protegido. Es decir, el pago se efectuaría en virtud del engaño que se ha hecho al titular del sistema, pues de conocer éste la naturaleza ilícita de la transferencia, no habría realizado el pago.

Consecuentemente, al crear el tipo penal de Fraude Informático se agotaría el tipo penal de fraude previsto por el artículo 386 del Código Penal.

El único elemento distintivo del fraude informático en relación con el fraude genérico previsto por nuestra legislación, es el medio comisivo. En palabras del Dr. Miguel del Castillo "cuando se utiliza una máquina para perjudicar a otro, el punto es que no son las máquinas las que pueden incurrir en error, sino que son las personas. A las máquinas simplemente se le han dado instrucciones para que entreguen dinero o para que se acredite en la cuenta de otro... estamos ante una maniobra que, de alguna manera, puede inducirnos a engañar a otro".[259]

Falsificación Informática

Para el Consejo de Europa, este delito consiste en "el ingreso, alteración o supresión de datos computarizados o de programas informáticos, o cualquier otra interferencia durante el procesamiento de datos, realizada de tal forma o bajo condiciones tales que constituyan un delito de falsificación, cuando sea cometido respecto de un objeto tradicional de tal delito".[260]

El Manual de las Naciones Unidas sobre la Prevención y Control del Crimen Relacionado con Computadoras le da a este "delito" un concepto más amplio, pues admite dos vertientes: la primera, cuando los datos son al-

[259] CONTRERAS SALDIVAR, Gabriel. *Op. Cit.*, pág. 52.
[260] *Ibidem*, pág.53.

terados respecto de documentos almacenados en la computadora, y la segunda, la utilización de los sistemas informáticos como instrumentos para la comisión del delito de falsificación.[261]

Por lo que hace al primer supuesto de la comisión de este delito informático, consistente en la alteración de documentos almacenados en la computadora, este acto sólo será sancionable si forma parte de los actos que den como resultado la falsificación de un documento (escrito), no el acto de alteración como tal (salvo en el caso de tentativa).[262]

Respecto del segundo supuesto, consistente en la utilización de sistemas informáticos como instrumento para la comisión del delito de falsificación, la conducta queda cubierta por el tipo penal existente, que no hace distinción respecto de los medios comisivos, por lo que no se considera necesaria la creación de una nueva figura típica que le otorgue un tratamiento especial.[263] Es claro que el único elemento distintivo respecto del delito de falsificación es el uso de la computadora como medio comisivo, por lo que ya se encuentra previsto por nuestra legislación en el Título Decimotercero del Libro II del Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la República en Materia de Fuero Federal, ya que los tipos penales de falsificación no requieren de un medio especifico de comisión.[264]

Daño o Modificaciones a datos computarizados o a Programas Informáticos.

Son materia de este apartado sólo aquellas conductas que ataquen directamente al software, que constituye la estructura lógica que permite a la computadora la

---

[261] *Idem.*
[262] *Ibidem*, pág.58.
[263] *Idem.*
[264] *Ibidem*, pág.54.

ejecución del trabajo que se ha de realizar, es decir, el equipo lógico informático –caben dentro de este los códigos fuente y objeto, vistos y definidos anteriormente-.

Siguiendo la lista de los delitos informáticos emitida por el Consejo de Europa, caben aquí dos tipos de conductas:

- Daños a datos computarizados o a programas informáticos. El daño, deterioro o supresión de datos computarizados o programas informáticos sin derecho a hacerlo.
- Sabotaje Informático. El ingreso, alteración o supresión de datos computarizados o programas informáticos, o cualquier otra interferencia en los sistemas informáticos con la intención de impedir el funcionamiento del sistema o de telecomunicaciones.[265]

Como es sabido, estas dos conductas pueden traer consigo grandes pérdidas económicas e incluso humanas; piénsese, por ejemplo, en la provocación de la destrucción del soporte lógico de la base de datos de la compañía competidora o de la torre de control de un aeropuerto.

Un criterio delimitador para el análisis de estas conductas es el bien jurídico protegido. Nos referimos en principio al daño, alteración o supresión de datos computarizados o a programas informáticos, independientemente de la forma en que se presenten estas conductas; lo cierto es que están orientadas a variar el estado en que se encuentra el soporte lógico, lo que podría considerase como daño.

[265] *Ibidem*, pág.60.

Algunos autores como Gustavo Arocena o Alberto Arteaga Sánchez sostienen que este tipo de conductas pueden encuadrarse dentro del tipo de daños; sin embargo, otros autores como Otto Banho Licks y Joao Marcello de Araujo Jr., consideran un error el querer dar a este tipo de conductas el mismo tratamiento que a aquellas dirigidas a los bienes tangibles. "El inconveniente de muchas legislaciones que han aparecido consiste en el hecho de tratar a estas nuevas conductas pertenecientes al medio tecnológico de procesamiento digital de datos y a la computarización de la sociedad, con los mismos principios penales legales aplicables a delitos de bienes tangibles o corporales... la cuestión principal de las leyes penales informáticas respecto de los sistemas informáticos y de comunicaciones es fundamentalmente la necesidad de proteger sus componentes inmateriales o intangibles, es decir, el software y los datos, que aún carecen de la misma protección que tiene el otro componente, el hardware.[266]

Y posteriormente a aquellas conductas efectuadas con el propósito de impedir el funcionamiento de sistemas de telecomunicaciones (sabotaje). La destrucción o deterioro exigidos por el tipo del Código Penal, así como el daño, perjuicio o destrucción exigidos por el tipo de la Ley de Vías Generales de Comunicación, no exige un medio comisivo específico por lo que la realización de tales conductas, por medios informáticos, así como por cualquier otro medio será punible de conformidad con los artículos 167 del Código Penal, Título Quinto "Delitos en Materia de Vías de Comunicación y de Correspondencia", artículo 533 Ley de Vías Generales de Comunicación, el artículo 4 de la Ley Federal de Telecomunicaciones, artículo 3, fracción VIII, XIII de la misma ley.[267]

---

[266] *Ibidem*, pág.62.
[267] *Ibidem*, pág.66.

Acceso no Autorizado a Sistemas Informáticos y Servicios

El deseo de introducirse sin autorización a un sistema informático puede obedecer a diversos motivos, desde la simple curiosidad hasta la comisión de conductas de gran trascendencia como fraude, sabotaje o espionaje. Este tipo de conducta suele ser el primer paso en la comisión de los demás delitos informáticos.

Como señala Gutiérrez Francés: [...] la criminalidad informática comenzó a manifestarse con los llamados computer hackers, quienes hicieron saltar inicialmente la alarmar en materia de seguridad de los sistemas informatizados [...] Asuntos de enorme repercusión, en los que han sido víctimas grandes multinacionales y compañías, el Departamento de Defensa, las Fuerzas Armadas de los Estados Unidos y hasta el propio F.B.I., han servido para poner de relieve que las conductas de intruismo informático (hacking), no sólo conllevan un efecto disruptivo implícito, sino seguridad nacional o internacional, el patrimonio, la intimidad, etc.[268]

Es importante señalar que en virtud del desarrollo de las telecomunicaciones modernas, que utilizan cada vez más sistemas informáticos, son igualmente vulnerables a este tipo de actividades.

Podemos distinguir dentro de este rubro tres distintas conductas:

1.- Acceso no autorizado al sistema informático.
2.- Acceso no autorizado a un servicio (también llamado robo de tiempo).
3.- Sustracción de información.

[268] *Ibidem*, pp.67-68.

1.-Acceso no autorizado al sistema informático

Dentro de esta categoría deben distinguirse además dos situaciones distintas; por un lado, el acceso no autorizado al sistema informático, y por el otro, el acceso no autorizado a determinada información.

Por lo que respecta al acceso no autorizado al sistema informático, éste podría encuadrarse dentro del tipo previsto en el artículo 380 del Código Penal:

Artículo 380.- Al que se le imputare el hecho de haber tomado una cosa ajena sin consentimiento del dueño o legítimo poseedor y acredite haberla tomado con carácter temporal y no para apropiársela o venderla, se le aplicarán de uno a seis meses de prisión o de 30 a 90 días de multa, siempre que justifique no haberse negado a devolverla, si se le requirió a ello. Además, pagará al ofendido, como reparación del daño, el doble del alquiler, arrendamiento o intereses de la cosa usada.[269]

Este tipo penal se conoce por la doctrina como robo de uso o apropiación indebida con carácter temporal y no requiere para su agotamiento el ánimo de apropiación de la cosa, por lo que encuadraría el acceso no autorizado al equipo informático. La conducta, desde este punto de vista, atentaría en contra del bien jurídico señalado como patrimonio.

En relación con el acceso no autorizado a determinada información, podría aplicarse igualmente el artículo 380 del Código Penal si el equipo informático no es propio del que accesa, si no está autorizado para usarlo, o habiendo sido autorizado para ello, su uso vaya más allá del autorizado, pues independientemente de la informa-

[269] *Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la República en Materia de Fuero Federal.* Op. Cit., pág.121.

ción a la que se accese, no es lícito el uso del equipo informático. Sin embargo, cuando el equipo informático es propio del que accesa a la información o éste está autorizado para usarlo, el tratamiento jurídico será otro. No se vulnera ya, en términos de nuestra legislación, al patrimonio, sino a la información, que como tal no está protegida salvo pocas excepciones.[270]

2.-Acceso no autorizado a un servicio

Independientemente de que el equipo informático sea usado con o sin autorización, nos encontramos en el supuesto en que a través del equipo informático se logra la obtención de un servicio informático sin el correspondiente pago.

No nos referimos a las relaciones contractuales que puedan tener lugar a través de los medios informáticos, en cuyo caso podría configurarse el delito de fraude si concurren los elementos previstos por el tipo, sino más bien a aquellas situaciones en las que se logra la prestación de un servicio informático por manipulaciones informáticas, por ejemplo el que prestan los servidores de red, servicios de consulta, de noticias, o acceso a páginas de internet que requieren de un pago.

Consideramos que esta conducta encuadraría en el tipo previsto por la fracción II del artículo 368 del Código Penal.

> I. ...
> II. El aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y sin consentimiento de la per-

[270] CONTRERAS SALDIVAR, Gabriel. *Op. Cit.*, pág.70.

sona que legalmente pueda disponer de los mismos.

III. ...

Consideramos aplicable el comentario de Carrancá y Trujillo y Carrancá y Rivas al señalar que "por no constituir el fluido eléctrico una cosa stricto sensu, ya que carece de corporcidad y sólo existe como propiedad de la materia o estado transferible de la misma, no puede, en rigor, ser objeto material del delito de robo. Pero su aprovechamiento o consumo, al igual que el de cualquier otro fluido aprovechable como satisfactor de un costo económico, está equiparado al robo por la ley penal, a los efectos de la tutela patrimonial correspondiente.[271]

Efectivamente, no puede hablarse en estricto sentido de robo por no reunir las características que el tipo exige: sin embargo, el legislador le otorgó protección al patrimonio de quien provee de ese fluido y que no puede ser sujeto pasivo del robo, por lo que esta figura de delito informático encuentra eficaz protección por parte de nuestras leyes penales, concretamente en el llamando "robo de fluido".[272]

Existe además un tipo protector de las señales de satélite cifradas, previsto en la fracción II del artículo 426 del Código Penal.

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

I. ...

II. A quien realice con fines de lucro cualquier acto con finalidad de descifrar una señal de

[271] *Ibidem*, pág. 74.
[272] *Idem*.

satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.[273]

Aun cuando este artículo se ubica bajo el Título Vigésimosexto "De los delitos en Materia de Derechos de Autor", el bien jurídico protegido por el mismo es el patrimonio del titular de la señal. A diferencia del robo de fluido, además de la especialidad del objeto material de protección (señales de satélite cifradas portadoras de programas), la protección es mucho más amplia, ya que este tipo sanciona cualquier acto con al finalidad de descifrar, no admitiéndose la tentativa.

3.- Sustracción de información

No nos referimos aquí a la sustracción de los medios de almacenamiento o reproducción de la información, como discos, cassettes, o documentos escritos, en cuyo caso podría configurarse el delito de robo. El asunto a tratar en este apartado se limita a determinar si nuestro derecho protege la sustracción de información en sí misma, que puede lograrse por el sólo acceso a una base de datos.

Analizaremos si esta conducta está prevista dentro el tipo penal de robo.

Artículo 367.- Comete el delito de robo: el que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley.[274]

---

[273] *Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la República en Materia de Fuero Federal. Op. Cit.*, 2000, pág.141.
[274] *Ibidem*, pág.117.

En esta misma línea, Arteaga Sánchez señala que "la doctrina penal parece estar de acuerdo en considerar que no puede hablarse de hurto cuando se obtienen datos almacenados en una computadora por no tener éstos el carácter de bien mueble corporal exigido por el delito en cuestión, salvo por lo que respecta a la materialización del dato mismo en un documento o instrumento escrito.[275]

Además de carecer la información almacenada de este requisito de corporiedad, cabe cuestionarse si la misma puede ser objeto de apoderamiento.

El apoderamiento es la aprehensión de la cosa, por la que se entra en su posesión o sea que se ejerce sobre ella un poder de hecho. "El apoderamiento se consuma cuando, además de la simple remoción de la cosa del lugar en que se encontraba... el agente la tiene en su posesión material, por lo cual se requiere además de la posesión del sujeto activo, la desposesión del sujeto pasivo, mediante una remoción o desplazamiento físico".

A este respecto, Gutiérrez Francés opina que "en la sustracción de la información, el apoderamiento puede realizarse con una simple lectura o memorización de datos, de cuya utilización por lo demás no queda excluido el titular". Es por ello que Nimmer considera que en este delito lo que se lesiona es el derecho al secreto de los datos almacenados, el derecho a su exclusivo control, o un hipotético derecho a negar el acceso a terceros fuera de los que él decida.[276]

Por lo que hace al desplazamiento de la esfera de disposición del titular Jerome Roaché señala que "las cortes han interpretado el término propiedad dentro del estatuto (ley) de tal forma que no se incluye a los impulsos

[275] CONTRERAS SALDIVAR, Gabriel. *Op. Cit.*, pág.77.
[276] *Ibidem*, pág.78.

electrónicos en el sistema. El razonamiento es que la información permanece intacta dentro de la computadora, nunca abandona la estructura física de la computadora...[277]

En mi opinión considero, al igual que Gutiérrez Francés, que la sustracción de información puede realizarse por medios muy simples pero esto no quiere decir que no se esté cometiendo algún ilícito aún cuando la conducta no esté debidamente tipificada, pues un ejemplo de esto es violación que se realizó a los sistemas de seguridad de Microsoft cuando uno o varios "hackers" lograron acceso a los servidores centrales de Microsoft, en donde se mantiene el código fuente de varios productos clave, incluyendo el sistema operativo Windows y de la suite de aplicación de Office [...].[278] Como podemos ver hay un daño material al realizarse esta conducta, por lo cual se debe de analizar y posteriormente tipificar, para su mejor comprensión y análisis de estas conductas al momento es que se cometan.

Finalmente es importante mencionar que las conductas antes señaladas (fraude informático, falsificación informática, daños o modificaciones a datos computarizados o a programas informáticos, acceso no autorizado a sistemas informáticos y servicios) ya se habían analizado antes de este capítulo, pero se volvieron a tocar por las características propias de éstos y su relación con el presente capitulo, es decir, la protección del software; por lo anteriormente expuesto y por la necesidad de dar un amplio panorama del los delitos informáticos para hacer un mejor análisis en conjunto de su regulación actual, es por lo que decidí volver a mencionar particularmente estas conductas antes del último tema –reproducción no autorizada de programas protegidos legalmente-; así pues, dada

[277] *Ibidem*, pág.79.
[278] Ver *Infra.*, pág.80.

la anterior explicación, entremos al tema principal de nuestro estudio.

Reproducción no autorizada de programas protegidos legalmente

En lo que respecta a la materia penal federal en nuestro país, tenemos que se encuentran regulados estos delitos y particularmente el que es centro de nuestro estudio; conocido como piratería, en el Código Penal para el Distrito Federal en materia de Fuero Común y para toda la República en Materia de Fuero Federal. Título vigésimo sexto. De los delitos en materia de derechos de autor, artículo 424 y 424-Bis; que señalan:

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

I.- ...

II.- Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos;

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

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

I.- A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas,

videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos...[279]

Por otro lado, tenemos que existen problemas para poder fijar una protección total o mejor dicho una certidumbre jurídica por parte del Estado para con sus gobernados, pues actualmente hay diversas causas que nos dan la razón como las siguientes: no hay una legislación que regule a los delitos informáticos, los cuales en su caso serían delitos contra la informática; hay multiplicidad de conductas, algunas ya tipificadas, que tienen en común equipos de computo; a nivel internacional todavía no está reconocido el tema y, lo más importante, dentro de la regulación en nuestro país es que las reformas al Código Penal Federal realizadas el día 17 de mayo de 1999 no los considera como delitos informáticos.[280]

Por lo que respecta a las políticas o mecanismos de seguridad tanto técnicos, físicos, lógicos y jurídicos, se encuentran dentro de nuestro código en el artículo 211 del Código Penal Federal y subsecuentes. Un punto importante y como mero comentario relativo a la laguna legislativa es la regulación que nos da el artículo 211-bis-1., el cual señala "el que sin autorización modifique, destruya o provoque pérdida de... protegidos por algún mecanismo de seguridad, [...]". Lo anterior lo exponemos sólo para

[279] *Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la República en Materia de Fuero Federal. Op. Cit.*, pág.140.
[280] RIESTRA GAYTAN, Emma. *Op. Cit.*

demostrar una falla importante y consecuentemente, que refuerza mi tesis. Así pues únicamente se castigará si se daña, destruye, modifica, etc., a sistemas o equipos protegidos; esto quiere decir, y así lo entiendo, que aquellos sujetos que no lo estén o no tengan protegidos sus sistemas o equipos, por este simple hecho no encontrarán tácitamente una seguridad jurídica en sus bienes y no serán castigados aquellos que actúen contra estos.

Es por lo anterior que se propone legislar tipos penales entendibles y aplicables a cada caso,[281] pues no se están cubriendo todas las conductas criminólogicas en las últimas reformas penales. Ahora bien por lo que respecta a la protección jurídica del software tenemos que hay tres implicaciones que se deben tomar en cuenta para la determinación de los derechos intelectuales en lo referente a:

1.- El contenido informacional de una base de datos.
2.- La estructura y funcionamiento de un programa de computación.
3.- Determinando al: Código Fuente y al Código Objeto, en cuanto a estos códigos, los cuales ya describimos anteriormente, sólo cabe señalar dentro de este inciso, y afirmar que éstos son el elemento por medio del cual se puede proteger a los programas o software de los actos de piratería, aunque por otro lado está la muesca notarial, la cual va insertada en el código objeto. Se trata de un clip que se activa cuando hay más de tres copias, si esto sucede manda una señal a la autoridad -

[281] Respecto a esta propuesta, es importante señalar que la realiza la Dra. Emma Riestra a mutuo personal y de acuerdo a su experiencia propia.

previamente creada para tal fin-, pero actualmente este sistema, es costoso por lo que veo más viable el proteger los códigos fuente y objeto.[282]

Hay otro punto importante el cual no se debe de ignorar ni pasar por alto, pues es un área donde también se regulan las conductas más usuales y típicas en el área de la informática; este es el Tratado del Libre Comercio con América del Norte (TLC). Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la 6ª parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta, que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.

De esta forma, debe mencionarse que los tres estados parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual, comprendidos en el capítulo específico del tratado.

[282] RIESTRA GAYTAN, Emma. *Op. Cit.*

Debemos de destacar el contenido del párrafo 1 del artículo 1717 titulado "Procedimientos y Sanciones Penales", en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial. Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excederá a tres años a partir de la fecha de la firma del TLC.

En cuanto a los acuerdos firmados por México, tenemos al Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio incluso el Comercio de Mercancías Falsificadas. Al inicializar el contenido de este apartado, debemos aclarar que si bien el GATT se transformó en lo que hoy conocemos como Organización Mundial de Comercio OMC, todos los acuerdos que se suscribieron en el marco del GATT siguen estando vigentes.

En este entendido, cabe mencionar que el Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda de Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT), manteniendo su vigencia hasta nuestros días.

Consideramos que debe destacarse el hecho de que en este acuerdo, en el artículo 10, relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidas como creaciones de carácter intelectual.

Además, en la parte III sobre observancia de los derechos de propiedad intelectual, en la sección I de obligaciones generales, específicamente en el artículo 41, se incluye que los miembros del acuerdo velarán porque en su respectiva legislación nacional se establezcan procedimientos de observancia de los derechos de propiedad intelectual.

Asimismo, en la sección 5, denominada procedimientos penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales, además de que "los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias".

Finalmente, en la parte VII, denominada disposiciones institucionales, disposiciones finales, en el artículo 69 relativo a la cooperación internacional, se establece el intercambio de información y la cooperación entre las autoridades de aduanas, en lo que se refiere al comercio de mercancías de marca de fábrica o de comercio falsificadas y mercancías pirata que lesionen el derecho de autor. Como se observa, el tratamiento que los dos instrumentos internacionales que se han comentado otorgan a las conductas ilícitas relacionadas con las computadoras, es en el marco del derecho de autor.

En este entendido, cabe destacar que el mismo tratamiento que le han conferido esos acuerdos internacionales a las conductas antijurídicas antes mencionadas, es otorgado por la Ley Federal de Derechos de Autor, la cual veremos posteriormente.

Respecto a la rama internacional, es importante señalar que existe un consenso dentro de ésta respecto de la existencia de esta nueva forma de crimen. Así pues, he

de señalar a los países en donde se ha impuesto ésta, y consecuentemente se han adoptado las medidas legislativas para hacer frente a estas conductas ilícitas.

[...] algunos autores se han pronunciado a favor de la creación de nuevas figuras típicas por las ventajas pragmáticas que ello representa, independientemente de la naturaleza jurídica de estas conductas, o si encuadran o no en los tipos penales clásicos. Tal es el caso de Nimmer que distingue, entre otras, las siguientes ventajas:

- Se facilita la labor del intérprete y la aplicación de estos preceptos por los tribunales.
- Ahorran la engorrosa tarea de convencer a los jueces de que la conducta ilícita por medios informáticos puede reconducirse a una cierta figura penal clásica.
- Se gana seguridad jurídica en la medida en que se puede apreciar con facilidad qué conductas integran el fraude informático.[283]

Como lo señalan Banho Licks y De Araujo Jr., "la comunidad internacional se ha dado cuenta durante los ochentas que las leyes penales tradicionales han sido inadecuadas para hacer frente a ciertos tipos de abusos con computadoras. Hemos sido testigos de la aparición, en los llamados países desarrollados, de leyes específicas ante la falta de capacidad de los tipos penales tradicionales.[284]

Sin embargo, las posturas legislativas adoptadas por los diversos Estados que ya cuentan con legislación para hacer frente a estas conductas no han sido uniformes, sino por el contrario han abordado esta problemática des-

[283] CONTRERAS SALDIVAR, Gabriel *Op. Cit.*, pág.38.
[284] *Idem.*

de diversas perspectivas: protección de la integridad de los datos almacenados en la computadora, protección del derecho de uso exclusivo de los datos o información almacenada, protección de la esfera privada, protección del patrimonio, etc.[285]

Como podemos ver, las anteriores posturas se inclinan totalmente a la protección desde el punto de vista de los sujetos que usan a la computadora como medio o fin de la conducta ilícita, pero hasta el momento no se toma en cuenta a los empresarios, ya sean personas físicas o morales, como aquellos sujetos que tienen bastante responsabilidad en cuanto a la proliferación de las conductas en comento.

Siguiendo con el estudio, tenemos que algunos sostienen que basta reformar el Código Penal, ya sea agregando un nuevo título que contemple estas conductas o ubicando las mismas en los distintos títulos del código, en atención a los diversos bienes jurídicos que pretendan tutelarse. Esta ha sido la postura adoptada por países como Canadá, Dinamarca, Finlandia, Francia, Grecia, Italia, Noruega, Países Bajos y Suiza, entre otros.[286]

Dentro de estos países se encuentra también España con las últimas reformas que realizó a su código penal, aunque ellos tienen la política de prevenir antes que castigar al sujeto activo, por lo que podemos ver el grado de peligrosidad que tienen estos delitos para este país, como para que se les haya tipificado penalmente. Por lo que respecta a Estados Unidos, tenemos que también ha tomado medidas para contrarrestar estas conductas ilícitas, tanto interna como externamente en este último rubro no tan

---

[285] *Ibidem*, pág.39.
[286] *Idem*.

amplio principalmente por la falta de cooperación internacional, pero aún así ha logrado grandes avances como lo pudimos constatar anteriormente. Alemania es otro país que ha tomado medidas para regular el problema, aún con los argumentos que ha señalado para regular la iniciativa privada, ya sea persona física o moral, podemos darnos cuenta que ha seguido una sola línea para estos delitos, que a consideración de ellos y de su experiencia han encontrado y a la vez exteriorizado una certidumbre jurídica funcional y protectora de los derechos de sus ciudadanos, aunque para nosotros y nuestro tema de estudio no es suficiente, quizás en estos momentos sí les funcione, pero al poco tiempo verán que ya no es funcional su sistema y entonces se decidan a tomar otras medidas, y en algún momento dado nuestra propuesta.

Otra forma de regular estos delitos es el crear leyes específicas. Tal es el caso de China, Luxemburgo, Portugal, Suecia y Reino Unido, entre otros. Para Gustavo Arocena esta es la mejor opción, ya que "... las características definitorias de la estructura de estos delitos; ...la pluralidad de bienes jurídicos de distinta naturaleza que vulneran estas conductas; la singular característica del sistema informático (compuesto de una parte tangible –hardware- y un elemento lógico o intangible –software), como objeto de determinados delitos; y los particulares caracteres del sujeto activo de la mayoría de estos delitos" justifican la creación de una ley especial complementaria del Código Penal.[287]

En lo que respecta a la creación de estas leyes específicas, considero que es de gran importancia tener si no pronto, sí en un futuro no lejano estas leyes, pues con el

[287] *Ibidem*, pág.40.

avance tecnológico que se está dando a cada momento en el mundo, las conductas que en este momento se han tipificado con otros tipos no tardarán en ser rebasadas por el propio avance tecnológico. Así pues sino se actúa y se creen estas leyes específicas, pronto veremos cómo sujetos diversos cometen actos ilícitos y no se les castigará o en su defecto saldrán libres por causas diversas, así como del principio jurídico mencionado al inicio de este estudio "*nullum crimen nulla poena sine lege*".

De lo anteriormente expuesto podemos concluir que la forma de erradicar y regular la tipificación de estos delitos siempre ha sido y es hacia aquellos individuos que realizan los actos, aquellos que ocupan a las computadoras como medio o fin de actos ilícitos, pero hasta el momento no se han preocupado nuestros legisladores por regular, tipificar, la conducta de aquellas personas que son las responsables directas de la creación y venta al público de los programas de cómputo y del propio equipo donde se comete la conducta propuesta a castigar, las cuales tienen los medios técnicos, económicos y humanos necesarios para poder proteger, en primer caso, su propiedad, en segundo, se fomenta el uso y compra de productos originales y como punto final participa conjuntamente con el Estado para proteger tanto sus derechos como los del usuario final, pues al proteger sus productos, inventos o programas, el Estado se dedicaría a la persecución de los sujetos activos que por sus características sería más rápida la investigación (comparativamente con el estado actual de ésta), llegando así al castigo e incluso me atrevería a decir que se llegaría a la extinción de esta conducta. Esto no quiere decir que se libere de su responsabilidad al Estado como garante de la seguridad en general para con la población, sino que el Derecho y sus instituciones deben de actuar y avanzar de acuerdo al propio avance

de la humanidad y su tecnología, es decir, como se señaló en los capítulos iniciales, darle forma a la interacción entre Derecho y tecnología.

4.5 Derecho de la Propiedad Industrial-Patentes

De entre el llamado Derecho de la Propiedad Industrial resalta la figura de las patentes, la cual, surgida a raíz de la Revolución Industrial y por tanto más reciente que las analizadas antes, se le ha considerado como uno de los métodos más apropiados para resolver el problema.

Sabemos que toda invención, para ser susceptible de atribuirle una patente, requiere denotar una novedad, actividad inventiva, así como una aplicación industrial. De estos elementos, los dos primeros son los que revisten mayor grado de dificultad en función de la complejidad del llamado estado de la técnica con base en la existencia o no de antecedentes, así como que dicha invención resulte o no evidente.

En el caso de los programas de cómputo, se discute en torno a estos asuntos y se evidencia de que no presentan caracteres suficientes como para atribuirles una patente. Algunos autores (y aun plasmado a nivel legislativo y jurisprudencial) consideran dicha figura como no aplicable, mientras que otros opinan lo contrario. Lo cierto es que, atendiendo a un criterio rígido, difícilmente podríamos dar cabida a una eventual patentabilidad de los programas; de aquí que se recurra a un análisis a la luz de otras formas de protección, bajo reserva de explotación de derechos.

Aun con lo anterior en materia de propiedad industrial, la Ley de Propiedad Industrial contiene varias normas que podría adecuarse a los supuestos de sustracción de información:

Título Tercero. De los Secretos Industriales. Capítulo Único. Artículo 82.- Se considera secreto industrial a toda información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener o mantener una ventaja competitiva o económica frente a terceros en al realización de actividades económicas y respecto de la cual haya adoptado los medios a sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.

La información de un secreto industrial necesariamente deberá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o a los medios o formas de distribución o comercialización de productos o prestación de servicios.

No se considerará secreto industrial aquella información que sea del dominio público, la que resulte evidente para un técnico en la materia, con base en información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial. No se considerará que entra al dominio público o que es divulgada por disposición legal aquella información que sea proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando la proporcione para el efecto de obtener licencias, permisos, autorizaciones, registros, o cualesquiera otros actos de autoridad.[288]

Artículo 83.- La información a que se refiere el artículo anterior deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros instrumentos similares.[289]

Capítulo III. De los Delitos. Artículo 223.- Son delitos:

---

[288] *Legislación Sobre Propiedad Industrial e Inversiones Extranjeras.* Leyes y Códigos de México. 24ª edición. Porrúa, 1999, pp.82-83.
[289] *Idem.*

V. Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que lo guarde o de su usuario autorizado, para usarlo o revelarlo a un tercero con el propósito de obtener un beneficio económico para sí o para el tercero, con el fin de causar un perjuicio a la persona que guarde el secreto industrial o a su usuario autorizado, y

VI. Usar la información contenida en un secreto industrial, que conozca por virtud de su trabajo, cargo o puesto, ejercicio de su profesión o relación de negocios, sin consentimiento de quien los guarde o de su usuario autorizado, o que le haya sido revelado por un tercero, a sabiendas que éste no contaba para ello con el consentimiento de la persona que guarde el secreto industrial o su usuario autorizado, con el fin de causar un perjuicio a la persona que guarde el secreto industrial o su usuario autorizado.[290]

De acuerdo con las disposiciones transcritas, esta ley protege la sustracción de información pero sólo aquélla que en términos de la misma constituya un secreto industrial, además de que para la configuración del delito se requiere de un elemento subjetivo especifico que está orientado a lesionar un interés patrimonial, por lo que más que una protección a la privacidad de la información, puede decirse que la protección al secreto industrial es una protección al patrimonio de su titular.

Como puede apreciarse, el tipo penal al igual que el de robo exige un "apoderamiento"; sin embargo, éste

[290] *Ibidem*, pp.74-75.

no debe entenderse en los mismos términos que aquel ya que en este supuesto el tipo exige que dicho apoderamiento se realice sobre un secreto industrial, que en términos del artículo 82 de la citada ley no es más que información. En virtud de que en términos del artículo 83 la información debe constar, entre otros, en medios electrónicos o magnéticos, el apoderamiento de la misma puede darse a través de un sistema informático.

Considerando que la sustracción de información no encuadra dentro del tipo penal de robo, y que la protección que otorga la Ley de Propiedad Industrial en esta materia se limita exclusivamente a los secretos industriales, puede concluirse que no existe una protección eficaz por parte de nuestro sistema jurídico frente a este tipo de conductas, respecto del área del Derecho que se estudia.

4.6 Derecho de la Propiedad Intelectual

Nuestro país ha alcanzado un grado de desarrollo muy prometedor en la industria de programación, lo cual, evidentemente, ha motivado la aparición de considerables controversias en relación con la propiedad de los programas, que trataron de resolverse, aunque no con mucho éxito, con un acuerdo ministerial de fecha 8 de octubre de 1984, que posibilitó la inscripción de los programas de computación en el Registro Público del Derecho de Autor, con más alcances administrativos que jurídicos propiamente dichos, constituyendo efectos meramente declarativos y no tanto constitutivos.[291]

Es así que con las últimas reformas los programas de computación, las bases de datos y las infraccio-

[291] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pág.93.

nes derivadas de un uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997.

Sobre el particular, y por considerar de interés el contenido de la exposición de motivos cuando esta ley se presentó ante la Cámara de Diputados, a continuación se presentan algunos comentarios pertinentes respecto a los elementos que deben contemplarse en la atención a la problemática de los derechos de autor en nuestro país.

De esta forma, cuando se presentó la iniciativa correspondiente, se dijo que la importancia de pronunciarse al respecto era que con dicha iniciativa se atendería la complejidad que el tema de los derechos autorales había presentado en los últimos tiempos, lo cual exigía una reforma con objeto de aclarar las conductas que podrían tipificarse como delitos y determinar las sancione que resultaran más efectivas para evitar su comisión.

Además, se consideraría que debido a que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de Decreto de Reforma al Código Penal para el Distrito Federal en materia de Fuero Federal, proponiendo la adición de un título Vigésimo Sexto denominado "De los delitos en materia de derechos de autor".

Al respecto, se consideraría conveniente la inclusión de la cuestión en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas, y por otro en un instrumento más adecuado para la procuración y administración de justicia, al poderse disponer en la investigación de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.

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

En este sentido, consideramos importante detenernos en los artículos 102 y 231.[292] El primero de ellos, regula la protección de los programas de computación y señala además que los programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos. El segundo, en su fracción V, sanciona el comercio de programas de dispositivos a sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo.

Un ejemplo de la falta de acción del Estado o autoridad encargada de la protección de los programas aún con la tipificación de estas conductas es el siguiente reportaje ubicado en la sección Interfase del diario Reforma, llamado "El mejor copiador de discos compactos", [...] "Nero" es un programa creado en Alemania simplemente

[292] LEGISLACIÓN SOBRE DERECHOS DE AUTOR. Leyes y Códigos de México. 21ª edición, porrúa, 1999, pp.34-72.

para grabar CDs. Pero eso de simplemente es muy relativo; la verdad es que cuenta con tantas opciones que puede convertirse en indispensable.

De entrada, a diferencia de la mayoría de los programas de su tipo que sólo permiten grabar dos tipos de discos -de música o de datos-, Nero ofrece nada menos que nueve formatos distintos, que incluyen video, discos de arranque e incluso discos híbridos.

Permite también manipular casi cualquier parámetro del disco a crear, aunque en realidad no hay mucho motivo para hacerlo (pero se siente bien tener la posibilidad abierta). Quizá la característica que ha convertido a este programa en un favorito, es su habilidad para vencer a la protección anticopias que muchos programas –particularmente juegos- incorporan en sus CDs. Por lo general, Nero logra realizar copias utilizables a partir de programas con este tipo de protección. [...].[293] En estos casos, cuando vienen de otros países los medios, es difícil castigarlos, pues como se vio y se vera posteriormente hay muchos problemas a nivel internacional para poder tener una línea tanto de investigación como de detención y castigo de los sujetos creadores de estos programas: este programa viene de Alemania, que dentro de su legislación no tiene tipificada esta conducta que señalan los artículos 102 y 231 de la legislación en comento, ya que ellos consideran que el empresario o productor no debe de tener o adquirir alguna responsabilidad, y por otro lado cada país trata al problema de diversa forma aún cuando ya hay de por medio un acuerdo o tratado firmado en este rubro; quizás sea por los resultados que puedan darse si aplicaran lo firmado en sus medios económicos, desarrollo tanto tec-

[293] LINX. "El mejor copiador de discos compactos", en Reforma, sección A. Interfase, Lunes 5 de febrero del 201, pág.4ª.

nológico como científico, primeramente a nivel nacional y posteriormente habría que soportar la embestida tecnológica de los otros países si no se tiene una actualización de estos medios, sin tener que preguntarse si es legal o no el hacerlo.

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

Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, artículo 424, fracción IV del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, del que se infiere la sanción al uso de programas virus.

Si bien pudiera pensarse que la inclusión de las sanciones a la fabricación de programas de virus en el Código Penal lleva implícito el reconocimiento de un delito informático, debe tenerse presente que los delitos a regular en este título son en materia de derecho de autor, en la que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los delitos informáticos el bien jurídico a tutelar son la intimidad, patrimonio, etcétera.

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

Por su parte, el artículo 231, fracciones II y III contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar

copias ilícitas de obras protegidas por esta Ley "y usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular".

La redacción de estas fracciones trata de evitar la llamada piratería de programas en el área del comercio, permite la regulación administrativa de este tipo de conducta, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, al igual que las infracciones contempladas para los programas de virus.

Además, la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su artículo 215 al Título Vigésimo Sexto del Código Penal citado, donde se sanciona con multa de 300 a 3 mil días o pena de prisión de seis meses hasta seis años al que incurra en este tipo de delitos.

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

Por otra parte, debe mencionarse que en abril de 1997 se presentó una reforma a la fracción III del artículo 231 de la Ley Federal del Derecho de Autor, así como a la fracción III del artículo 424 del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal. De esta forma, las modificaciones a la ley autoral permitieron incluir en su enunciado la expresión "fonogramas, videogramas o libros", además del verbo "reproducir".

Sobre el particular, debe mencionarse que durante la modificación a la Ley en diciembre de 1996 se con-

templó parcialmente lo que se había acordado en el Tratado de Libre Comercio y que por tal razón fue necesaria una segunda modificación en el mismo año, es decir en 1997, para incluir la acción de "reproducción".

Tal y como hemos sostenido, México no está exento de formar parte de los países que se enfrentan a la proliferación de estas conductas ilícitas. Recientemente la prensa publicó una nota en la que informaba sobre las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que alcanzaban un valor de mil millones de dólares por concepto de piratería.

Muchas personas sentirán que el país es ajeno a estas pérdidas por cuanto estas compañías no son mexicanas. Sin embargo, si analizamos a los sujetos comisores de estos delitos, según la nota de prensa, podríamos sorprendernos al saber que empresas mexicanas como "TAESA" y Muebles "DICO" entre otras, enfrentan juicios administrativos por el uso de programas piratas.

Esto, a la larga, podría traer implicaciones muy desventajosas para México entre las que podemos citar: la pérdida de prestigio a nivel internacional por el actuar ilícito de empresas cuyo radio de acción no está reducido al ámbito nacional, y la pérdida de credibilidad por parte de las compañías proveedoras de programas informáticos, lo que se traduciría en un mercado poco atractivo para ellas lo que pondría al país en una situación marginada respecto al desarrollo tecnológico.

Por otro lado y teniendo como mejor lugar éste para hacer mención de la situación internacional actual en general y como conclusión al presente capitulo, expondré una síntesis, tratando de realizarla conforme al anterior desarrollo de este capítulo; así pues, los países altamente informatizados, con una economía de corte capitalista, han concedido una importancia diferente al problema con res-

pecto a los países de economía socialista y más aún de los países en desarrollo.

En los países capitalitas se ha considerado que la vulnerabilidad de los programas está ligada estrechamente a los intereses de empresas privadas, particulares y también, claro está, del gobierno mismo. De esta forma, se habla de la necesidad de un régimen jurídico de carácter interno y externo que permita salvaguardar adecuadamente el desarrollo de la industria de la programación. Así, por ejemplo, en los Estados Unidos se han llegado a considerar a los secretos comerciales, las patentes y los derechos de autor, al igual que a la competencia desleal, como figuras aplicables sin que por el momento exista una definición al respecto. Por otra parte países como Canadá, Gran Bretaña, los países escandinavos, Alemania, Austria, Suiza, Bélgica, Holanda, Italia, Austria, España, y Portugal, han tratado de encontrar asimismo una solución al problema, sin que se manifieste un consenso unánime cuanto al régimen jurídico aplicable.

Por otra parte, países tales como Francia o Japón han generado incluso regulaciones específicas en torno a los programas, considerando que dicha cuestión amerita una resolución impostergable.

Por lo que respecta a los países socialistas, tenemos que en este tipo de naciones en que el control económico recae en el Estado el problema alcanza un significado diverso. Si bien el grado de información es suficiente como para que surjan dificultades alrededor de la protección de los programas, es el Estado a quien directamente le interesa controlar la producción y distribución de programas; de aquí que de un país de este bloque, como es el caso de Bulgaria, haya surgido un régimen específico relativo a los programas de cómputo. Dicha reglamentación, que data de 1979, tiende a estimular la actividad creadora de pro-

gramas, atribuyendo al reconocimiento de una serie de derechos sobre el mismo, lo cual le permite obtener al creador ciertos ingresos con motivo de la difusión de su obra. Esto es controlado por dos órganos estatales, uno encargado del registro de programas denominado Fondo Nacional de Proyectos y Programas, y el otro encargado de la difusión de éstos como lo es la Biblioteca Central de Proyectos y Programas (BCPP), un dispositivo sin duda interesante que permite beneficios considerables tanto a creadores de programas, usuarios de los mismos y el Estado, quien recibe ingresos a manera de "comisión" por fungir como ente "mediador" y aun como autoridad en caso de suscitarse litigio, con motivo de la creación y explotación de programas.[294]

Lo anteriormente expuesto es una forma de poder contrarrestar y estimular a los programadores de nuestro país, pues como lo mencione al principio de nuestro estudio, ellos actúan a veces de forma ilícita creando programas dañinos o perjudiciales para diversas áreas o tecnologías. porque son explotados y no se les toma en cuenta posteriormente como parte importante del desarrollo de un programa.[295]

Otros países de este bloque como Rusia, Hungría y Polonia, también han manifestado interés en el problema aunque sin que hasta la fecha (al menos en lo que sabemos) dispongan de un método de protección.

Respecto de los países en desarrollo tenemos que la informática se presenta, al igual que otros productos y servicios, como la "solución" indiscutible a sus problemas. La variedad de equipos introducidos genera, a su vez, la aparición de diversos programas, muchos de ellos de ori-

[294] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pág.92.
[295] Ver *Supra.*, pág.38.

gen extranjero, que por momentos impiden el surgimiento y desarrollo de una industria nacional, por lo que en la mayoría de las ocasiones se presenta como más recomendable el surgimiento de normas (entiéndase política informática) que favorezcan la buena marcha de dicha industria, complementado por reglas jurídicas (entiéndase derecho de la informática) que provean de elementos de protección como lo serían para los programas mismos.[296]

La formalización de figuras de reserva privativa (sea patente o derechos de autor), aunada a una incipiente creación de programas nacionales, generaría que los países en desarrollo con un determinado grado de informatización continuaran siendo verdaderas "cajas de pago" por concepto de regalías producidas por la explotación de inventos u obras como en este caso serían los programas de cómputo, por lo que es necesario un análisis cuidadoso que dé lugar a un régimen favorecedor a los intereses de este tipo de países. Naciones como Brasil, Argentina y la India han dado la pauta para que el desarrollo informático sea un verdadero recurso hacia el progreso y no un problema más que propicie un deterioro todavía más pronunciado en las de por sí ya endebles economías en este bloque de países.[297]

En este entendido, consideramos que por la gravedad de la conducta ilícita en éstos y las implicaciones que traería aparejada, justifica su regulación penal actual, pero esto no debe de terminar con la tipificación de dichas conductas y de quien las comete, pues como hemos venido diciendo en el transcurso del presente estudio, si tipificamos la conducta de los productores o creadores de programas o software así como de equipos o hardware,

[296] TÉLLEZ VALDÉS, Julio. *Op. Cit.*, pp.92-93.
[297] *Idem.*

ya sean personas físicas o morales, grandes o pequeños empresarios; con el fin de que éstos protejan a los medios por los cuales se realizan las conductas ilícitas y particularmente la piratería de programas o software, antes de su venta o salida al mercado tanto nacional como mundialmente.

De esta forma podemos eliminar a los piratas "empíricos" y a los que no cuenten con los conocimientos tanto técnicos como equipos para dichos actos ilícitos, pues al estar protegidos estos medios, si no se tienen los conocimientos profesionales para poder eliminar esta protección, pues no podrán cometer el delito tan fácilmente, y digo tan fácilmente porque para que lo pudieran hacer tendrían que contratar los servicios de un profesional, el cual cobraría una cantidad considerable por violar-destruir esta protección; este profesional, para haber aceptado, tuvo que pasar por diversas etapas de análisis de la conducta y sus consecuencias, lo cual nos lleva a concluir que serían pocos aquellos que lo llegasen a realizar, por varias causas, las principales serían el castigo a dicha conducta, la pérdida de su profesión así como su licencia para ejercerla, por lo que no sería tan fácil el realizar piratería al tipificar la conducta de los creadores de los medios por los cuales se cometen estas conductas.

CAPÍTULO QUINTO

CRIPTOLOGÍA, MARCO CONCEPTUAL Y CRÍTICA A DICHO SISTEMA

5.1 Criptología

El principal interés que tenemos, y por el cual se analiza al presente sistema de seguridad es con el fin de que conozcamos para que sirve, cómo se aplica, sus diversas acepciones, así como sus principales ventajas e implicaciones. De igual forma y siguiendo con el análisis de dicho sistema de seguridad podremos dar una conclusión y crítica del sistemas en comento, el cual hasta el momento se considera un método seguro por medio del que se envía y recibe todo tipo de información, que regularmente tiene relación directa con un texto, el cual puede ser tanto una simple carta como una fórmula secreta o algún comunicado entre gobiernos a nivel internacional. Así pues, veremos qué tan segura es esta forma de protección, si es tanto como se afirma y, como cuando se produce un quebranto a ésta se viola el derecho a la privacidad. Con lo anteriormente dicho y una vez ya hecho el análisis podremos fundar nuestra propuesta dando un pilar más a la misma, pues es otra forma de demostrar que al no regular la conducta del productor, creador o inventor de software o hardware con el fin de realizar actos que se consideran ilegales, se violan tanto los sistemas de seguridad como el derecho; finalmente haremos una crítica a la criptología.

El ataque a los datos ha sido siempre el más sencillo de realizar, ya que no es necesaria ninguna especiali-

zación para ello. Interceptado el mensaje (o el mensajero) o alcanzada la información, el atacante logra su objetivo. Por ello, desde la más remota antigüedad, los que poseían información valiosa (estadistas, militares, diplomáticos, etc.) intentaron hacerla ininteligible a toda persona, no autorizada mediante su cifrado.

La Criptografía (del Griego Kriptos, secreto u oculto, y Graphos, escrito) es *la ciencia que estudia la escritura secreta,* la forma de ocultar el significado de una información. Pero como el conocimiento de la información puede proporcionar beneficios siempre ha habido personas dispuestas a atacar una información, aunque se encuentre cifrada, por encargo de gobiernos (espías), empresas (espías industriales) o para su propio beneficio (chantajistas, estafadores o ladrones informáticos). Surge entonces la ciencia contraria, el Criptoanálisis. Podemos definir el Criptoanálisis como *la ciencia que estudia como esclarecer la escritura secreta u oculta.*[298]

Aunque durante mucho tiempo ambas ciencias se han considerado un arte, no cabe duda que hoy día constituyen conjuntamente una ciencia bien estructurada llamada **Criptología**. Se puede definir a la Criptología como *la ciencia que estudia como cifrar y descifrar información.*

La criptología se incorpora al sistema de información una vez determinado qué ha de protegerse y con qué niveles. Se puede definir como un sistema de codificación de un texto, con claves confidenciales y de procesos matemáticos complejos (algoritmos), de forma que resulte in-

[298] MINGUET MELIÁN, Jesús Ma. "Criptología", en *Informática y Derecho, Revista Iberoamericana de Derecho Informático.* Jornadas: Marco Legal y Deontológico de la Informática, actas Volumen I, UNED. Centro Regional de Extremadura. Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura-Mérida. 1998, pág.527.

comprensible para el tercero que desconozca la clave descodificadora.[299]

Es importante tomar en cuenta y tener presente en el transcurso del presente, lo anteriormente expuesto; es decir, la importancia que tiene el que las claves o passwords del sistema de seguridad no los sepa otra persona o tercero ajeno, o no aplicar las medidas de seguridad para su protección tanto de las claves como del propio sistema, pues entonces sería en vano el aplicar dicho sistema, con lo cual quiero señalar que si en algún momento el diseñador, creador o inventor de dicho sistema aplicara un sistema de seguridad ajeno al funcionamiento de éste, pero intrínsecamente ligado al mismo, los resultados serían otros y en consecuencia, los ilícitos que se pudieran dar serían mínimos y estos serían a la vez dirigidos a sujetos específicos dentro de las distintas ramas de la tecnología, la industria, la política u operaciones militares, por lo cual se podría realizar una investigación más específica y con resultados óptimos, al no tener que hacer un análisis global de todas las posibles personas o atacantes, dirigiéndose a una sola línea de los posibles delincuentes cibernéticos.

La criptología ha sido utilizada tradicionalmente en los ámbitos militar, diplomático y comercial. Actualmente se ha ampliado a otros usos mucho más próximos aunque con niveles de exigencias diferentes, entre los que son cada vez más frecuentes las aplicaciones destinadas a la protección de los derechos y libertades. La forma tradicional de preservar la confidencialidad de una red de comunicaciones ha sido la protección criptológica, que implica

[299] NÚÑEZ JIMÉNEZ, José Manuel. *"Valor Probatorio del Documento Electrónico. Su autenticidad a través de la Criptografía o Criptología como garantía del Documento Electrónico"*, en Informática y Derecho, Revista Iberoamericana de Derecho Informático. Jornadas: Marco Legal y Deontológico de la Informática, actas Volumen II, UNED. Centro Regional de Extremadura. Universidad Nacional de Educación a Distancia. Centro Regional de Extre madura-Mérida. 1998, pp.1076-1077.

la utilización de técnicas que permiten llevar a cabo el ocultamiento de la información protegida a personas no autorizadas. Siendo esto así, la criptología se convierte en una exigencia imprescindible. La protección criptológica presenta diversos grados de infalibilidad, según se trate de intereses de extrema importancia o de intereses de menor relevancia, es decir, según se trate de comunicaciones públicas o privadas. Mientras que en las primeras la regla general es la transparencia, en las segundas prima el imperio del secreto profesional. Esto nos llevaría a la necesidad de protección sistemática de las comunicaciones privadas y, excepcionalmente, de las públicas.[300]

En base a lo anteriormente expuesto podemos afirmar el comentario hecho anteriormente, pues al ver las áreas donde se aplica la criptología, nos preguntamos por qué no se obliga al creador de dicho sistema de seguridad a tomar las medidas necesarias, idóneas para el caso de que cuando se llegase a violar la seguridad del sistema en comento, se destruyese tanto el hardware y software del atacante como, y en caso extremo, la propia información que se trata de copiar o extraer ilegalmente.

La protección criptológica de los datos "sensibles" se sitúa en el contexto de la aplicación de las nuevas tecnologías de la información, en el entorno social, jurídico y político de una sociedad democrática, donde encuentra su reforzamiento y legitimación, pero también sus límites. Globalmente considerada, requiere la adecuación de los niveles de protección a la naturaleza de la información protegida, de forma que haga posible el juego de los distintos derechos afectados.[301]

Podemos ver que la propia doctrina está acorde con nuestra opinión, pues primeramente sitúa a la criptología

[300] *Idem.*
[301] *Ibidem*, pág.1078.

en la era moderna tecnológica y a la vez la considera limitada. En consecuencia, falta el tomar una decisión firme sobre la regulación de este sistema mediante la cual se pueda otorgar seguridad a los usuarios de la criptología, pero sin violentar la de otros o la ya establecida.

Como lo señalamos en el texto anterior, todo derecho tiene sus límites en relación a los derechos fundamentales que establece la Constitución. La protección criptológica debe respetar la Norma Suprema, evitando posibles colisiones con derechos y libertades que gozan de protección específica. Este es el caso de entrar en polémica con los derechos al honor, la intimidad y la propia imagen.

Por otro lado, existen dos grandes técnicas criptológicas:

a) sistemas simétricos: el emisor, como el destinatario de un mensaje disponen de la misma clave para el cifrado y descifrado de aquél.
b) sistemas asimétricos: funcionan por la combinación de dos tipos de claves una pública y otra secreta que se corresponden.[302]

Uno de los grandes inconvenientes de la protección criptográfica es su costo tan elevado. Si bien, y a pesar de esto, las ventajas que supone la transmisión electrónica, aunadas a las garantías de seguridad que nos ofrece la criptología, superan con mucho el inconveniente anterior.

Ciertamente su costo es elevado, pero los resultados hasta el momento han sido positivos como para seguir aplicándolo, pero si las autoridades exigieran tanto su aplicación como el que tuvieran una seguridad como la expuesta anteriormente para con los usuarios finales, el propio

[302] *Idem.*

usuario compraría el producto recuperando el empresario el gasto realizado.

Un ejemplo de esto es lo siguiente: "En los llamados sellos del software", es el mismo ordenador el que asocia a cada instrucción un valor numérico, y así, si el programa se modifica, el valor de las instrucciones que lo componen se altera, y es el mismo ordenador el que, comprobando la desigualdad entre las claves y el valor numérico del programa, rechazaría la ejecución del mismo, señalando sus alteraciones".[303]

Este sistema podría ser uno de los que se utilizarían para la protección del software por parte de los empresarios, creadores o inventores de ellos, antes de que estos salgan al comercio mundial, pues así no habría tanta proliferación de piratería en lo que respecta al software, pero vemos que actualmente no se ha tomado alguna decisión al respecto, sólo se han realizado acciones en contra de quienes cometen el delito, con la tipificación de las conductas, el aumento de penas, decomisos de los bienes con cuales se cometen las conductas ilícitas o bien que son producto de dichas conductas, etc.

El uso de la criptología para la codificación de la información en ordenadores y redes, al igual que los sistemas de control de accesos mediante passwords, suponen un obstáculo técnico para la investigación de los hechos presuntamente delictivos, pero es la única forma, también, de preservar la intimidad y propiedad de la información. Dilema éste que debe ser resuelto al tenor de conceptos genéricos tales como la Justicia y la Seguridad, bajo la perspectiva de nuestra Constitución y de todo el Ordenamiento Jurídico. Por lo tanto, es conveniente que los países

[303] *Ibidem*, pág.1079.

vayan incluyendo en sus leyes la regulación y consecuencias de las prácticas criptológicas, ya que éstas no son inocuas. Utilizadas de forma abusiva o fraudulenta pueden, no sólo atentar contra la libertad de información, sino obstaculizar el normal desenvolvimiento de la sociedad y el Estado a través de la creación de reductos impenetrables.[304]

Como podemos ver la doctrina vuelve a darnos otro punto a nuestro favor, pues en el texto anterior nos señala las implicaciones propias de la aceptación y puesta en marcha de dicho sistema de seguridad, así como sus consecuencias tanto previsibles como realizables; de igual forma conocemos las consecuencias para el propio Estado y la Sociedad.

5.1.1 Fundamentos Teóricos de la Criptología

Aunque Baueren en su trabajo ha demostrado que todos los algoritmos criptográficos de la historia obedecen a los principios de la ciencia criptográfica, se considera que el nacimiento como verdadera ciencia de la criptografía se basa en dos hechos recientes:

- Los estudios de Shannon sobre los fundamentos matemáticos de la teoría de la comunicación (1948) y su aplicación a los criptográficos (1949).
- La publicación de Diffe sobre las bases teóricas de la criptografía de clave pública en 1976.[305]

[304] *Ibidem*, pp.1079-1080.
[305] MINGUET MELIÁN, Jesús Ma. *Op. Cit.*, pp.533-534.

La ciencia criptológica se basa en aspectos de la Teoría de la Información y de la Codificación, de la Teoría de números, de la Teoría de la Complejidad Algorítmica y de la Teoría de la Probabilidad. –Respecto a estas teorías sólo hacemos mención de ellas como tales, sin profundizar en el análisis de éstas, pues para nuestro fin basta con conocerlas únicamente y diferenciar a unas de otras mediante sus características más particulares–.

Dentro de la Teoría de la Información los aspectos más fundamentales son los conceptos de entropía, entropía condicional, secreto perfecto, distancia de unicidad, confusión y difusión.

De la Teoría de Números destacaremos la aritmética modular, los logaritmos discretos, el cálculo de inversos, la función de Euler, el teorema chino del resto y el cálculo aritmético en campos de Calois.

La Teoría de la Complejidad Algorítmica trata de la clasificación de los problemas en función de que se conozca o no un algoritmo para su resolución, y del tipo de estos algoritmo en función de su tiempo de computación. Es de destacar que la evolución de la tecnología en el campo de la velocidad de cómputo hace que problemas que eran intratables o computacionalmente incalculables años atrás sean hoy día totalmente resolubles en tiempo y costo admisibles.

Por último, la Teoría de la Probabilidad, aunque importante para algunos aspectos de la Criptología, es básica para la práctica del Criptoanálisis.

Como podemos ver, estas teorías son muy amplias y complejas principalmente por su relación con los cálculos, pero al mismo tiempo no deja de ser impresionante la forma en que ocupan a estas mismas para llevar acabo conductas ilícitas en el área de la informática; así pues, conociendo ya las ramas diversas por las cuales se forma o se da vida tanto a la criptología como al

criptoanálisis, pasemos al estudio de la información ya como un sistema propiamente dicho.

5.2 Sistemas de Información

De hecho el Sistema de Información desempeña cada vez un papel más importante en el funcionamiento de las organizaciones, las cuales llegan casi a depender totalmente de ellos. Un Sistema de Información está compuesto por los recursos informáticos (soporte informático tanto físico como lógico), activos de información (datos o información) y personas (usuarios informáticos o usuarios finales).[306]

Pero a la vez que los sistemas informáticos se han ido haciendo más complejos, aparecen más y más puntos vulnerables. El número de posibles atacantes a los sistemas de información crece día a día y con las más variadas motivaciones (beneficios económicos, espionaje, venganza, terrorismo, reto personal, etc.). Simultáneamente los medios técnicos para intentar vulnerar un sistema informático son muy sofisticados y de su mismo nivel tecnológico.

De ahí que sea imprescindible el pensar en proteger los sistemas de información. Es necesario el practicar la Seguridad Informática.

Es verdad que en la actualidad los sistemas de información tienen que estar con una protección no al cien por ciento sino al doscientos por ciento, así como de igual forma deben de tener una actualización en sus áreas de informática, tanto en su software como en hardware, para que el día menos pensado no se encuentren con la sorpresa de que han sido atacados de una forma cibernética u informática en sus bienes o patrimonio.

---

[306] *Ibidem*, pág.528.

5.3 Seguridad Informática

Resulta en general muy difícil hablar de seguridad, ya que la seguridad absoluta no existe. Para poder establecer que un sistema informático es seguro sería necesario identificar todas las amenazas a las que puede verse sometido. Por ello quizás sea más apropiado hablar de vulnerabilidad.

Según el profesor Valentín San Caja, la vulnerabilidad de un sistema informático es la cualidad que le hace susceptible de ser afectado, alterado o destruido por algún hecho o circunstancia indeseados, de recibir algún daño o perjuicio en cualquiera de las partes o componentes, que afecte al funcionamiento normal o previsto de dicho sistema informático.[307]

Análogamente define a la seguridad de un sistema informático como el estado de protección del mismo, establecido con el fin de evitar la aparición de las distintas amenazas posibles que puedan alterar su normal funcionamiento, o de aminorar las consecuencias negativas de los distintos riesgos, una vez producidos.

Actualmente se está tendiendo por los responsables de la seguridad de las empresas con grandes sistemas de información a una normalización de la terminología de seguridad informática. Según la Comisión de Seguridad de SEDISI, se distinguen los siguientes componentes en un análisis de riesgos:

- Sistemas de Información. Son los Recursos Informáticos y Activos e Información de que dispone la empresa para su correcto funcionamiento y la consecución de los objetivos propuestos por la Dirección.

[307] *Idem.*

- Amenaza. Cualquier evento que pueda provocar daño en los Sistemas de Información, produciendo a la empresa pérdida materiales o financieras.
- Vulnerabilidad. Cualquier debilidad en los SI que pueda permitir a las amenazas causarles daño y producir pérdidas a la empresa.
- Impacto. Es la medición y valoración del daño que podría producir a la empresa la materialización de una amenaza sobre los SI. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles.
- Riesgo. Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del SI, causando un impacto en la empresa.
- Defensa. Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo. Debe realizarse una valoración cuantitativa de su coste.[308]

En estos momentos no sólo se trata de identificar las posibles formas de ataque y de prevenirlas, sino más bien, claro está, una vez ya identificados los posibles atacantes o agresores, tomar medidas estrictas contra estos delincuentes informáticos, de tal forma que se disminuyan las conductas antijurídicas realizadas por estos sujetos.

[308] *Ibidem*, pp.528-529.

5.4 Activo Información

El activo información puede adoptar muchos formatos, tanto dentro de los sistemas como fuera de ellos. Así podemos clasificar la información en:

- Impresa. Escrita en papel;
- Almacenada. En los sistemas o en medios portables;
- Transmitida. A través de redes o entre sistemas;
- Hablada. En conversaciones.[309]

Pero independientemente de su formato, la clasificación que más nos interesa es la que se relaciona con el valor que la información tiene para la organización. Según este criterio, podemos dividir las informaciones en clasificadas y no clasificadas.

Las informaciones no clasificadas son aquellas que su divulgación o uso no autorizado no ocasionan pérdidas significativas para la organización. A su vez se subdividen en: de uso general (información que puede ser conocida y utilizada por todos los empleados y algunos colaboradores externos autorizados, y cuya divulgación o uso no autorizados podrían originar pérdidas leves y asumibles por la organización).

Los activos clasificados se subdividen en: confidencial (información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesitan para realizar su trabajo, y cuya divulgación o uso no autorizado podría ocasionar pérdidas significativas, materiales o de imagen) y secreta o reservada (información que sólo pue-

[309] *Ibidem*, pág.530.

de ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección, y cuya divulgación o uso no autorizados podrían ocasionar graves pérdidas materiales o de imagen).

Cada nivel de información debe tener defensas o prevenciones en función de la gravedad del impacto que produciría su vulnerabilidad.

Ejemplificando lo anteriormente expuesto, pues según la clasificación que se mencionó hay uno que es público y otro privado, pero para un concepto rápido, podemos decir que si se tienen los medios suficientes, se pueden obtener de estos sistemas de seguridad sin mayor problema la autorización para introducirse a ellos, quedando así una vez más vulnerable el sistema que se haya forzado o engañado para poder acceder.

5.5 Seguridad Activo Información

Según el Libro Naranja de los E.E.U.U. (normas del Truster Computer System Evaluation Criteria) y el ITSEC (Information Technology Segurity Evaluation Criteria), al establecer la seguridad de la información hay que tener en cuenta tres criterios fundamentales: confidencialidad, integridad y disponibilidad.

La confidencialidad (secreto) protege a los activos de información contra acceso o divulgación no autorizados.

La integridad garantiza la exactitud de los activos contra alteraciones, pérdida o destrucción, ya sea accidental o intencionada.

Por último, la disponibilidad asegura que los recursos y activos informáticos pueden ser utilizados en la

forma y el momento requeridos. También incluye su posible recuperación en caso de desastre.[310]

La transmisión de datos a través de redes de computadoras ha creado nuevos problemas de seguridad, por lo que a las normas ISO y CCITT se añaden dos nuevas características: la autenticidad y la imposibilidad de rechazo.

La autenticidad asegura el origen y el destino de la información.

La imposibilidad de rechazo o no repudio asegura que cualquiera que envíe o reciba un activo información no pueda alegar ante terceros que no la envió o la recibió.[311]

5.5.1 Defensa de los Activos de Información

Las defensas o medidas de seguridad a establecer en un sistema de información se agrupan en cuatro tipos: legales, administrativas u organizativas, físicas y lógicas.

Los informáticos deben conocer la legislación vigente, pues a veces imponen obligaciones de seguridad, para conocer qué tipos de amenazas deben ser prevenidas especialmente y qué tipos de impactos pueden ser perseguidos legalmente. En algunos casos esto es especialmente importante como cuando los activos a proteger contienen datos de carácter personal, los que afectan al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1 de la vigente Constitución Española).[312]

Es verdad que en nuestra actualidad la persona que se dedique a la informática debe conocer los alcances legales de su actuar pues ya no estamos como para

[310] *Ibidem*, pp.530-531.
[311] *Idem*.
[312] *Ibidem*.

evadir responsabilidades y la acción de la justicia, aún cuando así ha pasado frecuentemente, pero no es por la mala actuación de la autoridad sino por la falta de figuras acordes con la realidad informática y las conductas que derivan de ella, por la aplicación ya sea de software o hardware para la comisión del delito.

Una primera forma de defensa y aplicación de la legislación vigente son las medidas de carácter administrativo u organizativo, como la creación de una infraestructura de seguridad informática en los distintos niveles (Comité de Dirección, Comité de Seguridad Informática, Responsable de Seguridad, etc.), normativas de seguridad y planes de seguridad y contingencias.[313]

El siguiente nivel de protección es el Físico. Sin entrar en detalles, este nivel abarca la construcción y control de acceso a los centros de Proceso de Datos, las medidas de protección contra fuegos, fallos de energía eléctrica o falta de aire acondicionado, los armarios de almacenamiento de las cintas de back-up, la protección durante el transporte de los soportes de almacenamiento, las llaves de disqueras, etc. En el nivel más cercano a los activos de información se encuentran las medidas de protección lógicas: identificación, autorización y autentificación de usuarios, contraseñas (password), claves, cortafuegos (firewalls), cifrado, etc.[314]

5.6 Criptografía de Clave Privada

La característica de los criptosistemas de clave privada o secreta es utilizar la misma clave para el cifrado y el descifrado, por lo que también se llaman simétricos. Como in-

[313] *Idem.*
[314] *Idem.*

dicamos anteriormente, proporcionan secreto y autentificación. El secreto quedará garantizado si los comunicantes mantienen la clave común en secreto. La autenticidad se consigue al emplear ambos la misma clave y, por lo tanto, sólo el emisor legitimado puede enviar un mensaje cifrado que al descifrarse quede en claro. El principal problema de estos sistemas es el intercambio seguro de las claves, aunque existen algunos protocolos, como el de Diffie-Hellman, que lo facilitan y añaden seguridad. También hay que limitar el número de corresponsales ya que el número de claves aumenta con el cuadrado del número de nodos. Además casi todos los algoritmos de este tipo han sido vulnerados.

Aquí podemos ver que sigue existiendo el problema de la seguridad para con las claves y otras formas de seguridad, pues si a alguno de los propietarios o encargados de estas se les ocurre darlas a conocer o por algún error las conoce otra persona, el sistema de seguridad deja de ser seguro y por ende se debe de desechar, llegando así otra vez a la pregunta que hemos hecho en el transcurso del presente análisis, ¿a caso no tienen responsabilidad los creadores o proveedores de programas, por no aplicar un sistema de seguridad confiable al cien por ciento?.

Existen dos esquemas principales de cifrado: el cifrado en flujo (se cifra cada uno de los bits del mensaje) y el cifrado en bloque (se cifran conjuntos de bits).

El más utilizado actualmente de los cifradores en bloque es el DES (Data Encryption Standard) desarrollado por IBM y estándar del NIST (National Institute of Standards and Technology) para las aplicaciones no clasificadas del Gobierno de USA. Aunque parece ser que todavía no ha sido vulnerado, ha sufrido numerosas críticas.[315]

La única forma conocida de ataque es probar las

[315] *Loc. Cit.*

72.057.594.037.927.936(2^{56}) claves distintas, lo que para un ordenador que pudiera probar un millón de claves por segundo supondría unos 2.285 años. Este tiempo se reduciría de forma considerable utilizando supercomputadoras con muchos procesadores en paralelo (hasta unas pocas horas) y que sólo están al alcance de ciertas organizaciones.

Como podemos ver, es difícil pero no imposible el que se pueda vulnerar este tipo de seguridad; lo único que hay que hacer es acabar con todas las posibilidades y alguna de ella será la correcta.

5.6.1 Criptografía de Clave Pública

Se caracteriza por el uso de dos claves por cada miembro del sistema: la pública (que sirve para que el resto de los miembros puedan cifrar los mensajes que quieran dirigirle) y la privada (que evidentemente es secreta y sirve para recuperar la información).

Se basa en las llamadas funciones unidireccionales con trampa. Una función unidireccional es aquella que es fácil de calcular, mientras que su inversa es difícil de computar por su elevada complejidad. Se denomina función unidireccional con trampa a aquellas funciones unidireccionales que pueden ser invertidas fácilmente, si se conoce alguna información adicional extra (trampa).[316]

Para una clave de 200 bits el número de pasos que necesitaría un atacante para violar el sistema sería de $2{,}7 \times 10^{11}$ que a un microsegundo por paso supondría varios días. Si la clave sube a 664 bits (200 dígitos decimales) el número de pasos asciende a $1{,}2 \times 10^{23}$ lo que supondría actualmente 10^{12} años.[317]

---

[316] *Ibidem*, pág.540.
[317] *Idem*.

5.7 Criptoanálisis

Si queremos comprobar la seguridad de un criptosistema, hemos de considerar todos los posibles ataques que pueden sufrir los mensajes cifrados por parte de personas que no poseen la clave. De hecho en los congresos internacionales no se admite ningún trabajo sobre un nuevo algoritmo que no vaya acompañado del correspondiente criptoanalisis, y no olvidemos que hoy día el criptoanalista posee unos medios muy poderosos.

Una de las técnicas más utilizadas es el análisis estadístico de los mensajes cifrados para determinar la frecuencia de aparición de los diferentes símbolos, el tamaño de las palabras, las palabras más comunes, etc. Por ello los criptosistemas que proporcionan una correspondencia, uno a uno entre los símbolos de los alfabetos del mensaje y del cifrado, son muy vulnerables al criptoanálisis.

Existen principalmente tres métodos de atacar a los criptosistemas: ataques a partir sólo del texto cifrado, ataques a partir de algún mensaje conocido y ataques por elección del mensaje.

El ataque por elección del mensaje se produce cuando el criptoanalista tiene acceso al sistema informático para introducir mensajes y observa el resultado privado. Por ejemplo, el atacante podría introducir un registro apropiado en una base de datos criptografiada y obtener cómo se ha cifrado la información. Insistimos por tanto en la aplicación conjunta de diversas defensas o medidas de seguridad (control de acceso, autentificación de usuarios, etc.), además de las criptológicas.

También es importante para que los criptoanalistas, aunque lleguen a consumar su ataque y

obtengan las claves, éstas les sean inútiles, el recordar que la fortaleza de los criptosistemas reside en el secreto de las claves. Por ello aparece un problema que suele traer de cabeza a los responsables de seguridad y administradores de sistemas de información: la generación, administración y distribución de claves.

5.8 Aplicaciones Criptográficas

La criptología permite realizar con seguridad muchas aplicaciones informáticas en redes de computadores que están revolucionando la sociedad actual y lo harán mucho más en el futuro, cuando se regulen legalmente. Entre ellas destacaremos la firma digital, las elecciones electrónicas, la autenticidad, integridad y reutilización de mensajes, la certificación y notaría electrónicas, la firma de contratos, demostrar el conocimiento de secretos sin proporcionar ninguna información de ellos, la transferencia electrónica de fondos, el manejo de tarjetas inteligentes en cajeros automáticos, etc.

Para la resolución de estos problemas se emplean los algoritmos de clave pública y privada existentes, siguiendo protocolos de funcionamiento bien determinados. Un protocolo es una secuencia ordenada de pasos a realizar por dos o más entidades para completar una tarea.

5.9 Crítica al Sistema

Como hemos podido darnos cuenta, la criptología hasta cierto punto nos ha servido como un sistema de seguridad "efectivo", pero en el propio transcurso de este capítulo

también nos hemos podido dar cuenta que este sistema deja de ser seguro o privado cuando se conoce o se da a conocer su mecanismo de protección, el cual puede ser por medio de claves, passwords o sistemas lógicos de protección, por lo cual no es infalible. Es posible entrar a los sistemas presumiblemente protegidos, quedando dentro de éstos la pregunta que se realizó anteriormente en cuanto a la responsabilidad de los creadores o proveedores de software o hardware por su implicación dentro de estos ilícitos, al proporcionar los medios y facilitar la comisión de las diversas conductas ilícitas.

Propuesta Final

Como lo señala el título, es aquí donde desarrollaremos nuestra teoría a proponer, la cual se ha mencionado en varias ocasiones en el transcurso del desarrollo del presente estudio. Iniciaremos con una pequeña síntesis de lo hasta aquí desarrollado para poder enlazar esta propuesta con la legislación que se pretende aplicar a la conducta a tipificar. Pasemos pues a la exposición de nuestra propuesta.

El auge que ha tenido esta rama de la Informática, la cual es conocida como software y, la cual día a día aumenta su potencialidad dado el perfeccionamiento de los sistemas de programación en las diversas áreas en que se utiliza, así como el aumento de quehaceres o trabajos donde se utiliza una computadora como el medio idóneo para realizarlos, al igual que el perfeccionamiento de éstos, obliga a que nos preguntemos sobre la necesidad de una reforma en esta materia que proteja especialmente a dichos programas o software de la figura delictiva conocida como piratería, ya vista anteriormente. No es que no esté regulada o esté tratando de invalidar el tipo penal establecido, sino que se debe de tipificar la conducta del proveedor o inventor de dichos programas.

Esta reforma planteada encuentra su justificación en la existencia de un bien que ciertamente ya se ha protegido pero esta protección no ha dado los resultados esperados, desde nuestro punto de vista, porque la conducta del sujeto que debe adecuarse a las características delictivas, la del proveedor o creador de programas que son realizados y sirven específicamente para llevar a cabo la conducta delictiva.

En lo concerniente a ésta, debemos señalar primeramente que la conducta que se propone tipificar con-

tiene características que la hacen especial entre las demás, pues el que se trate la conducta de un sujeto como ilegal o se castigue a éste por proporcionar los medios para cometer la conducta ilícita, que incide directamente sobre la economía de un país no es fácil, primeramente porque nos encontraremos con opiniones en contra para este tipo de propuestas y, una de ellas es quizás la que ya habíamos mencionado en el apartado que le correspondió al estudio de los delitos informáticos, particularmente en Alemania. En dicho país se señala que las personas físicas o morales, mejor conocidas como proveedores, creadores, diseñadores o inventores de un programa de cómputo, no adquieren ni son responsables por algún tipo de ilícitos que se cometan con dichos programas registrados como suyos; este tipo de impedimentos sociopolíticos y económicos son, desde mi punto de vista, los que han hecho que este tipo de personas sigan actuando impunemente tanto a nivel nacional como internacional, creando un sin fin de programas que facilitan la comisión de diversas conductas ilícitas y particularmente la conocida como piratería en su modalidad de copia ilegal de software o programas de cómputo; un ejemplo claro de lo que acabamos de mencionar es el reportaje que apareció en el periódico Reforma en el cual se da conocer la nueva versión de un programa llamado "Nero", que es capaz de traspasar la seguridad impuesta por algunos –señaló algunos porque actualmente no están obligados a proteger la información o productos que saquen a la venta en general– de los fabricantes originales de la información.[318]

Como hemos visto a lo largo del presente estudio, la responsabilidad de las personas morales –en este caso de los proveedores y/o de las encargadas de la crea-

[318] Ver *Infra*, pág.133.

ción, invento diseño de programas de computadora, mejor conocidos como software–, es actual y cierta, pues a lo largo del desarrollo de la industria y la tecnología estos sujetos siempre han estado presentes como un elemento imprescindible, tanto para su desarrollo como para su distribución, venta y comercialización a nivel nacional e internacional. Hasta estos momentos hemos visto la indiferencia con que se trata por parte de las autoridades este problema, que a pesar de los avances mismos de la tecnología y de la legislación en estas áreas, siguen habiendo y realizándose actos ilícitos contra el software o programas de computadora, conocidos o llamados generalmente piratería.

Es importante señalar también que –y como ya hemos afirmado anteriormente–, no se trata de limitar y hasta en un momento de extinguir la producción, creación o invención de programas, en los diversos niveles tecnológicos tanto nacional como internacionalmente, pero debemos de hacer hincapié en que si no se regula esta conducta, muy pronto –de hecho como lo podemos ver ya hay evidencias claras– habrá programas que no sólo violarán la seguridad de fábrica sino también darán la facilidad de hacer una copia total y fidedigna de cualquier tipo de información que se encuentre en almacenamiento,[319] no importando si está o no penada esta conducta, pues el

[319] Al decir cualquier tipo de información, me refiero a que en la actualidad dicho software -a reserva del nuevo programas llamado "Nero" el cual ya vimos sus características anteriormente- sólo hace la copia ilegal si no hay algún tipo de seguridad o medio de protección, y si lo hay simplemente no lo realiza señalando algún posible error, sin embargo podemos afirmar que muy pronto si no es que ya los hay en existencia, tengamos presente al software llamado "Nero"-, así que tendremos programas que no sólo traspasen esta seguridad sino que copiará todas las características que hacen original a un producto resultando de esto que no sea posible en algunos casos determinar cual es la copia y cual el original con todas las implicaciones económicas y jurídicas que representa esto.

proveedor, productor o inventor se escudaría y se escuda en que no se tipifica a esta conducta, diciendo que creó dicho software como un medio o herramienta de trabajo, mas no como un medio para crear o realizar ilícitos ya tipificados dentro de nuestro país y fuera de él, y no habría ni tendría responsabilidad alguna pues en el último de los casos él no realizó la conducta, pero sin embargo, sí facilitó, prestó, los medios para que esta conducta ilícita se llevara a cabo.

Es así como podemos comprender la propuesta de tipificación de la conducta de los sujetos o individuos conocidos como proveedores, diseñadores o inventores de programas de software, en cuanto que estos tienen una responsabilidad por poner a la venta programas que son diseñados "según ellos" para mejorar y hacer más fácil el trabajo de las personas que los usen. Sin embargo estos programas, si bien es cierto, que hacen más fácil la labor de los operadores o administradores que ocupan dicho software, también es cierto que traen consigo en una forma intrínseca y siendo parte importante de ellos, acciones que sirven para realizar actos que son o están tipificados como ilícitos; un claro ejemplo de esto es el programa "Nero" el cual ya se mencionó anteriormente, este programa es uno de tantos que hay en el mercado con un registro de autor en regla e igualmente con todos sus derechos y obligaciones en orden y, sin embargo no se les prohibe a las personas morales la creación de éstos y en el peor de los casos que se saquen a la venta con las características ya mencionadas, las cuales son en potencia un arma para realizar actos de piratería en manos de personas que no están capacitadas, así como aquellas que lo están.

Por lo anteriormente dicho se propone tipificar la conducta de los proveedores, creadores o inventores de

software o programas que faciliten la piratería o copia ilegal de software o programas de computadora.

Siguiendo con el tema, consideramos que dicha conducta se adapta a lo expresado en el Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la República en Materia de Fuero Federal, Título Primero, Responsabilidad Penal, Capítulo Primero, Reglas Generales sobre Delitos y Responsabilidad, Artículo séptimo, párrafo segundo, el cual señala: "En los delitos de resultado material también será atribuible el resultado típico producido al que omita impedirlo, si éste tenía el deber jurídico de evitarlo. En estos casos se considerará que el resultado es consecuencia de una conducta omisiva, cuando se determine que el que omite impedirlo tenía el deber de actuar para ello, derivado de una ley, de un contrato o de su propio actuar procedente".

Como podemos ver, hay y existe una responsabilidad por parte de los sujetos a tipificar por su conducta omisiva. Sin embargo, como no está regulada su conducta y la legislación que hay actualmente omite a estos sujetos de responsabilidad, no son castigados por la creación de software o programas que facilitan la realización de actos de piratería.

Consecuentemente, proponemos la creación en el Título Noveno, un capítulo tercero que lleve como título "De los Mecanismos de Seguridad Informática y Aplicaciones en los Software o programas", y un articulado que es el siguiente:

Artículo 211-bis-8. Comete el Delito de Facilitación de medios:

I.- Toda persona física o moral que omita proteger la creación de todo tipo de software o programas de cómputo.

II.- Toda persona física o moral, debidamente registrada como tal, que facilite la piratería de software o programas, creando para ello también software o programas dándoles un registro de derechos de autor, y que realicen materialmente o ayuden a realizar esta conducta ilícita, y que contenga los medios técnicos para violar los diversos sistemas de seguridad o de protección.

III.- Toda persona física o moral que invente, cree o diseñe un programa que facilite la copia ilegal de software, independientemente si es con fin de lucro o no.

Artículo 211-bis-9. Se impondrá prisión de uno a diez años y sanción de trescientos días multa, al que cometa alguna de las infracciones que señala el artículo anterior, si sus software no han salido al mercado.

Artículo 212-bis-10. Se aplicará la misma sanción del artículo anterior y el cierre de la empresa hasta en forma definitiva si el software ya salió a la venta o esta distribuido, según el caso.

Se puede justificar plenamente la intervención del Derecho Penal como instrumento para regular a este tipo de conductas, toda vez que se cumple con los requisitos necesarios para su correcta tipificación, es decir, la gravedad de la ofensa y la calidad del bien jurídico puesto en peligro o destruido, siendo éstos parte de los presupuestos definitorios de la misión del Derecho Penal.

Siguiendo el mismo sentido, la creación de un tipo penal nuevo se justifica con la protección de un bien jurídico que ha cobrado suma importancia con el desarrollo de las nuevas tecnologías, tanto el hardware como el software, así como aquellas que se relacionan con estos y

cuya afectación puede repercutir de manera directa en el desarrollo de los países tanto internamente como a nivel internacional, pues de no darle un tratamiento acertado a estas conductas pronto tendremos no sólo la realización de copias ilegales de software sino también de los códigos fuente y objeto de éstos, no teniendo más que reformarlos o reprogramarlos para evitar conflictos legales a nivel de propiedad intelectual.

CONCLUSIONES

PRIMERA. Referirnos a los delitos informáticos actualmente no es correcto, pues dichos delitos no se encuentran tipificados en nuestras leyes como tales.

SEGUNDA. Es importante tener presente los antecedentes de la Informática y las materias que se interrelacionan con ella, ya sea como parte interna de ésta o como ciencia que se considera iniciadora de la misma; y la interrelación que se da con el Derecho en cuanto a la regulación de las conductas negativas que se dan o pudieran darse en el transcurso y avance propio de la tecnología, pues de éstos podremos tener siempre antecedentes y herramientas idóneas para tomar decisiones mediatas y futuras para contrarrestar este tipo de ilícitos, y también respecto de aquellos que se relacionaren en un futuro próximo con los mismos, teniendo una capacidad de respuesta pronta ante cualquier nueva conducta delictiva; esto con el fin de que no se legisle de forma improvisada y sin tener los conocimientos necesarios para realizar una tipificación correcta y sin omisiones o faltas de conductas potencialmente delictivas, como la propuesta en la presente tesis.

TERCERA. Ante la innegable relación que se ha dado y existe entre la Informática y el Derecho, debemos tener presente todos aquellos que de alguna forma nos relacionamos con estas ramas ya como informáticos ya como abogados ya como juristas, etc., que no podemos hacer a un lado a esta relación pues es sólo el principio de un fenómeno que regirá las vidas y el trabajo de los seres humanos, y por lo tanto debemos de legislar y regular todas y cada una de las nuevas acciones o avances tecnológicos dentro de la informática, si no queremos vernos envueltos

muy pronto en un vacío legal para poder encuadrar y castigar las próximas conductas delictivas por nacer ante el irreversible avance informático.

CUARTA. Podemos deducir en sentido estricto y de la general a lo particular que sí existen los delitos informáticos, entendidos éstos como conductas típicas, antijurídicas y culpables que tengan como objeto la información almacenada en los equipos o sistemas informáticos. Por otro lado y en atención a la conducta que se propone tipificar y al bien jurídico que se trata de proteger, se justifica la existencia de un nuevo tipo penal con carácter autónomo de los tipos tradicionales.

QUINTA. Por la ubicación y composición de los nuevos tipos penales se puede desprender el reconocimiento, por parte del Congreso de la Unión, de una noción restringida de los delitos informáticos, es decir, *del modus operandi* y del *modus vivendi* del delincuente, de los medios físicos y materiales que utiliza el delincuente para poder realizar la conducta, haciendo especial mención de piratería.

SEXTA. En cuanto a la regulación que se ha hecho nacionalmente, podemos señalar que si bien ha sido un adelanto legislativo tenemos, por otra parte, que se han tipificado sólo aquellas conductas que se consideran más utilizadas, sin tomar en cuenta la base o herramienta que es fundamental en estos casos para la comisión de los delitos informáticos.

SÉPTIMA. Internacionalmente la cuestión se ha regulado en la forma que los diversos países consideran idónea desde el punto de vista territorial, económico e industrial, así como las condiciones específicas necesarias y oportunas para la correción, represión y eliminación de los delitos informáticos, considerando al último la relación que se tiene con otros países y que estos delitos por sus carac-

terísticas tecnológicas no respetan fronteras, dejando así al descubierto áreas que son de suma importancia para la eficaz lucha contra estos delincuentes cibernéticos, pues aunque hayan firmado acuerdos, tratados o convenios, estos países verán siempre por el cuidado de sus intereses y de sus grandes empresarios o corporativos, olvidándose de las obligaciones contraídas a nivel internacional.

OCTAVA. Los diversos países que han regulado estos delitos han optado por tipificar cada una de las conductas que comprenden la noción más amplia de los delitos informáticos, esto con el fin de que se tenga a la mano el medio por el cual se pueda tipificar toda posible acción delictiva en cualquier forma o medio donde participe algún medio informático.

NOVENA. La protección jurídica que se le ha otorgado al software ha sido principalmente dentro de la legislación sobre derechos de autor y en el Código Penal, desde la perspectiva que se ha manejado hasta nuestros días en cuanto a que se tipifica y castiga a los autores materiales que cometieron el delito. Con esto no quiero decir que no debe de ser así, pero se ha dejado a un lado la responsabilidad penal de los creadores, proveedores o inventores de programas de software, en cuanto a la facilitación de medios para la comisión de conductas delictivas.

DÉCIMA. El reconocimiento que se ha hecho a esta forma mediante la cual se facilitan los medios para la comisión de las conductas delictivas y especialmente la figura de piratería, ha sido nulo en nuestra doctrina y legislación nacional.

DÉCIMA PRIMERA. La criptología es hasta el momento la forma idónea, según los expertos, para proteger la información, y a la vez el principio de protección para todo tipo de software o programa, pero hemos visto

que esta es efectiva sólo si se tienen en forma segura las claves de este sistema; y por otro lado, también se pueden encontrar mediante diversas formas pues teniendo una computadora lo suficientemente rápida y eficiente no se necesita mucho tiempo para encontrar dicha clave de seguridad, traduciéndose esto en que no es un sistema seguro, ni puede haberlo pues al momento que sale un sistema de seguridad ya hay otro que sirve para traspasarlo.

DÉCIMA SEGUNDA. Las reformas propuestas al Código Penal encuentran su justificación en la calidad del bien jurídico y en la gravedad de su ofensa, es decir, en la necesidad de un nuevo tipo penal que responda a la exigencia de proteger un bien jurídico que ha cobrado vital importancia con el desarrollo de las nuevas tecnologías de la información -software y hardware-, cuya afectación repercute de manera directa en la vulneración de otros bienes jurídicos de gran importancia. Esto acorde al carácter fragmentario del Derecho Penal, si consideramos la gravedad de las consecuencias que traen aparejadas este tipo de conductas que facilitan los medios para cometer una conducta ilícita.

BIBLIOGRAFÍA

Award, Elías M. *Procesamiento automático de datos.* México. 1982.

Barriuso Ruíz, Carlos. *Interacción del Derecho y la Informática.* Dykinson. Madrid, 1996.

Beer Stafford. *Cibernética y Administración.* México. 1965.

Bruno Nedelec, Charles. Instituto de Nacional de Ciencias Penales. *Curso de Introducción a los Delitos Informáticos.* La Experiencia Francesa. México, julio 2000.

Bustos Ramírez, Juan J. y Hormazábal Malarée, Hernán. *Lecciones de Derecho Penal.* Trotta, Madrid. 1999.

Cámara de Diputados del H. Congreso de la Unión. *Derechos del pueblo mexicano. México a través de sus constituciones.* Porrúa, México, 2000, tomo III, artículos 12-23.

Castellanos Tena, Fernando. Concepto de Delito. *Antología Jurídica 1992-1996.* Consejo de Egresados de Posgrado en Derecho. Poder Judicial del Estado de Morelos. 1997.

Contreras Saldivar, Gabriel. *El Derecho Penal ante el Crimen Informático.* Escuela Libre de Derecho. México, 1999.

García Máynez, Eduardo. *Introducción al Estudio del Derecho.* Porrúa, México. 1997.

González Quintanilla, José Arturo. *Derecho Penal Mexicano.* Porrúa, México. 1997.

H. Sanders, Donal. *Informática Presente y Futuro.* Trad. Roberto Luis Escalona. Segunda Edición. McGraw-Hill. México. 1993.

Orjales, Rodolfo. Instituto Nacional de Ciencias Penales. *Curso de Introducción a los Delitos Informáticos. La Experiencia Estadounidense.* Computer Crime Intellectual Property Seccion (CCIPS). U.S. Dept. Justice. Washington D.C., México, julio 2000.

Rangel Medina, David. *Panorama del Derecho Mexicano.* MacGraw-Hill, México, 1998.

Riestra Gaytan, Emma. Instituto Nacional de Ciencias Penales. *Curso de Introducción a los Delitos Informáticos. La Experiencia Mexicana.* México, julio 2000.

Righi, Alberto / Fernández, Alberto A. *Derecho Penal. La Ley. El Delito. El proceso y la pena.* Hammurabi. S.R.L. Buenos Aires. 1996.

Ríos Estavillo, Juan José. *Derecho e Informática en México.* UNAM. 1997.

Téllez Valdés, Julio. *Derecho Informático.* Segunda Edición. McGraw-Hill, México.1996.

Zaffaroni, Eugenio Raúl. *Manual de Derecho Penal.* Parte general, 4ª reimpresión. Cárdenas Editor. México. 1998.

LEGISLACIÓN

Código Civil para el Distrito Federal. Porrúa 68ª Edición, 2000.

Código Penal para el Distrito Federal. Leyes y Códigos de México. Porrúa, 59ª edición, México, 2000.

Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal. Sista. 2000.

Código Penal y de Procedimientos Penales para el Estado de Sinaloa. Porrúa, tercera edición, 1997.

Constitución Política de los Estados Unidos Mexicanos. Secretaría de Gobernación. México, 5 de febrero de 2001.

Compilación Jurídica (CD-ROM). Secretaría de Gobernación. Julio 2000.

Legislación Sobre Derechos de Autor. Leyes y Códigos de México, 21ª edición, Porrúa, México, 1999.

Legislación Sobre Propiedad Industrial e Inversiones Extranjeras. Leyes y Códigos de México. 24ª edición, Porrúa, México, 1999.

HEMEROGRAFIA

Acedo Quezada, Octavio R. *Curso de Informática en las Escuelas de Derecho,* en Revista Tribunal, Poder Judicial de Jalisco, 1997.

Chávez, José Antonio. Periódico Reforma, *"Hackean" a Microsoft,* sección A, interface, Lunes 30 de octubre de 2000.

Cuadernos de Doctrina y Jurisprudencia Penal. Software: Reforma a la Ley de Propiedad Intelectual. A. Ley 25.036. Protección Penal del Software. Año 5, número 8 C, Adhoc-Buenos Aires. 1998.

De Rivera, Laura G. Guía Básica del Hacktivismo. Los Guerreros de la Red, en *Revista Milenio,* número 160. Octubre 2 de 2000.

Internet. *http://www.reforma.com/negocios_y_dinero/artículo/009049/.*

Internet. *Ingeniería en Cibernética ... y temas afines! http://www.mxl.cetys.mx/Escuelas/Ingenieria/alumnos/mo13645/ciber.htm.*

Marcelo A: Riquert. *Cuadernos de Doctrina y Jurisprudencia Penal.* Ley 25.036: Análisis de sus cláusulas sobre protección penal del software. Año 5, número 8 C, Adhoc-Buenos Aires. 1998.

Minguet Melián, Jesús Ma. "Criptología", en *Informática y Derecho, Revista Iberoamericana de Derecho*

Informático. Jornadas: Marco Legal y Deontológico de la Informática, actas Volumen I, UNED. Centro Regional de Extremadura. Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura- Mérida. 1998.

Monzón, Enrique. "El Hermano Grande nos Vigila", en *Periódico Tiempos del Mundo*, año2/número43/ (206), semana del 26 al 2 de noviembre del 2000.

Núñez Jiménez, José Manuel. "Valor Probatorio del Documento Electrónico. Su autenticidad a través de la Criptografía o Criptología como garantía del Documento Electrónico", en *Informática y Derecho, Revista Iberoamericana de Derecho Informático*. Jornadas: Marco Legal y Deontológico de la Informática, actas Volumen II, UNED. Centro Regional de Extremadura. Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura-Mérida. 1998.

Periódico Reforma. LINX. *"El mejor copiador de discos compactos"*, sección A, interfase. Lunes 5 de febrero del 2001.

Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura-Mérida. Informática y Derecho. *Revista Iberoamericana de Derecho Informático,* Jornadas Marco Legal y Deontológico de la Informática. Actas Volumen I. Mérida. 1998.

Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura-Mérida. Informática y Derecho. *Revista Iberoamericana de Derecho Informático,* Jornadas Marco Legal y Deontológico de la Informática. Actas Volumen II. Mérida. 1998.

DICCIONARIOS

De Pina Rafael / De Pina Vara Rafael. *Diccionario de Derecho*. Vigésimo tercera edición. Porrúa. México. 1996.

Díaz de León, Marco Antonio. *Diccionario de Derecho Procesal Penal y de Términos usuales en el Proceso Penal*. Porrúa, México, 1997, tomo I, tercera edición.

Diccionario Enciclopédico Larousse. Tercera edición, 1998.

Instituto de Investigaciones Jurídicas. *Diccionario Jurídico Mexicano*. Porrúa, novena edición, México, 1996.