UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN

LA NECESIDAD DE TIPIFICAR LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL FEDERAL DE LOS ESTADOS UNIDOS MEXICANOS

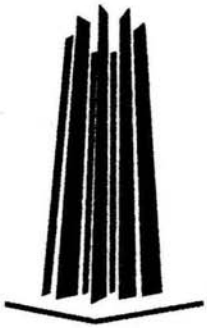
T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

P R E S E N T A:

NORMA ANGÉLICA OLVERA ALVARADO



ASESOR: LIC. JUAN JESÚS JUÁREZ ROJAS

MÉXICO 2004

AGRADECIMIENTOS:

A **DIOS**, por permitirme culminar otro peldaño de mi vida profesional y empezar otro con mayor fuerza que el anterior.

A la **UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO,** por medio de la **ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN**, por las facilidades otorgadas dentro de la **LICENCIATURA EN DERECHO**, a los catedráticos tan entregados a dar clases, más que con la sapiencia, con el corazón.

Al **LICENCIADO JUAN JESÚS JUÁREZ ROJAS**, por la paciencia y la dedicación, tanto en el aula como en el seminario.

A **MIS PADRES**, por siempre estar en el lugar y en el momento preciso para impulsarme a salir adelante; por todos sus desvelos, alegrías, enojos, y la gran herencia recibida en vida. **LOS QUIERO MUCHO**.

A **ERNESTO OTTO BELTRÁN CORIA Y ANDRÉS ALMONASÍ LOZANO** por su apoyo y amistad incondicional.

A **MIS AMIGOS;** Por que antes de entrar a la universidad me hubiera gustado saber.

1. Que puedo cambiar muchísimo y ni siquiera notarlo.
2. Que puedes querer a muchas personas de diferentes formas.
3. Que los niños de la universidad... también avientan papelitos y juegan cebollitas.
4. Que normalmente conoces ahí al amor de tu vida, al cual siempre recordarás, o tienes a tu lado.
5. Que si fuiste inteligente en la prepa. ¿Importa?, es pasado ¿no?
6. Que copiar puede ser sinónimo de verificar o corregir.
7. Que puedes estar en una fiesta la noche anterior del examen final.

8. Que si llevas una chamarra que te cubra completamente del frío, todos te preguntarán: ¿dónde cayó la nevada?

9. Que existen materias que requieren más tiempo que todas las clases juntas.

10. Que puedes saber todo y reprobar el examen.

11. Que puedes no saber nada y sacar una buena calificación.

12. Que la mayor parte de mi educación la obtuve fuera del salón de clases.

13. Que la casa es un gran lugar para visitar cuando hay exámenes.

14. Que es posible estar solo aun cuando estás rodeado de mil personas.

15. Que USTEDES tomaron caminos diferentes, pero nunca se olvidarán de la amistad.

16. Que quisiera volver a la Universidad, para volver a estar con ustedes y revivir tantas cosas bellas.

17. Que cada reloj en el campus tiene diferente hora.

18. Que USTEDES son quienes hicieron de la Universidad, un lugar valioso e importante.

19.-Que Valió la pena salirme de clases para apoyar a los Pumas Aragón en cada uno de sus partidos.

20.- Que la UNAM fue, es y seguirá siendo "NUESTRA MÁXIMA CASA DE ESTUDIOS"

Porque al pasar unos años después de graduarnos... tal vez no recordaré muy bien lo que aprendí en clases, pero siempre recordare todo aquello que viví con ustedes, con quienes estudie, me desespere, llore, grite y festeje, con quienes compartí todo mi tiempo...

"Quien logra hacer un amigo en la Universidad, logra hacer un amigo para toda la vida"

¡GOOYA! ¡GOOYA!

CACHUN CACHUN RA RA, CACHUN CACHUN RA RA,

¡GOOYA!

¡¡¡UNIVERSIDAD!!!

"POR MI RAZA HABLARÁ EL ESPÍRITU"

INTRODUCCIÓN

Los beneficios de los medios de comunicación y el uso de la informática en la sociedad actual son muchos, sin embargo, este trabajo trata de analizar las conductas delictivas, que llegaron junto con el avance tecnológico en el campo de la informática; y la manera en la que puede cometerse una conducta que vaya en contra del bienestar de la sociedad.

Dentro de este desarrollo tan amplio de la tecnología informática, se encuentra una gran desventaja, que es dar pie a conductas delictivas, que se presentan de manera que hasta algunos años atrás era imposible imaginar. Los computadores junto con la Internet, ofrece muchas posibilidades nuevas y muy complicadas de infringir la ley; o de cometer conductas que no están reguladas, dentro de la misma, es decir, se ha creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

Ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología; sin embargo es necesario tipificar y ampliar la regulación de las cada vez más frecuentes consecuencias del uso indebido de las computadoras, sistemas informáticos y el internet, se debe adecuar la tecnología a la realidad mexicana.

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

No existe un consenso en cuento al concepto de delito informático, y que estudiosos del tema lo han definido desde diferentes puntos de vista como son el

criminógeno, formal, típico y atípico, etcétera; dando lugar a que la denominación de esta conducta haya sufrido diferentes interpretaciones, señalando los sujetos, activos, pasivos, clasificación y los tipos de delitos informáticos considerados tanto en la doctrina como en la legislación de diferentes países.

Se estudia la problemática de los delitos informáticos en países de Europa y de América donde mayor incidencia ha tenido este fenómeno, el tratamiento penal que algunos gobiernos le han dado, y la parcial inercia que otros han mantenido sobre el tema, lo que se ha traducido en proyectos que hasta el momento no han fructificado.

Se analiza la regulación que han tenido en la legislación mexicana las conductas ilícitas relacionadas con la informática. Para ello estudiamos los antecedentes que a mi juicio han tenidos las regulaciones vigentes en esta materia: El Acuerdo General de Aranceles Aduaneros y Comercio y El Tratado de Libre Comercio de América del Norte.

Me detengo un poco en el tratamiento administrativo que se realiza a través de la Ley Federal del Derecho de Autor, como en el penal que se ha establecido en el Libro II, Título Noveno, Capitulo II del Código Penal Federal.

Finalizando con algunas consideraciones sustentadas en el estudio comparativo antes mencionado, ya que la finalidad primordial es la adecuación a la realidad existente en México, pero previendo que no estamos exentos de la velocidad del desarrollo tecnológico y de las exageraciones que éste genera.

LA NECESIDAD DE TIPIFICAR LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL FEDERAL DE LOS ESTADOS UNIDOS MEXICANOS

INTRODUCCIÓN

CAPÍTULO I

GENERALIDADES DE LA INFORMÁTICA.

Es necesario que en este capítulo se describan las bases de la Informática, los avances y su importancia, hasta llegar a diferenciar la cibernética con la informática, haciendo hincapié en la informática jurídica para facilitar la formación de un esquema meramente conceptual, para integrar conocimientos que se van adquiriendo; ya que sin ellos, sería muy difícil la comprensión de esta investigación.

El hombre se ha enfrentado a arduas tareas repetitivas, rutinarias, de cálculo y de gestión, entendiendo las primeras como todas aquellas operaciones con números, es decir, aritméticas, lógicas simples o un poco más complejas; y las segundas son aquellas que tienen como finalidad la recopilación de datos, tanto contables, administrativos, económicos, entre otros; como consecuencia se desarrollaron aparatos y herramientas para la realización de los mismos, hasta llegar a lo que ahora conocemos como las computadoras u ordenadores, que trajeron consigo una nueva ciencia para ayudar al hombre y a la sociedad, para hacer una gran variedad de cosas.

La palabra *informática*, "...abarca toda actividad relacionada de cualquier forma con los ordenadores..."[1], esto se debe a la gran funcionalidad de las computadoras, ya que ahora influyen en casi todos los aspectos de nuestras vidas,

---

[1] DUFFY Tim, Introducción a la Informática, traductor Eduardo de la Calle, Grupo Editorial Iberoamericana S. A. de C. V., México, Distrito Federal. Pp. 1-3.

provocando cambios en múltiples actividades de la sociedad. Este término se compone de la fusión de los términos **infor**mación y auto**mática**, se considera como información, "...ciencia del tratamiento lógico y automático de la información, principalmente a través de las computadoras..."[2]. Con ello podemos apreciar que es una transición de la sociedad, para simplificación del trabajo, por medio de un ordenador.

Esto trae consigo la rápida evolución y perfeccionamiento de las computadoras, dando un gran impulso a esta ciencia, hasta el punto en que las actividades, rubros y campos de la vida social, tales como la economía, política, cultura, el derecho, etcétera, experimentan los cambios en menor o mayor grado su transformación a la era de la informática. No se podría avanzar esta investigación, sin antes mencionar la diferencia entre los términos que muchos confunden: cibernética e informática. "...La cibernética designa a la nueva ciencia de la comunicación y control entre el hombre y la máquina..."[3], o sea, esta disciplina que dentro de su ámbito mantiene una relación hombre-ordenador como medio de comunicación; el control relacionado con el campo de estudio; su aparición se debe a tres factores primordiales:

a) Social: por requerimiento al aumento de producción.
b) Técnico-científico: la ciencia y la técnica se empezaron a reunir y lograron hacer una ciencia que facilitara su desenvolvimiento e interrelación.

---

[2] INSTITUTO DE INVESTIGACIONES JURÍDICAS, Enciclopedia Jurídica Mexicana, editorial Porrúa, UNAM, Tomo IV, Primera Edición, México 2002.
[3] BEER, Stafford. Cibernética y Administración. México, 1965, página 21

c) Histórico: para controlar y vincular a los demás.

Mientras tanto, la informática, se encarga de facilitar actividades, que la misma sociedad te exige a conocer, lo que antes era una opción se convierte en obligación, una ciencia de empleo racional, mediante máquinas automáticas, en base a conocimientos previamente adquiridos. Quedando claro este punto, se hace mención de algunas de las ventajas de la ciencia informática, con base en la sociedad:

- La necesidad de compilar grandes bancos de datos y su facilitación de procesamiento.
- Organización de datos comunes para múltiples procesos o distintas aplicaciones, evitando así el acumulamiento en el espacio físico y problemas de actualización.
- Precisión y rapidez en la realización de cálculos de cualquier tipo.
- Procesamiento de las mismas instrucciones, para diferentes datos. Como por ejemplo las nóminas de las empresas.
- Amplitud de posibilidades como:
    - ✓ La inteligencia artificial que se define como el razonamiento de ciertos procesos independientes que la computadora hace para la imitación más cercana de su comportamiento, es decir, respuestas muy cercanas a las humanas.
    - ✓ Visualización de imágenes con apariencia mas cercana a la real, que van de dos a tres dimensiones, modificación de tamaño, rotación de los

mismos, deformarlos, animación, imágenes digitales, entre muchas otras cosas más.

- ✓ Habilidad para recrear lugares físicos, y fenómenos con apariencia real, simulación de objetos, exploración de edificios, planetas y aviones.

Con estas aplicaciones nos damos cuenta de la infinidad de aplicaciones que se tienen por medio de las computadoras, sin embargo, a lo largo de esta investigación, con la utilización de Internet (que es de gran utilidad por ser un tema seminuevo); Enciclopedias Jurídicas, libros y revistas especializadas, que realmente son pocas; La falta de Tipificación en la Ley Penal Federal vigente en los Estados Unidos Mexicanos, y las tesis de algunos abogados que ya obtuvieron su título, se desentraña la identificación de los problemas relacionados con la informática, y con ello plantear una propuesta para la solución de los mismos.

1.1. ANTECEDENTES DE LA INFORMÁTICA.

Para continuar este apartado, tendremos que mencionar que a lo largo de la historia, se identifican muchos autores, y existe la controversia de que si fueron cuatro o cinco generaciones, para el fin primordial de esta investigación, se toma en cuenta las cinco generaciones, ya que se identifican varias tendencias que más adelante se precisarán.

A lo largo de la humanidad, el hombre se ha visto en la necesidad de cuantificar objetos, pertenencias, animales, etcétera, es decir, procesar datos; limitado por sus manos y su mente; esto fue evolucionando gracias a su ingenio, utilizando piedras, granos, u objetos similares.

El origen de las máquinas de calcular está dado por el ábaco chino, éste era una tablilla dividida en columnas en la cual la primera, contando desde la derecha, correspondía a las unidades, la siguiente a la de las decenas, y así sucesivamente. A través de sus movimientos se podía realizar operaciones de adición y sustracción. "...La palabra ábaco encuentra su raíz etimológica en la voz fenicia *abak* que significa "tabla lista y cubierta de arena"..." (Sic).[4]

Otro de los hechos importantes en la evolución de la informática lo situamos en el siglo XVII, donde el científico francés Blas Pascal inventó una máquina calculadora. "Ésta sólo servía para hacer sumas y restas, pero este dispositivo sirvió como base para que el alemán Leibnitz"[5], en el siglo XVIII, desarrollara una máquina que, además de realizar operaciones de adición y sustracción, podía efectuar operaciones de producto y cociente.

En el siglo XIX se comercializaron las primeras máquinas de calcular. En este siglo el matemático inglés Babbage desarrolló lo que se llamó Máquina Analítica, la cual podía realizar cualquier operación matemática. Además disponía de una

---

[4] Cfr. TELLEZ, Valdés Julio. Derecho Informático. Mc Graw Hill. 2ª edición. Página 6
[5] Cfr. http://www.geocities.com/ruben_apg/abacoalordenadorelectronico.htm, 17 de Octubre del 2003.

memoria que podía almacenar 1000 números de 50 cifras y hasta podía usar funciones auxiliares, sin embargo seguía teniendo la limitación de ser mecánica.

Recién en el primer tercio del siglo XX, con el desarrollo de la electrónica, se empiezan a solucionar los problemas técnicos que acarreaban estas máquinas, reemplazándose los sistemas de engranaje y varillas por impulsos eléctricos, estableciéndose que cuando hay un paso de corriente eléctrica será representado con un *1* y cuando no haya un paso de corriente eléctrica se representaría con un *0*.

Con el desarrollo de la segunda guerra mundial se construye el primer ordenador, el cual fue llamado Mark I y su funcionamiento se basaba en interruptores mecánicos. En 1944 se construyó el primer ordenador con fines prácticos que se denominó Eniac.

En 1951 son desarrollados el Univac I y el Univac II (se puede decir que es el punto de partida en el surgimiento de los verdaderos ordenadores, que serán de acceso común a la gente).

GENERACIONES

1° Generación: se desarrolla entre 1940 y 1952. Es la época de los ordenadores que funcionaban a válvulas y el uso era exclusivo para el ámbito

científico / militar. Para poder programarlos había que modificar directamente los valores de los circuitos de las máquinas.

2° *Generación:* va desde 1952 a 1964. Ésta surge cuando se sustituye la válvula por el transistor. En esta generación aparecen los primeros ordenadores comerciales, los cuales ya tenían una programación previa que serían los sistemas operativos. Éstos interpretaban instrucciones en lenguaje de programación (Cobol, Fortran), de esta manera, el programador escribía sus programas en esos lenguajes y el ordenador era capaz de traducirlo al lenguaje máquina.

3° *Generación:* se dio entre 1964 y 1971. En esta, se comienzan a utilizar los circuitos integrados; esto permitió por un lado, abaratar costos y por el otro aumentar la capacidad de procesamiento reduciendo el tamaño físico de las máquinas. Por otra parte, esta generación es importante porque se da un notable mejoramiento en los lenguajes de programación y, además, surgen los programas utilitarios.

4° *Generación:* se desarrolla entre los años 1971 y 1981. Esta fase de evolución se caracterizó por la integración de los componentes electrónicos, y esto dio lugar a la aparición del microprocesador, que es la integración de todos los elementos básicos del ordenador en un sólo circuito integrado.

5° Generación: va desde 1981[6] hasta nuestros días (aunque ciertos expertos consideran finalizada esta generación con la aparición de los procesadores Pentium, consideraremos que aun no ha finalizado) Esta quinta generación se caracteriza por el surgimiento de la PC, tal como se la conoce actualmente.

Dando las características principales de la historia de la informática, pasaremos a describir la evolución de los hackers entendiéndolas como personas que se dedican a entrar a husmear a nuestras computadoras caseras, o a diversas redes como la de los bancos, industrias, pequeñas y medianas empresas, entre otros.

1.1.1. LOS PRIMEROS HACKERS.

..."Todo comienza el 10 de marzo de 1876, aquel día, Alexander Graham Bell se convirtió en la primera persona que logró transmitir eléctricamente voz humana comprensible. Lo que ocurrió fue que el joven Profesor Bell, trabajando intensamente en su laboratorio de Boston, se echó ácido accidentalmente en los pantalones. Su ayudante, el Sr. Watson, oyó sus gritos de ayuda a través del audio-telégrafo experimental de Bell. Había surgido el teléfono..."[7]

La primera red telefónica fue creada en Boston, mayoritariamente creada entre gente interesada en la tecnología y gente con buena situación económica. Después,

---

[6] http://www.geocities.com/ruben_apg/losprimerosanos.htm, 22 de Diciembre del 2003.
[7] http://orbita.starmedia.com/fortiz/LasTelecomunicaciones/Tema01HistoriaDeLasTelecomunicaciones.htm, 29 de Diciembre del 2003.

la red telefónica se extendió a gran velocidad. Hacia 1890, cubría toda Nueva Inglaterra. Hacia 1893 se completaba la red de Chicago. Hacia 1897, cubría Minnesota, Nebraska y Texas. Hacia 1904 se extendía por todo el continente. Después de que las patentes exclusivas de Bell expiraran, empezaron a expandirse compañías telefónicas rivales por toda América. La compañía de Bell, American Bell Telephone, pronto tuvo problemas.

En 1907, American Bell Telephone cayó en poder del siniestro cártel financiero J. P. Morgan, tiburones especuladores que dominaban Wall Street. La nueva dueña de Bell, American Telephone and Telegraph o AT&T, puso al frente de aquella a un nuevo hombre, un visionario industrial llamado Theodore Vail. Vail, un antiguo funcionario de Correos, era capaz de comprender el funcionamiento de una gran organización y tenía un sentido innato para comprender la naturaleza de la comunicación a gran escala. Vail se ocupó rápidamente de que AT&T se hiciera con la tecnología punta de nuevo.

El tipo de cable conocido como loading coil de Pupin y Campbell y el audion de Forest son tecnologías que han desaparecido hoy en día, pero en 1913 dieron a la compañía de Vail las mejores líneas de *larga distancia* que jamás se hubieran construido. Con el control de la larga distancia - los enlaces entre y a través de las más pequeñas compañías locales AT&T rápidamente llevó la voz cantante y empezó a devorarlas a diestro y siniestro.

AT&T al principio no dio empleo a mujeres para conseguir la liberación femenina. AT&T hizo esto por importantes razones comerciales. Los primeros operadores telefónicos del sistema Bell no fueron mujeres, sino adolescentes americanos. Eran chicos encargados de transmitir mensajes en el telégrafo (un grupo a punto de volverse técnicamente obsoleto), que hacían la limpieza de la oficina telefónica, iban a reclamar los pagos no abonados por los clientes, y hacían conexiones telefónicas en la centralita, todo por poco dinero.

Los chicos eran muy groseros con los clientes contestaban mal, con descaro, haciendo observaciones impertinentes. Esta combinación de poder, habilidades técnicas y total anonimato parece que actuó como un fuerte estimulante entre los adolescentes. Pero el fenómeno de chicos locos en los cables no se limitó a los Estados Unidos; desde el principio, ocurrió lo mismo en el sistema telefónico británico.

Así, los chicos fueron apartados del sistema, o al menos, privados del control de la centralita. Pero el espíritu aventurero e inquisitivo de los adolescentes volvería a aparecer en el mundo de la telefonía una y otra vez.

Algunas décadas después surgirían los primeros hackers de computadoras auténticos, en los años 60's en ese entonces existían programadores, que se distinguían de los demás por su creciente curiosidad de saber como funcionaban las

cosas, en aquellos días las computadoras eran enormes "mainframes",[8] encerradas en habitaciones con la temperatura controlada, en ese entonces compilar un programa además de ser muy tardado era altamente costoso, así los programadores tenían un acceso limitado a estos dinosaurios, sin embargo los mas listos crearon lo que llamaron hacks atajos en los programas para completar la ejecución mas rápidamente, muchas veces estos atajos eran mas eficientes y elegantes que el programa original.

Tal vez el mejor hack que se haya hecho fue desarrollado por dos empleados de Bell labs en 1969, Dennis Ritchie y Ken Thompson quienes crearon un nuevo sistema operativo, lo llamaron **UNIX**.

Las raíces genuinas del moderno hacker underground seguramente se pueden buscar de forma más exitosa en un tipo de movimiento hippie anarquista de finales de los 60's, "conocido como los yippies".[9]

Los dos yippies más activos eran Abbie Hoffman y Jerry Rubin. Rubin acabó convirtiéndose en un broker de Wall Street. Hoffman, buscado constantemente por las autoridades federales, estuvo escondido durante siete años en México, Francia y los Estados Unidos. Mientras estaba oculto, Hoffman continuó escribiendo y publicando, con la ayuda de simpatizantes en el underground americano anarquista de izquierdas. Durante buena parte de su tiempo, Hoffman sobrevivió gracias a

---

[8] A los Mainframes también se les conoce con el nombre de grandes ordenadores. Se dedican principalmente a la gestión, pudiendo realizar muchos trabajos a la vez. Una de sus aplicaciones puede ser controlar la red de cajeros automáticos de un Banco. El mainframe será capaz de gestionar la información de todos los cajeros conectados a él.

[9] El movimiento estudiantil europeo inspirado bajo la influencia de Marshall Mcluhan, con su «el medio es el mensaje»

tarjetas de identidad falsas y trabajos atípicos. Finalmente, se hizo la cirugía facial plástica y adoptó una personalidad totalmente nueva como Barry Freed.

Le encantaba participar activamente en manipular la televisión por cable y otros medios hambrientos de imágenes. Mediante mentiras estrambóticas, rumores alucinantes, suplantaciones de personalidad y otras siniestras distorsiones con la garantía de que todas ellas molestarían a la policía, los candidatos presidenciales y los jueces federales. El libro más famoso de Hoffman era el libro conocido como roba este libro, que divulgaba un conjunto de métodos mediante el que los jóvenes agitadores hippies sin dinero podrían buscarse la vida en un sistema mantenido por androides sin humor. Roba este libro, cuyo mismo título urgía a sus lectores a dañar el propio medio de distribución que lo había puesto en sus manos, podría describirse como el antecesor espiritual de un virus informático.

Hoffman, como muchos otros conspiradores de última hora, hizo extensivo el uso de teléfonos de pago para su campaña de agitación, en su caso utilizando chapas baratas de metal como monedas falsas.

Durante la guerra del Vietnam, había un impuesto extra sobre el servicio telefónico; Hoffman y sus cohortes podían, y de hecho lo hacían, argumentar que al robar sistemáticamente servicio telefónico estaban activamente implicados en desobediencia civil, negando virtuosamente financiar mediante los impuestos telefónicos una guerra inmoral e ilegal.

Pero este débil velo de decencia cayó rápidamente. *Destripar al Sistema* encontró su propia justificación en la profunda alienación y una repugnancia del fuera de ley por los valores convencionales de la burguesía. Estos principios podrían describirse como anarquía por conveniencia y se hicieron muy populares entre el propio movimiento yippie, y ya que destripar es tan útil, sobrevivió el mismo movimiento.

A principios de los setenta, se requería una experiencia bastante limitada e ingenuidad para hacer trampa en los teléfonos de pago, obtener electricidad o gas gratis o robar en máquinas distribuidoras o parquímetros para tener algo de líquido. También se necesitaba una conspiración para extender ese movimiento, y el valor y el nervio para cometer pequeños hurtos, pero los yippies tenían una nota alta en todo eso.

En junio de 1971, Abbie Hoffman y un entusiasta del teléfono conocido sarcásticamente como Al Bell empezaron a publicar un boletín de noticias conocido como Party Line de la Juventud Internacional (*the youth international party line YIPL-TAP*). Este boletín estaba dedicado a reunir y divulgar las técnicas yippies de destripar, especialmente los teléfonos, ante la alegría del underground de espíritu libre y la rabia insensata de la gente normal.

En tanto que táctica política, el robo de servicio telefónico aseguraba que los defensores de los yippies siempre tendrían acceso inmediato a las llamadas de larga

distancia como medio, a pesar de la falta crónica de organización, disciplina o dinero de los yippies, por no decir de una dirección fija.

Party Line estaba dirigida desde Greenwich Village durante un par de años, pero entonces Al Bell desertó más o menos de las filas del yippismo y cambió el nombre del boletín por TAP o Technical Assistance Program. Una vez finalizada la guerra del Vietnam, el vapor empezó a escaparse de la disidencia americana radical. Pero en aquel entonces Bell y más o menos una docena de colaboradores habituales habían cogido el bit por los cuernos y habían empezado a generar una satisfacción interna tremenda ante la sensación de puro poder técnico. Los artículos en TAP, antes altamente politizados, se fueron convirtiendo en más técnicos, en homenaje o parodia a los propios documentos técnicos del sistema de Bell, que TAP estudiaba con detalle, interiorizaba y reproducía sin permiso. La élite de TAP estaba en posesión del conocimiento técnico necesario para golpear al sistema.

Al Bell dejó el juego a finales de los setenta, y lo substituyó Tom Edison; los lectores de TAP (entre todos, unos 1400) en los interruptores del telex y el fenómeno creciente de sistemas de ordenadores. En 1983, a Tom Edison le robaron su ordenador y algún imbécil quemó su casa. Era un golpe mortal para TAP.

Desde el primer momento en el que los teléfonos empezaron a ser rentables, ha habido gente interesada en defraudar y robar a las compañías telefónicas. Existen legiones de insignificantes ladrones telefónicos que superan con creces el número de phone phreaks que exploran el sistema por el simple reto intelectual.

Debido a que la red telefónica es anterior a las redes de ordenadores, el colectivo formado por los phone phreaks es anterior a los hackers. En la práctica, hoy en día la línea que separa el phreaking y el hackear está muy difuminada, al igual que la que separa a los teléfonos y los ordenadores. El sistema telefónico ha pasado a ser digital, y los ordenadores han aprendido a hablar a través de las líneas telefónicas. Y lo que es peor y ésta era la clave de los argumentos defendidos por el Servicio Secreto de los Estados Unidos algunos hackers han aprendido a robar, y algunos ladrones han aprendido a hackear.

En la segunda década de los ochenta, hasta la introducción de medidas de seguridad más fuertes en las telecomunicaciones, el robo de códigos utilizando ordenadores funcionó sin problemas, y fue algo casi omnipresente en el underground digital formado por phreaks y hackers. Se realizaba probando aleatoriamente con un ordenador códigos en un teléfono hasta que se daba con uno correcto. Había a disposición del mundo este underground, programas simples que podían hacer esto; un ordenador que permaneciera funcionando durante toda la noche podía obtener aproximadamente una docena de códigos correctos. Este proceso podía repetirse semana a semana hasta que se conseguía una gran biblioteca de códigos robados.

Antes de que los ordenadores y los módems llegaran masivamente a los hogares americanos, los phreaks disponían de su propio dispositivo de hardware especial, la famosa blue box (caja azul). Este dispositivo utilizado para el fraude (hoy en día cada vez menos útil debido a la evolución digital del sistema telefónico) podía engañar a las centrales de conmutación consiguiendo acceso gratuito a las líneas de

larga distancia. Lo hacía imitando una señal del propio sistema telefónico, un tono de 2600 hertzios.

Steven Jobs y Steve Wozniak, los fundadores de Apple Computer Inc., se dedicaron en su día a vender cajas azules en colegios mayores de California. Para muchos, en los primeros tiempos del phreaking, el uso de una caja azul era apenas considerado un robo. Alrededor de 1971 un veterano de Vietnam, John Draper, descubrió que un juguete que venia de regalo en las cajas de cereal de Capitan Crunch, podía reproducir perfectamente un sonido de 2600 hertzios, simplemente soplando a través de el, se podía engañar a la central telefónica y hacer llamadas gratis, a John Draper (mejor conocido como Cap'n Crunch) se le considera el padre del phreacking.

1.2. CONCEPTOS DE LOS DELITOS INFORMÁTICOS.

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

En nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se

han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que Julio Téllez Valdés señala que "...no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión delitos informáticos esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún..."[10]. Aunque menciona que no es una labor fácil dar un concepto de delitos informáticos; este trabajo, sostiene que no están contempladas en textos jurídicos, y es el objetivo primordial dentro de esta investigación, que se encuentre dentro del Código Penal Federal de los Estados Unidos Mexicanos; basándose en legislaciones de otros países, para que no haya ninguna dificultad en denominarlas, ya que en el antiguo Código Penal para el Distrito Federal del 2 de Enero de 1931, en su artículo 7°, que a la letra dice: "Delito es el acto u omisión que sancionan las leyes penales...", por lo consiguiente que si lo contempla en una ley penal, estaríamos hablando de delito; y el término informático, se deriva de que son medios electrónicos o informáticos por los que se cometen delitos de una forma no convencional.

[10] Cfr. TELLEZ Valdés, Op. Cit. Página 103

Para Carlos Sarzana, en su obra Criminalitá e tecnologia, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo"[11]. En esta definición, se involucra un término de Criminología, sin embargo en nuestra legislación, es el lenguaje más sencillo; solo tomaremos que la computadora está involucrada, sin embargo; hay que considerar la idea que es solo un medio, por que el individuo que conoce de la informática es la persona que comete la destrucción, alteración, sustracción de dinero, información entre muchas otras cosas.

Nidia Callegari define al delito informático como "...aquel que se da con la ayuda de la informática o de técnicas anexas..."[12]. La autora en su artículo dentro de la Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Boliviana, no determina que son las técnicas anexas, pero podemos tomar en cuenta que la persona que comete las acciones multicitadas, tiene conocimientos de programación, de Internet, de redes, de métodos de seguridad establecidos dentro de un sistema o red informática, técnicas de cracker, mainframes, virus, gusanos, y bombas lógicas.

Rafael Fernández Calvo define al delito informático como "...la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se

---

[11] Cfr. SARZANA, Carlo. "Criminalitá e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2. Roma, Italia.

[12] Cfr. CALLEGARI, Lidia. "Delitos Informáticos y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No 70 julio- agosto-septiembre. 1985. página 115.

ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título I de la constitución española..."[13].

María de la Luz Lima dice que "...el delito Electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin..."[14].

Julio Téllez Valdés define al delito informático en forma típica y atípica, entendiendo por la primera a "...las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y por las segundas actitudes ilícitas en que se tienen a las computadoras como instrumento o fin..."[15].

Por otra parte, se debe mencionar que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como delitos informáticos, delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora, delincuencia relacionada con el ordenador, como necesidad para la regulación y la necesidad de tipificar estas conductas antisociales que deben ser castigadas con el rigor de la ley.

---

[13] Cfr. FERNÁNDEZ Calvo, Rafael. "El tratamiento de llamado "delito informático" en el proyecto de Ley Orgánico del Código Penal: reflexiones y propuestas de la Comisión de Libertades e Informática" en Informática y Derecho. Página 1150

[14] Cfr. LIMA DE LA LUZ, María. "Delitos Electronicos" en Criminalia. Mexico. Academia Mexicana de Ciencias Penales. Editorial Porrúa. No 1-6. Año L. Enero Julio 1984. página 100

[15] Cfr. TELLEZ Valdés, Julio. Op. Cit. Página 104

En este orden de ideas, en el presente trabajo se entenderán como delitos informáticos todas aquellas conductas antisociales susceptibles de ser sancionadas por las leyes penales, por hacer uso indebido de cualquier medio informático.

Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes en México debido a que la legislación se refiere a normas de comercio, derechos de autor y propiedad intelectual sin embargo, deberá tenerse presente que lo propuesto al final de este trabajo tiene por objeto la regulación penal de aquellas actitudes antisociales que se estiman graves, hechas de una manera nada convencional, y con el fin de evitar su impunidad.

1.2.1. SUJETO ACTIVO.

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

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de

los cometidos. De esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

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

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

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

Asimismo, este criminológico estadounidense dice que tanto la definición de los delitos informáticos como las de los delitos de cuello blanco no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Hay dificultad para elaborar estadísticas sobre ambos tipos de delitos. La cifra negra es muy alta; hay dificultades para descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos respetables otra coincidencia que tiene estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Por nuestra parte, se considera que a pesar de que los delitos informáticos no poseen todas las características de los delitos de cuello blanco, si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objetos de un estudio más profundo, y dado el objeto de esta investigación se ve limitada.

1.2.2. SUJETO PASIVO.

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

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

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

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, debemos destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

1.3. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

Julio Téllez Valdés clasifica a los delitos informáticos base a dos criterios: como instrumento o medio, o como fin u objetivo.

- Como instrumento o medio: se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.
- Como medio y objetivo: en esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.[16]

María de la Luz Lima, presenta una clasificación, de lo que ella llama delitos electrónicos, diciendo que existen tres categorías, a saber:

- ❖ Los que utilizan la tecnología electrónica como método;
- ❖ Los que utilizan la tecnología electrónica como medio; y
- ❖ Los que utilizan la tecnología electrónica como fin.

- Como método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
- Como medio: son conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.
- Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla[17].

---

[16] Cfr. TELLEZ Valdés, Julio. Op. Cit. Página 105
[17] Cfr. LIMA DE LA LUZ, María. Op. Cit. 100 y 101

CAPÍTULO II

TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR LA ORGANIZACIÓN DE LAS NACIONES UNIDAS.

Para profundizar en este tema, es importante resaltar donde surgió la Organización de las Naciones Unidas, su objetivo, sus precursores, los organismos que son encargados de velar por este tema tan importante, para el amplio mundo de la tecnología.

El nombre de Naciones Unidas, acuñado por el Presidente de los Estados Unidos Franklin D. Roosevelt, se utilizó por primera vez el 1° de enero de 1942, en plena segunda guerra mundial, cuando representantes de 26 naciones aprobaron la "Declaración de las Naciones Unidas", en virtud de la cual sus respectivos gobiernos se comprometían a seguir luchando juntos contra las Potencias del Eje.

Las primeras organizaciones internacionales establecidas por los Estados tenían por objeto cooperar sobre cuestiones específicas. La Unión Internacional de Telecomunicaciones fue fundada en 1865 bajo la denominación de Unión Telegráfica Internacional, y la Unión Postal Universal se creó en 1874. Hoy día son organismos especializados de las Naciones Unidas.

En 1899 se celebró en La Haya la primera Conferencia Internacional de la Paz con el objeto de elaborar instrumentos que permitieran resolver pacíficamente las crisis, evitar la guerra y codificar normas de conducta en tiempo de guerra. La Conferencia aprobó la Convención para el arreglo pacifico de los conflictos internacionales y estableció la Corte Permanente de Arbitraje, que comenzó a operar en 1902.

El precursor de las Naciones Unidas fue la Sociedad de las Naciones, organización concebida en similares circunstancias durante la primera guerra mundial y establecida en 1919, de conformidad con el Tratado de Versalles, "para

promover la cooperación internacional y conseguir la paz y la seguridad". También en el marco del Tratado de Versalles se creó la Organización Internacional del Trabajo como organismo afiliado a la Sociedad de las Naciones. La Sociedad de las Naciones cesó su actividad al no haber conseguido evitar la segunda guerra mundial.

En 1945, representantes de 50 países se reunieron en San Francisco en la Conferencia de las Naciones Unidas sobre Organización Internacional, para redactar la Carta de las Naciones Unidas. Los delegados deliberaron sobre la base de propuestas preparadas por los representantes de China, la Unión Soviética, el Reino Unido, y los Estados Unidos en Dumbarton Oaks, Estados Unidos, entre agosto y octubre de 1944. La Carta fue firmada el 26 de junio de 1945 por los representantes de los 50 países. Polonia, que no estuvo representada, la firmó mas tarde y se convirtió en uno de los 51 Estados Miembros fundadores.

Las Naciones Unidas empezaron a existir oficialmente el 24 de octubre de 1945, después de que la Carta fuera ratificada por China, Francia, la Unión Soviética, el Reino Unido, los Estados Unidos y la mayoría de los demás signatarios. El Día de las Naciones Unidas se celebra todos los años en esa fecha.

Los llamados delitos informáticos, que como menciona Julio Téllez Valdés, para hablar de ellos, deben de estar tipificadas en textos jurídicos, o en su defecto en Códigos Penales, y que en nuestro país no ha sido objeto de legislación federal.[18]

Es menester de esta propuesta definir cada uno de los tipos de delitos que se pueden cometer por medio de una computadora, basándonos en los reconocidos por la Organización de las Naciones Unidas; y señalando los que de manera tradicional, están regulados por el Código Penal Federal de los Estados Unidos Mexicanos, para la debida comprensión de este capítulo.

---

[18] Cfr. TÉLLEZ VALDÉS, Julio. Op. Cit. Página 103.

Cabe mencionar que no hay un organismo especializado en el tema, sin embargo se puede mencionar que la Organización Mundial de la Propiedad Intelectual, ya que su objetivo principal es: "...mantener y mejorar el respeto por la propiedad intelectual en todo el mundo. Esto significa que se debe evitar la erosión de la protección existente y que tanto la adquisición de la protección, como su aplicación práctica, una vez adquirida, deben ser más sencillas, económicas y seguras..."[19]. De tal objetivo se deriva que se debe proteger todo aquello es de propiedad intelectual, industrial, etcétera, obviamente de los países contratantes. De los cuales México, si lo es.

2.1. FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS.

Fraude "proviene del latín *fraus, udis*, *fraudis*, que es genitivo de *fraus* y que significa engañar, usurpar, despojar... y gramaticalmente es engaño o acción contraria a la verdad o rectitud"[20]. Ahora para profundizar en este tema, se entenderá como el engaño mediante un conocimiento avanzado de informática, utilizando como medio un ordenador o una computadora.

Infinidad de casos alrededor del mundo, han orillado a reconocer tales conductas como delitos informáticos, por la Organización de las Naciones Unidas. [21]

Desde el momento en que se realiza una acción que reúna las características que delimitan el concepto de delito, y sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea de hardware o de software, estamos en presencia de un delito informático.

Estos delitos pueden adoptar alguna de las siguientes formas:

- Robos, hurtos, vaciamientos, desfalcos, estafas o fraudes

---

[19] Cfr. http://www.wipo.int/about-wipo/es/dgo/pub487.htm, 03 de Febrero del 2004.
[20] INSTITUTO DE INVESTIGACIONES JURÍDICAS, Enciclopedia Jurídica Mexicana, editorial Porrúa, UNAM, Tomo II, Primera Edición, México 2002.
[21] Cfr. http://www.apc.org/espanol/rights/lac/docs.shtml?-1-'Privacidad', 24 de Febrero del 2003.

cometidos mediante manipulación y uso de computadoras

- Apropiación no autorizada de los datos de entrada o de salida
- Cambios no autorizados en programas- que consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas
- Sabotaje informático
- Falsificaciones informáticas
- Violación de la privacidad
- Interceptación de comunicaciones
- Robo de servicios- se alude a las conductas que tienen por objeto el acceso ilícito a los equipos físicos o a los programas informáticos, para utilizarlos en beneficio del delincuente
- Hurto por transacciones electrónicas de fondos- Hurto que se comete mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o también cuando se viola el empleo de claves secretas
- Robos de hardware

Tradicionalmente, las organizaciones han confiado en el sistema de control interno como la herramienta para prevenir y detectar el fraude, incluyendo las auditorías internas sobre los procesos del negocio. Sin embargo, el mejor sistema de control interno no evita que el fraude ocurra. De acuerdo con las estadísticas de la Asociación de Examinadores de Fraudes Certificados de Argentina[22], sólo la mitad de los fraudes son descubiertos por el sistema de control interno o por auditores internos o externos. El resto de los fraudes es detectado por accidente o por denuncias de empleados o terceros. Se produce cuando con ánimo de lucro, para sí

[22] Cfr. http://www.kpmg.com.ar/services/services_fraud.html, 23 de marzo del 2004.

o para un tercero, mediante cualquier manipulación o artificio tecnológico semejante de un sistema o dato informático, procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. El fraude informático, hipótesis en la cual se utiliza el medio informático como instrumento para atentar contra el patrimonio de un tercero

2.1.1. MANIPULACIÓN DE LOS DATOS DE ENTRADA.

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

2.1.2. LA MANIPULACIÓN DE PROGRAMAS.

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

Otro caso muy difícil de descubrir y a menudo pasa inadvertida debido a que el sujeto activo en este caso debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado **Caballo de Troya,** que consiste en insertar

instrucciones de computadora en forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. El nombre se debe al episodio de la Ilíada de Homero, Ulises urdió una estratagema en virtud de la cual le regala a los troyanos un gran caballo de madera, que en el interior ocultaba soldados, haciendo creer que el ejército griego abandonaba el sitio de la ciudad. El caballo entró en el recinto amurallado de Troya y aprovechando la noche y la confianza de los habitantes, los guerreros ocultos hicieron entrar a las tropas griegas que aguardaban en las puertas de la ciudad.

2.1.3. MANIPULACIÓN DE LOS DATOS DE SALIDA.

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica del salchichón en la que rodajas muy finas apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2.2. FALSIFICACIONES INFORMÁTICAS.

Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando surgieron en el mercado impresoras y fotocopiadoras computarizadas en color a base a tecnología láser, chorro de tinta o

impresión a burbujas, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas impresoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo expertos puede diferenciarlos de los documentos auténticos.

2.2.1. COMO OBJETO.

En la mayoría de las empresas, instituciones bancarias y entre muchas empresas que venden productos y ofrecen sus servicios, y no hay quien los asesore, ante los daños que pueden tener por medio de internet o el correo electrónico, ya que en México hay muy pocas compañías las que se dedican a la seguridad informática. Es por esto que una de sus características principales es cuando se alteran datos de los documentos almacenados en forma computarizada.

2.2.2. COMO INSTRUMENTOS.

Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

2.3. DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS.

Estas figuras delictivas son previamente calificadas según el perjuicio causado, el papel que el computador desempeñe en la realización del mismo, el modo de actuar, el tipo penal en que se encuadren, y el tipo de actividad que

implique según los datos involucrados. Como instrumento o medio- conductas criminógenas que se valen de las computadoras, como método, medio, o símbolo en la comisión del ilícito; ejemplo de esto es: las falsificaciones de crédito, billetes, documentación oficial, acceso no autorizado, destrucción de datos, violación de derecho de autor, interceptación de correos electrónicos, estafas electrónicas. Pudiendo apreciar en ellos el elemento común el atentado a la propiedad electrónica.

Como fin u objetivo- conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como cosa material. Especificaremos que la afectación a lo material parte del elemento que exista de índole informática y constituya una perdida valiosa; La referencia a los programas es desde el punto de vista en que estos sean los medios que se utilicen para dañar la base de datos, que es generalmente el objetivo final de los comisores, de la cual pueden percibir beneficios lucrativos. Ejemplo aquí son los Crackers y los Hackers quienes han revolucionado los programas de seguridad. Estos sujetos generalmente cuando se producen los delitos informáticos suelen aparecer como el centro de atención tanto de rebote como por ser efectivamente los responsables del supuesto penal del que se trate. También podemos apreciar la ingeniería social la cual consiste en un arte de convencer a la gente de entregar información que en circunstancias normales no entregaría; así como la distribución de virus a la cual haremos referencia más delante, entre otras conductas.

Es de conocimiento de todos que estas acciones son llevadas a cabo por personas que posee conocimientos especiales respecto al tema, por lo que es obvio que se produzcan como consecuencia de estos actos perjuicios más graves, que pueden incluso repercutir desfavorablemente contra terceros, personas que estén ajenas alas ilegalidades que se cometan

Posee un bien jurídico el cual es atacado por el delincuente que se apellida informático, la calidad, pureza e idoneidad de la información en toda su amplitud, o sea su naturaleza, entendiéndolo como un todo, en la seguridad de la información

contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación, o sea su titularidad, integridad, autoría, disponibilidad, seguridad, transmisión, confidencialidad; sin perjuicio que con su ataque afecte otros bienes jurídicos como la intimidad o la propiedad.

Así mismo, aceptamos que las sanciones impuestas a tales hechos están acorde al carácter real de peligrosidad que tienen intrínsicamente con la visión futura de los resultados que traería llevar a vías de hecho una acción de esta índole en cualquiera de las ramas sociales o hacia cualquier persona si de violación de la intimidad se tratase. Teniendo que la acción sancionable estará más allá de un actuar o un no actuar, enmarcada en la intención del comisor, su dolo. Posee sujetos, quiénes llevan a cabo la acción debiéndosele sancionar por su conducta antijurídica y socialmente peligrosa, y otros que son los afectados por la acción. Dichos sujetos pueden ser tanto personas naturales como personas jurídicas.

2.3.1. SABOTAJE INFORMÁTICO.

"...Un sabotaje informático puso en peligro la vida de una tripulación de la NASA

La vida de varios astronautas de la NASA estuvo en peligro por culpa de un hacker. Según ha revelado la televisión inglesa BBC, en 1997, durante una de las misiones del transbordador espacial Atlantis en la estación Mir, un pirata informático bloqueó las comunicaciones entre el control central de Houston y el transbordador. El sabotaje fue crítico, ya que se produjo en un momento muy delicado: cuando el Atlantis maniobraba para acoplarse a la Mir. Por suerte la NASA pudo recuperar el contacto con la tripulación del transbordador por medio de los sistemas de comunicación de estación orbital rusa.

La agencia espacial estadounidense ha admitido este episodio que pone de manifiesto la fragilidad de sus sistemas ante los piratas de la red. La Nasa es, para los hackers, como el Everest para los alpinistas: el objetivo número uno. La agencia

espacial, para protegerse, cuenta con su propio equipo de "ciberdetectives", aunque reconocen que se encuentran saturados. Sólo en el año pasado, los ordenadores de la NASA registraron cerca de medio millón de ataques informáticos..."[23]

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

2.3.2 VIRUS.

Por concepto: "es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya"[24].

El primer virus se le escapo a alguien o **lo soltó** deliberadamente en la red, causando un colapso en las comunicaciones. Se trataba de un worm o gusano, el cual más adelante se hará mas preciso su estudio. El creador se sorprendió de sus efectos y tuvo que crear otro programa que anulara las funciones del primero. Así nació también el primer antivirus.

Los virus son la principal amenaza en la Red. Son programas de extensión relativamente pequeña, son programas capaces de autoaplicarse o dicho de otra manera, son capaces de hacer copias de si mismo en otro archivo al que ocupa. Este método bloquea y llena el disco duro de una computadora.

Otros virus además poseen funciones de modificaciones en los principales ficheros del sistema operativo de nuestro ordenador, los hay benignos, que solo muestran mensajes en la pantalla. Nos detendremos a estudiar los diferentes tipos

---

[23] http://es.gsmbox.com/news/mobile_news/all/3689.gsmbox, 22 de marzo del 2004.
[24] HERNÁNDEZ Claudio. Hackers Los piratas del Chip y de Internet. Página 86. (Sin Pie de Imprenta)

de virus y analizaremos algunos de ellos, estos poseen un Proceso de creación, incubación y reproducción:

a) La vida de un virus: el virus se crea o nace, esta claro en el ordenador como subprograma o microprograma ejecutable. Después este se "suelta" en la Red, se copia, se inserta dentro de un programa comercial de gran difusión, para asegurar un contagio rápido y masivo.

b) El contagio: Es la parte más fácil del ardua proceso. El virus debe ir incrustado en un archivo de instalación o en una simple página Web a través de los cookies. Las vías de infección son también principalmente los disquetes, programas copiados, Internet y correo electrónico.

c) La incubación: El virus permanece escondido reproduciéndose en espera de activarse cuando se cumplan las condiciones determinadas por el creador del virus. Este proceso varía según el tipo de virus.

d) La Replicación: Consiste en la producción del propio virus de una copia de si mismo, que se situará en otro archivo distinto al que ocupa, de esta forma el virus se contagia en otros archivos y otros programas, asegurándose de que el proceso de multiplicación sea asegurado, extendiéndose a otros ordenadores y debe hacerlo de la forma más discreta y rápida posible.

e) El Ataque: Cuando se cumplen las condiciones, efectuadas por el creador del virus, este entra en actividad destructora. Aquí es donde formatea el disco duro o borra archivos con extensión COM o EXE, por citar algunos ejemplos. Este es el escalafón final del trabajo del virus

¿Por qué llamarlos Virus? La gran similitud entre el funcionamiento de los virus computacionales y los virus biológicos, propició que a estos pequeños programas se les denominara virus.

Los virus de las computadoras no son mas que programas; y estos virus casi siempre los acarrean las copias ilegales o piratas. Provocan desde la pérdida de datos o archivos en los medios de almacenamiento de información (diskette, disco

duro, cinta), hasta daños al sistema y, algunas veces, incluyen instrucciones que pueden ocasionar daños al equipo.

Estos programas tienen algunas características muy especiales:

- Son muy pequeños.
- Casi nunca incluyen el nombre del autor, ni el registro o copyright, ni la fecha de creación.
- Se reproducen a sí mismos.
- Toman el control o modifican otros programas.

Los científicos del área de la computación discutieron por primera vez la posibilidad de un programa capaz de duplicarse a sí mismo y extenderse entre las computadoras desde los 50. Pero no fue sino hasta 1983 que un software de virus real fue creado, cuando un estudiante en la Universidad de California, Fred Cohen, escribió una tesis de doctorado sobre el tema.

Algunos motivos para crear un virus; A diferencia de los virus que causan resfriados y enfermedades en humanos, los virus de computadora no ocurren en forma natural, cada uno debe ser programado. No existen virus benéficos. Algunas veces son escritos como una broma, quizá para irritar a la gente desplegando un mensaje humorístico. En estos casos, el virus no es más que una molestia. Pero cuando un virus es malicioso y causa daño real, ¿quién sabe realmente la causa? ¿Aburrimiento? ¿Coraje? ¿Reto intelectual? Cualquiera que sea el motivo, los efectos pueden ser devastadores.

Los fabricantes de virus por lo general no revelan su identidad. y algunos retan a su identificación.

¿Cómo Evitarlos? Sospecha de los programas activos todo el tiempo (residentes en memoria). Los virus tienen la mala costumbre de quedarse en memoria para realizar sus fechorías.

Sospecha de cualquier programa gratuito (shareware, freeware; fotos, videos, rutinas, patchs) que bajes de Internet. Los fabricantes de virus colocan frecuentemente en estos sus nocivos productos.

Obtén una lista de los virus mas comunes y verifica contra esta lista cualquier programa nuevo que tengas.

Fíjate en el tamaño de los archivos del sistema [COMMAND.COM principalmente]. Sospecha si es diferente del original.

Haz una copia de la Tabla de Localidades para Archivo [File Allocation Table] y CMOS si te es posible. Te ahorrará mucho tiempo, dinero y esfuerzo el copiarla de nuevo si algún virus la dañó.

Al estar buscando un virus, y si tienes disco duro, bloquea el acceso a este temporalmente.

Actualiza mensualmente tu AntiVirus. Si no lo tienes puedes conseguir una copia gratuita en: Symantec Corp., Network Associates Inc., Command Software Systems, Inc., Aladdin Knowledge Systems, Data Fellows, Norman Data Defense Systems, Panda Software International, Sophos Inc., entre otros.

Origen de los Virus. Los virus tienen la misma edad que las computadoras. Ya en 1949 John Von Neumann, describió programas que se reproducen a sí mismos en su libro "Teoría y Organización de Autómatas Complicados". Es hasta mucho después que se les comienza a llamar como virus. La característica de auto-

reproducción y mutación de estos programas, que las hace parecidas a las de los virus biológicos, parece ser el origen del nombre con que hoy los conocemos.

Antes de la explosión del micro computación se decía muy poco de ellos. Por un lado, la computación era secreto de unos pocos. Por otro lado, las entidades gubernamentales, científicas o militares, que vieron sus equipos atacadas por virus, se quedaron muy calladas, para no demostrar la debilidad de sus sistemas de seguridad, que costaron millones, al bolsillo de los contribuyentes. La empresa privada como Bancos, o grandes corporaciones, tampoco podían decir nada, para no perder la confianza de sus clientes o accionistas. Lo que se sabe de los virus desde 1949 hasta 1989, es muy poco.

Se reconoce como antecedente de los virus actuales, un juego creado por programadores de la empresa AT&T (mamá Bey), que desarrollaron la primera versión del sistema operativo Unix, en los años 60. Para entretenerse, y como parte de sus investigaciones, desarrollaron un juego, "Core War", que tenía la capacidad de reproducirse cada vez que se ejecutaba. Este programa tenía instrucciones destinadas a destruir la memoria del rival o impedir su correcto funcionamiento.

Al mismo tiempo, desarrollaron un programa llamado "Reeper", que destruía las copias hechas por Core Ware. Un antivirus o antibiótico, al decir actual. Conscientes de lo peligroso del juego, decidieron mantenerlo en secreto, y no hablar más del tema. No se sabe si esta decisión fue por iniciativa propia, o por órdenes superiores.

En 1982, los equipos Apple II comienzan a verse afectados por un virus llamado "Cloner" que presentaba un mensaje en forma de poema.

El año siguiente, 1983, el Dr. Ken Thomson, uno de los programadores de AT&T, que trabajó en la creación de "Core War", rompe el silencio acordado, y da a conocer la existencia del programa, con detalles de su estructura, en una alocución ante la Asociación de Computación.

La Revista Scientific American a comienzos de 1984, publica la información completa sobre esos programas, con guías para la creación de virus. Es el punto de partida de la vida pública de estos aterrantes programas, y naturalmente de su difusión sin control, en las computadoras personales.

Por esa misma fecha, 1984, el Dr. Fred Cohen hace una demostración en la Universidad de California, presentando un virus informático residente en una PC. Al Dr. Cohen se le conoce hoy día, como "el padre de los virus". Paralelamente aparece en muchas PCs un virus, con un nombre sim ilar a Core War, escrito en Small-C por un tal Kevin Bjorke, que luego lo cede a dominio público. ¡La cosa comienza a ponerse caliente!

El primer virus destructor y dañino plenamente identificado que infecta muchas PC's aparece en 1986. Fue creado en la ciudad de Lahore, Paquistán, y se le conoce con el nombre de BRAIN. Sus autores vendían copias pirateadas de programas comerciales como Lotus, Supercalc o Wordstar, por suma bajísimas. Los turistas que visitaban Paquistán, compraban esas copias y las llevaban de vuelta a los EE.UU. Las copias pirateadas llevaban un virus. Fue así, como infectaron mas de 20,000 computadoras. Los códigos del virus Brain fueron alterados en los EE.UU., por otros programadores, dando origen a muchas versiones de ese virus, cada una de ellas peor que la precedente. Hasta la fecha nadie estaba tomando en serio el fenómeno, que comenzaba a ser bastante molesto y peligroso.

Comienza la lucha contra los virus. En 1987, los sistemas de Correo Electrónico de la IBM, fueron invadidos por un virus que enviaba mensajes navideños, y que se multiplicaba rápidamente. Ello ocasionó que los discos duros se llenaran de archivos de origen viral, y el sistema se fue haciendo lento, hasta llegar a paralizarse por mas de tres días. La cosa había llegado demasiado lejos y el **Big Blue** puso de inmediato a trabajar en los virus su Centro de Investigación Thomas J. Watson, de Yorktown Heights, NI. Las investigaciones del Centro T. J. Watson sobre

virus, son puestas en el dominio público por medio de Reportes de Investigación, editados periódicamente, para beneficio de investigadores y usuarios.

El virus Jerusalén, según se dice creado por la Organización de Liberación Palestina, es detectado en la Universidad Hebrea de Jerusalén a comienzos de 1988. El virus estaba destinado a aparecer el 13 de Mayo de 1988, fecha del 40 aniversario de la existencia de Palestina como nación. Una interesante faceta del terrorismo, que ahora se vuelca hacia la destrucción de los sistemas de cómputo, por medio de programas que destruyen a otros programas.

El 2 de Noviembre del 88, dos importantes redes de EE.UU. se ven afectadas seriamente por virus introducidos en ellas. Mas 6,000 equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados se ven atacados.

Por 1989 la cantidad de virus detectados en diferentes lugares sobrepasan los 100, y la epidemia comienza a crear situaciones graves. Entre las medidas que se toma, para tratar de detener el avance de los virus, es llevar a los tribunales a Robert Morís Jr. acusado de ser el creador de un virus que infectó a computadoras del gobierno y empresas privadas. Al parecer, este muchacho conoció el programa Core Ware, creado en la AT&T, y lo difundió entre sus amigos. Ellos se encargaron de diseminarlo por diferentes medio a redes y equipos. Al juicio se le dio gran publicidad, pero no detuvo a los creadores de virus. La cantidad de virus que circula en la actualidad es desconocida.

McAfee y Asociados, una empresa creada por John McAfee y dedicada a la producción de programas anti-virales. que distribuye sus trabajos por medio del sistema ***shareware***, o programas de uso compartidos identificaba a comienzos de 1996 los siguientes: Virus Principales Conocidos..... 534; Variaciones de esos Virus.....729; Total de Virus Identificados 1,263

Por ejemplo, del virus Stoned se conoce mas de 26 versiones diferentes, del virus Dark Avenger se identifica mas de 1 1 versiones, del virus Paquistaní Brain 8 versiones y del virus Plastique 9 versiones.

John McAfee es un nombre importante en la corta historia de la guerra contra los virus y en el desarrollo de programas preventivos (vacunas) y programas curativos (antibióticos). Sus esfuerzo en la identificación y destrucción de virus informáticos merece todo el respeto y apoyo de la comunidad de usuarios de computadoras.

Los virus de computadora son parte real y presente en la cultura computacional

2.3.3. GUSANOS O WORMS.

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus por que no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Estos programas su única misión es colapsar cualquier sistema, y que son programas que se copian en archivos distintos en cadena hasta crear miles de réplicas de si mismo. Los gusanos o también llamados Worms suelen habitar en la red como respuesta de grupos de Hackers que pretenden obtener algo. La existencia de estos gusanos se hace notar, cuando la Red se ralentiza considerablemente, ya que normalmente el proceso de autoreplicado llena normalmente el ancho de banda de un servidor en particular.

Son programas que se reproducen a sí mismos y no requieren de un anfitrión, pues se "arrastran" por todo el sistema sin necesidad de un programa que los transporte.
Los gusanos se cargan en la memoria y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente. Esto hace que queden borrados los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdida de datos

2.3.4. BOMBA LÓGICA O CRONOLÓGICA.

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

Las bombas lógicas, están especializadas para hacer daño. Existen dos definiciones de mismo acrónimo o programa asociado. Una es la de crear un subprograma que active después de un tiempo llenando la memoria del ordenador y la otra es de colapsar nuestro correo electrónico. De cualquier forma son dañinos, pero actúan de forma diferente, en la primera referencia se instala en nuestra computadora después de ser bajado junto a un mensaje de e-mail. Se incuba sin crear ninguna copia de si mismo a la espera de reunir las condiciones oportunas, tras ese periodo de espera el programa se activa y se autoreplica como un virus hasta dañar nuestro sistema.

En el segundo caso, alguien nos envía una bomba lógica por e-mail que o es más que un mismo mensaje enviado miles de veces hasta colapsar nuestra máquina. Los antivirus no están preparados para detectar estos tipos de bombas lógicas.

También se les denominan Bombas de Tiempo que son los programas ocultos en la memoria del sistema o en los discos, o en los archivos de programas ejecutables con tipo COM o EXE. En espera de una fecha o una hora determinadas para "explotar". Algunos de estos virus no son destructivos y solo exhiben mensajes en las pantallas al llegar el momento de la "explosión". Llegado el momento, se activan cuando se ejecuta el programa que las contiene.

2.4. ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS.

Por varios motivos, que van desde la simple curiosidad, hasta los mas complejos robos, o incluso sabotaje o espionaje informático; es algunos modos de operar de los amantes a la informática y al internet:

2.4.1. PIRATAS INFORMÁTICOS O HACKERS.

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

2.4.2. REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL.

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

CAPÍTULO III
TRATAMIENTO INTERNACIONAL

3.1. ORGANISMOS INTERNACIONALES

El objetivo de este capítulo es presentar todos aquellos elementos que han sido considerados por organismos gubernamentales internacionales así como por diferentes países, para enfrentar la problemática de los delitos informáticos a fin de que contribuyan al desarrollo de la tipificación, y de la importancia que tiene este tema.

Debe mencionarse que durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen algunos de los derechos penales de diferentes Estados.

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales[25].

Las posibles implicaciones económicas de la delincuencia informática, su ámbito internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables, así como de las propuestas de reforma. Las conclusiones político-jurídicas

[25] Cfr. http://www.funcionpublica.gob.mx/ocde/, 27 de Marzo del 2004.

desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

De esta forma, la OCDE en 1986 publicó un informe titulado "Delitos de Informática: análisis de la normativa jurídica"[26], en donde se reseñaban las normas legislativas vigentes y las propuestas de reformas en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales (lista Mínima), como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

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

Con objeto de que se finalizara la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema, a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección[27].

La lista mínima preparada por la OCDE se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité Especial de Expertos sobre Delitos relacionados con el

[26] Cfr. http://www.aaba.org.ar/bi180p43.htm, 1 de Abril del 2004.
[27] Cfr. http://assembly.coe.int/, 5 de Abril de 2004.

empleo de computadoras, del Comité Europeo para los Problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático[28].

Una vez desarrollado todo este proceso de elaboración de las normas en el ámbito continental, el Consejo de Europa aprobó la recomendación sobre delitos informáticos, en la que "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras (y en particular las directrices para los legisladores nacionales). Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa; el 13 de septiembre de 1989. Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación[29].

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

En este contexto, consideramos que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de delitos informáticos, ello es resultado de las características propias de los países que los integran, quienes, comparados con México y otras partes del mundo, tienen un

[28] Cfr. http://www.dpi.bioetica.org/softnotas3.htm, 3 de Abril del 2004.
[29] Cfr. http://www.aadat.org/delitos_informaticos20.htm, 2 de Abril del 2004.

mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

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

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

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados. Por todo ello, en vista que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras, a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado en nivel internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera del delito informático y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de

conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos.

Adicionalmente, deben mencionarse la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición. Teniendo presente esa situación, consideramos que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

En otro orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta qué punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados[30].

Asimismo, considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que pueden entrañar el adelanto tecnológico, se

[30] Cfr. www.htmlweb.net/seguridad/tesis/Cap4.pdf, 6 de Mayo del 2004.

recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la lista facultativa, especialmente la alteración de datos de computadora y el espionaje informático; así como que por lo que se refiere al delito de acceso no autorizado precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Además, señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

3.2. LEGISLACIÓN EN OTROS PAÍSES

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas.

En los Estados industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años. Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo, con el objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, a continuación se presentan los siguientes casos particulares:

3.2.1. ALEMANIA

En Alemania para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos[31]:

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

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, acusación del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o

[31] Cfr. www.stj-sin.gob.mx/Delitos_Informaticos2.htm, 8 de Marzo del 2004.

incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

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

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

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

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación a 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 pueda ser datos almacenados o transmitidos o se trate del daño al sistema informático. El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

Alemania también cuenta con una Ley de Protección de Datos, promulgada el 27 de Enero de 1977, en la cual, en su numeral primero menciona que "el cometido de la protección de datos es evitar el detrimento de los intereses dignos de protección de los afectados, mediante la protección de los datos personales contra el abuso producido con ocasión del almacenamiento, comunicación, modificación y cancelación (proceso) de tales datos. La presente ley protege los datos personales que fueren almacenados en registros informatizados, modificados, cancelados o comunidades a partir de registros informatizados"[32].

3.2.2. AUSTRIA

Ley de reforma del Código Penal de 22 de diciembre de 1987.

Esta ley contempla los siguientes delitos:

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

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

[32] www.usm.edu.ec/eticainformatica/estado%20arte/cap%20II%-20regimenjuridico.PDF, 25 de marzo del 2003.

sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

3.2.3. FRANCIA

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

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

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

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

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

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

Las disposiciones penales están contempladas en sus numerales del 41 al 44, los cuales contemplan lo siguiente: artículo 41. El que hubiere procedido o mandado proceder a la realización de tratamientos automatizados de información nominativa sin que hubieran sido publicados los actos reglamentarios previstos en el artículo 15 o formuladas las denuncias previstas en el artículo 16, será castigado con pena de privación de libertad de seis meses a tres años y con pena de multa de 2,000 a 200,000 francos, o con una sola de estas dos penas. Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos, en las condiciones que determinare y a expensas del condenado".

Artículo 42. El que hubiere registrado o mandado registrar, conservando o mandando conservar informaciones nominativas con infracción de las disposiciones de los artículos 25, 26 y 28, será castigado con pena de privación de libertad de uno a cinco años y con pena de multa de 20,000 a 2,000,000 francos, o con una de estas dos penas.

Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos en las condiciones que determine, y a expensas del condenado.

Artículo 43. El que habiendo reunido, con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento, informaciones nominativas cuya divulgación tuviere como efecto atentar contra la reputación o la consideración de la persona o la intimidad de la vida privada; hubiere, sin autorización del interesado y a sabiendas, puesto tales informaciones en conocimiento de una persona que no estuviere habilitada para recibirlas a tenor de las disposiciones de la presente ley o de otras disposiciones legales, será castigado con pena de privación de libertad de dos a seis meses y con pena de multa de 2,000 a 20,000 francos, o con una de las dos penas.

El que por imprudencia o negligencia, hubiere divulgado o permitido divulgar informaciones de la índole de las que se mencionan en le párrafo anterior, será castigado con pena de multa de 2,000 a 20,000 francos.

Artículo 44. El que, disponiendo de informaciones nominativas con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento las hubiere desviado de su finalidad, según la misma hubiera sido definida, bien en el acto reglamentario previsto en el artículo 15, o en las denuncias formuladas en aplicación de los artículos 16 y 17, bien en una disposición legal, será castigado con pena de privación de libertad de uno a cinco años y con multa de 20,000 a 2, 000,000 francos.

3.2.4. ESTADOS UNIDOS

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos técnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas. (18 U.S.C. Sec. 1030 [a] [5] [A]). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

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

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

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

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

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

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

gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

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

3.2.5. CHILE.

Cuenta con una ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993, la cual en sus cuatro numerales menciona: artículo 1°. El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Artículo 2°. El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.[33]

Artículo 3°. El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

---

[33] Cfr. http://www.monografias.com/trabajos12/tsinnom/tsinnom2.shtml, 24 de Febrero del 2004.

Artículo 4°. El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

3.2.6. ITALIA.

En un país con importante tradición criminalista, como Italia, nos encontramos tipificados en su Código Penal los siguientes delitos[34]:

- Acceso Abusivo. Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso a aquél sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.

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

- Introducción de virus informáticos. Es penalmente responsable aquel que cree o introduzca a una red programas que tengan la función específica de bloquear un sistema, destruir datos o dañar el disco duro, con un castigo de reclusión de hasta dos años y multas considerables.

- Fraude Informático.- Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un injusto beneficio, ocasionando daño a otro. También se entiende como tal la alteración del

[34] Cfr. www.alfa-redi.org/ upload/documento/110801--20-6-LA%20AUTORIA%20MEDIATA%20(PATRICIA%20COTRONE) 21 de Marzo del 2004.

funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en ellos contenidos o pertenecientes a ellos, cuando se procure una ventaja injusta, causando daño a otro. La punibilidad de este tipo de delito es de meses a tres años de prisión, más una multa considerable.

- Intercepción abusiva.- Es un delito que se comete junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. Asimismo, es la intercepción fraudulenta, el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público, mediante cualquier medio, de la información, de esas publicaciones; este delito tiene una punibilidad de 6 meses a 4 años de prisión. Asimismo, se castiga el hecho de realizar la instalación de equipo con el fin anterior.-

- Falsificación informática. Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. En este caso, se presupone la existencia de un documento escrito (aunque se debate doctrinariamente si los documentos electrónicos o virtuales pueden considerarse documentos escritos). En este caso, la doctrina italiana tiene muy clara la noción de "documento informático", al cual define como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.

- Espionaje Informático.- Es la revelación del contenido de documentos informáticos secretos o su uso para adquirir beneficios propios, ocasionado daño a otro.

- Violencia sobre bienes informáticos. Es el ejercicio arbitrario, con violencia, sobre un programa, mediante la total o parcial alteración, modificación o

cancelación del mismo o sobre un sistema telemático, impidiendo o perturbando su funcionamiento.

- ❖ Abuso de la detentación o difusión de Códigos de acceso (contraseñas).

- ❖ Violación de correspondencia electrónica, la cual tiene agravantes si causare daños.

3.2.7. PORTUGAL

Por su parte, la Constitución de la República Portuguesa, hace mención sobre la utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976, y la cual menciona[35]:

Artículo 35: Utilización de la Informática. 1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización. 2. La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos. 3. Queda prohibida la atribución de un número nacional único a los ciudadanos.

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

---

[35] http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap4.htm, 14 de Abril del 2004.

La legislación y regulación sobre los delitos informáticos en otros países, constituye un gran avance para países como en el nuestro que no tienen una legislación al respecto, por lo anterior, no se va ha realizar una crítica a las anteriores disposiciones legales, ya que cada país contempló dichas normas de acuerdo a sus necesidades propias, como se puede observar en líneas precedentes, (ya que algunos países se enfocaron propiamente a proteger el derecho a la privacidad, y a la propiedad intelectual, o como el que disponga de informaciones nominativas y haga un mal uso de ello; otros tantos a proteger al patrimonio de las personas afectadas como en los fraudes informáticos etcétera). Más sin embargo como se mencionó con anterioridad, nos ayudan y nos dan la pauta para que nuestros legisladores contemplen las figuras delictivas de "delitos informáticos", de acuerdo a nuestra realidad.

CAPITULO IV.

LEGISLACIÓN NACIONAL.

Para el desarrollo de este capítulo se analizará la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan que son los delitos informáticos, atendiendo al artículo 16 de la Constitución de los Estados Unidos Mexicanos, en el párrafo décimo, en el que a la letra contempla:

> **"...Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio..."**[35]

Se deduce que al no haber tipificación al respecto de los delitos que contempla la ley, o que no tiene ninguna apreciación informática; éstos no podrían ser objeto de un juicio penal, ya que no existe un tipo penal que los contemple, o en su caso alguna fracción que delimite un medio informático.

En este entendido, consideramos pertinente recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte en virtud de que el artículo 133 constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

4.1. TRATADO DE LIBRE COMERCIO DE AMÉRICA DEL NORTE (TLCN).

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual,

---

[35] Constitución Política de los Estados Unidos Mexicanos, Editorial Porrúa, 139ª edición, México Distrito Federal, 2002.

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[36].

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.

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse 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.

Asimismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos, sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información. Llama la atención que en su párrafo 2° habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que éstos consten en medios electrónicos o magnéticos.

---

[36] Cfr. www.presidencia.gob.mx/tratadosint.html, 16 de Abril del 2000.

4.2. ACUERDO SOBRE LOS ASPECTOS DE LOS DERECHOS DE PROPIEDAD INTELECTUAL RELACIONADOS CON EL COMERCIO, INCLUSO EL COMERCIO DE MERCANCÍAS FALSIFICADAS.

Al iniciar el contenido de este apartado, debemos aclarar que si bien la institución del GATT se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), todos los acuerdos que se suscribieron en el marco del GATT siguen siendo vigentes. En este entendido, cabe mencionar que el Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda de Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT) manteniendo su vigencia hasta nuestros días[37].

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 estè tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias, de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

Además, en la parte III sobre observancia de los derechos de propiedad intelectual, en la sección I de obligaciones generales, específicamente en el artículo 41, se incluye que los miembros del acuerdo velarán porque en su respectiva legislación nacional se establezcan procedimientos de observancia de los derechos de propiedad intelectual.

Asimismo, en la sección 5, denominada procedimientos penales, en particular el artículo 61. se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales, además de que los recursos

[37] Cfr. www.omc.onu.sa/es/html, 15 de Febrero del 2004.

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 piratas que lesionan 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 del Derecho de Autor que a continuación se analiza.

4.3. LEY FEDERAL DEL DERECHO DE AUTOR.

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

Sobre el particular, y por considerar de interés el contenido de la exposición de motivos cuando esta ley se presentó ante la Cámara de Diputados, 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 formuló la iniciativa correspondiente, se dijo que la importancia de pronunciarse al respecto era que con dicha iniciativa se atendía la

complejidad que el tema de los derechos autorales había presentado en los últimos tiempos lo cual exigía una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión[38].

Además, se consideró que debido a que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de Decreto de Reforma al Código Penal para el Distrito Federal en materia de Fuero Federal, proponiendo la adición de un título Vigésimo Sexto denominado "De los delitos en materia de derechos de autor".

Al respecto, se consideró conveniente la inclusión de la materia en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas y por otro en un instrumento más adecuado para la procuración y la administración de justicia, al poderse disponer en la investigación de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.

En este orden, como se mencionó anteriormente, esta Ley regula todo lo relativo a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos. 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 derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.

[38] Cfr. www.camaradediputados.gob.mx, Enero del 2003.

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

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

Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, Artículo 424, fracción IV del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal del que se infiere la sanción al uso de programas de virus. 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 el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los delitos informáticos el bien jurídico a tutelar serían por ejemplo, el de la intimidad, patrimonio, etcétera.

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

Por su parte, el artículo 231, fracciones II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilicitas 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[39].

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. Sin embargo, la regulación existente no ha llegado a contemplar el delito informático como tal, sino que se ha concretado a la protección de los derechos autorales y de propiedad industrial, principalmente.

Tal y como hemos sostenido, México no está exento de formar parte de los países que se enfrentan a la proliferación de estas conductas ilícitas. Recientemente, la prensa publicó una nota en la que informaba sobre las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que se remontaban a un valor de mil millones de dólares por concepto de piratería de estos programas.

Muchas personas sentirán que el país está ajeno a estas pérdidas por cuanto estas compañías no son mexicanas, sin embargo, si analizamos los sujetos comisores de estos delitos, según la nota de prensa, podríamos sorprendernos al saber que empresas mexicanas como TAESA y Muebles Dico enfrentan juicios administrativos por el uso de programas piratas[40].

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

---

[39] Cfr. www.monografias.com/leyesdmex/es.html, Febrero del 2003.

[40] Cfr. ICONOMIA, "Incurrieron TAESA y Muebles Dico en delitos informáticos", La Jornada, México, sábado 12 de abril de 1997.

informáticos, lo que se traduciría en un mercado poco atractivo para ellas que pondrían al país en una situación marginada del desarrollo tecnológico

En este entendido, consideramos que por la gravedad de la conducta ilícita en sí, y las implicaciones que traería aparejadas, justifica su regulación penal.

En otro orden, el artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información. Así, por ejemplo; el acceso no autorizado a una base de datos de carácter personal como el de un Hospital de enfermos de SIDA puede ser utilizado contra estas personas quienes a causa de su enfermedad, se encuentran marginados socialmente, en la mayoría de los casos. Asimismo, consideramos que la protección a este tipo de bases de datos es necesaria en virtud de que la información contenida en ellas, puede contener datos de carácter sensible, como son los de las creencias religiosas o la filiación política. Adicionalmente pueden ser susceptibles de chantaje, los clientes de determinadas instituciones de créditos que posean grandes sumas de dinero, en fin, la regulación de la protección de la intimidad personal es un aspecto de suma importancia que se encuentra regulado en este artículo.

Por lo anterior, el análisis de este artículo corrobora la posición que hemos sostenido respecto a que en las conductas ilícitas relacionadas con la informáticas el bien jurídico a tutelar no es únicamente la propiedad intelectual sino la intimidad por lo que este artículo no debería formar parte de una Ley de derechos de autor sino de una legislación especial tal y como se ha hecho en otros países.

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

investigaciones respecto de presuntas infracciones administrativas e imponer las sanciones correspondientes.

Por otra parte, 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", quedando:

> **Art. 231.**
> **"...III "Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta Ley"**

Con las reformas al Código Penal se especifica que:

> **Art. 424**
> **III "A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende, copias de obras, fonogramas, videogramas o libros protegidas por la Ley Federal del Derecho de Autor en forma dolosa, a escala comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos"**

Sobre el particular, debe mencionarse que durante la modificación a la Ley en diciembre de 1996 se contempló parcialmente lo que se había acordado en el TLCN y que por tal razón fue necesaria una segunda modificación.

De igual forma el artículo 424 que había sufrido una modificación en diciembre de 1996, fue reformado en su fracción tercera en abril pasado para incluir la reproducción y su comisión en una forma dolosa.

4.4. CÓDIGO PENAL FEDERAL, EN SU CAPÍTULO NOVENO.

Para el análisis de este apartado, el título noveno, capítulo segundo referente al acceso ilícito a sistemas y equipos de informática, que a la letra dice:

TÍTULO NOVENO
Revelación de secretos y acceso ilícito a sistemas y equipos de informática

Capitulo II
Acceso ilícito a sistemas y equipos de informática.

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le

impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa."

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

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

En estos artículos, se mencionan acciones encaminadas a modificar, destruir o provocar perdidas de información, pero la ley penal, exige que sea protegido por un mecanismo de seguridad, sin embargo, la mayoría de las empresas, instituciones y particulares, no tienen conocimiento de lo que eso conlleva, es decir, a la sociedad no se le ha especificado lo que eso implica, significa, ni hay en el mismo código, su definición, lo que la ley penal exige como requisitos de procebilidad para el tipo penal, la probable responsabilidad, y los supuestos delitos en que quedaría consignado; ante esto quedaría en el espacio lo que hace la Agencia Federal de Investigación (AFI), con su llamada policía virtual, por que aunque se determinara la persona o las personas, no hay delito que perseguir, por que no hay nada de lo que mencionamos con antelación.

Artículo 211 bis 3.

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

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa."

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa."

Artículo 211 bis 5.

"Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero."

Artículo 211 bis 6.
"Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7
Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno."

Después del estudio de las experiencias adquiridas por diferentes países al enfrentar el delito informático y la forma en que está siendo regulada esta problemática en México, además del evidente incremento de esta situación, es necesario, a pesar de que en el país el delito informático no ha alcanzado el grado de peligrosidad existente en esos países, regular penalmente las conductas ilícitas derivadas del uso de la computadora, como más adelante expondremos.

En primer término, la difusión a las empresas, organismos, dependencias, particulares y a la sociedad en general, contribuirá notoriamente al nivel de concientización sobre el problema que nos ocupa. El siguiente paso será dar a conocer las medidas preventivas que se deben adoptar para evitar estas conductas ilícitas.

Sin embargo, con base en que en la Ley Federal del Derecho de Autor se considera como bien jurídico tutelado la propiedad intelectual y que, el bien jurídico tutelado en los delitos informáticos es fundamentalmente el patrimonio, se sugiere que en el Título Vigésimo Segundo sobre los "Delitos en contra de las personas en su patrimonio" del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal se añada un capítulo especial para los delitos informáticos.

Teniendo en cuenta también la gravedad que implican los delitos informáticos, es necesario que el Código Penal Federal incluya figuras delictivas que contengan los delitos informáticos, ya que de no hacerlo, la ausencia de figuras concretas que se puedan aplicar en esa materia daría lugar a que los autores de esos hechos quedaran impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos. Por otra parte. teniendo presente que el Estado de Sinaloa a través de su Congreso Local ha legislado sobre el tema de delitos informáticos, contemplando de forma general una amplia variedad de los mismos y estableciendo las sanciones correspondientes, se establece que es necesario que con objeto de que se evite un conflicto de competencia entre los

congresos locales y el de la Unión, éste con base en las facultades que la Constitución Federal le confiere, establezca los criterios necesarios para delimitar, dada la naturaleza de los delitos informáticos, que pueden emplear para su ejecución las vías generales de comunicación entre otros elementos, la jurisdicción federal y local de estos ilícitos.

En México, Internet no se ha regulado de manera expresa, como tampoco en el resto de los países latinoamericanos. Su uso gira en torno a cierto Código Ético y la tendencia Institucional es que será un fenómeno "autorregulable". A pesar de los índices de crecimiento del uso de la computadora y de Internet, México enfrenta un problema social consistente en lo que denominamos "analfabetismo informático", del cual el Poder Legislativo no está exento, por lo que muchos congresistas no entienden el concepto y la estructura de Internet. Asimismo, nos atrevemos a afirmar que tanto los jueces como los magistrados que forman parte del Poder Judicial tienen hoy día la misma carencia. Es difícil prever el pronunciamiento de los tribunales federales o de la Suprema Corte de Justicia Mexicanos en un caso cuya resolución se base esencialmente en un conflicto por el uso de Internet, por lo cual no se tiene conocimiento de la existencia de tesis ni jurisprudencia algunas que se refieran a los medios electrónicos en general y a Internet en especial.

Como se mencionó es un Código Ético el que puede regular la conducta de los usuarios, mas sin embargo, existe en nuestro país una regulación administrativa sobre las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos, en este sentido, se considera pertinente recurrir a aquellos tratados internaciones de los que el Gobierno de México es parte en virtud de que el artículo 133 Constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

CAPÍTULO V.

TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN EL ÁMBITO FEDERAL.

Para hablar de tipificación es menester de esta investigación, adentrarnos a la definición de tipo; "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 entendida como la característica de una acción de adecuarse a una disposición legislativa"; es por ello que al hablar que un comportamiento es típico cuando coincide con lo previsto en un tipo penal.[40]

No podemos hablar sobre delitos informáticos cuando no están regulados dentro del Nuevo Código Penal, o en su defecto en algún otro ordenamiento, el concepto de delitos informáticos como ya lo hemos dicho es dentro de alguna legislación que en otro país así le han denominado, en los Estados Unidos Mexicanos se le denomina al delito como el acto u omisión que sancionan las leyes penales, en el Código Penal para el Distrito Federal de 1931.[41]

En este orden de ideas, a continuación explicaremos más detalladamente los problemas derivados a falta de la legislación de delitos informáticos, tanto en la doctrina, como en las leyes y jurisprudencias en el país.

5.1. PROBLEMAS DERIVADOS DE LA AUSENCIA DE LEGISLACIÓN EN MATERIA DE DELITOS INFORMÁTICOS.

En la actualidad es imposible que las empresas, la industria, Instituciones de banca múltiple, en cada una de las instituciones educativas y hasta el propio Estado dentro de sus oficinas administrativas, Juzgados de Paz. locales, federales y demás dependencias de cualquier poder del Estado del que deriven; utilizan las

---

[40] Cfr. INSTITUTO DE INVESTIGACIONES JURÍDICAS, Enciclopedia Jurídica Mexicana, editorial Porrúa, UNAM, Tomo V, Primera Edición, México 2002.
[41] COLECCIÓN PENAL, Ediciones Delma, Tercera Edición, México, 2000.

computadoras, y la mayoría de ellas en una interconexión entre las mismas; esto denominado Redes o sistemas informáticos.

Sin embargo, no hay una regulación adecuada sobre los medios informáticos que no están regulados en México, sin embargo el cuestionamiento no termina aquí, podemos decir que la mayoría de los Tratados Internacionales que hablan de los llamados delitos informáticos, obviamente ratificados por México, no tienen la observancia dentro del país y tendríamos que irnos a instancias internacionales para resolverlo.

5.1.1. DOCTRINA.

Dentro de la aplicación del derecho, nos encontramos con la aplicación privada y la aplicación oficial de las normas jurídicas, dentro de estas la aplicación de las normas de derecho a casos concretos que puede ser privada o pública. El primer caso tiene una finalidad de simple conocimiento, y el segundo una aplicación propiamente dicha.[42]

De esto se deriva que el poder penal del Estado lo entendemos como la facultad y el deber del propio Estado de emitir normas jurídicas que tipifiquen las conductas delictivas y proceder a la aplicación de tales normas a los casos concretos, sancionando con la pena correspondiente a los infractores de los mencionados preceptos, todo ello con el fin de hacer posible la adecuada convivencia social.[43]

Por lo consiguiente no sirve de nada que la Agencia Federal de Investigación tenga un departamento de ciberpolicías al servicio de la comunidad; ya que si encuentran a un cracker, un hacker o cualquier otra modalidad de pirata informático en el Internet, no podrá ser juzgado ya que no hay un delito que perseguir, solo en el Código Penal Federal, determina el acceso ilícito a computadores, mas sin en

[42] Cfr. GARCÍA MAYNES Eduardo. Introducción al Estudio del Derecho. Editorial Porrúa. México 1999, 50ª Edición. P.p. 322.
[43] Cfr. OSORIO Y NIETO César Augusto. Delitos Federales, Editorial Porrúa, México 2003, Sexta Edición, pp. 3.

cambio podemos ver en el análisis consiguiente lo que sucede. En este orden de ideas, otra de las cosas es que se de debe de comprobar el cuerpo del delito y la probable responsabilidad de ciertas conductas típicas y antijurídicas, pero la pregunta que nos hemos planteado desde el inicio de la investigación, es ¿Por qué la necesidad de tipificar los delitos informáticos en el área penal federal de los Estados Unidos Mexicanos?; para ir a favor de la realidad mexicana.

5.1.2. LEY NACIONAL.

De acuerdo con el artículo 73, fracción XXI, de la Constitución Política de los Estados Unidos Mexicanos; donde menciona las facultades del Congreso de la Unión; para establecer los delitos y las faltas contra la Federación y fijar los castigos que por ellos deban imponerse.[44]

Es por ello que deben de tipificar los delitos informáticos de manera Federal, ya que no es lo mismo que cada Estado tenga su capítulo de delitos Informáticos en su código Penal. Es mejor de fuero Federal, ya que la realidad es que podría sustraerse de manera fácil de la coercibilidad de cada Estado, así de manera Federal no podría triangular[45] sus fechorías y correr de un Estado a otro.

Por mencionar el Estado de la República Mexicana que tiene el su Código Penal vigente y que menciona los delitos informáticos es el de Sinaloa; que en su artículo 217 menciona:

> **"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,**

[44] CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, Editorial Porrúa, México 2002.
[45] Triangular implica saltar de un sistema a otro por medio de internet, simulando que esté en otro lugar, cuando está en otro.

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."

Para el análisis de este artículo debemos de recordar que para la ley penal mexicana, es un delito doloso; que denota la violación, apoyada en el conocimiento correspondiente, que preside la realización de la conducta descrita en los tipos del delito, esto es sumamente comprobable, ya que para ser un hacker, un cracker o cualquier otro tipo de pirata informático se necesita tener muchísimo conocimiento del área informática.[46]

Ahora, para comprobar el cuerpo del delito y la probable responsabilidad de esta norma jurídica, es necesario que el legislador determine que es una base de datos, un sistema de computadoras y una red, además de diseñar, ejecutar, alteración de un esquema o artificio, y en que hipótesis corresponde a cada una de las acciones encaminadas a defraudar, obtener dinero, bienes o información; con ello determinados que aun que contempla el Código Penal del Estado de Sinaloa vigente, no determina con exactitud que delito informático se encuentra, ya que como anteriormente lo hemos visto no es lo mismo ejecutar o alterar un esquema, y no son esquemas ni artificios, son archivos, programas, fotografías, datos de un Banco o peor aún de la filtración de información del Estado.

Aun que el legislador ocupa la mayoría de los términos en la segunda fracción como son: intercepte, interfiera, reciba, use, altere o destruya un soporte lógico o

[46] Cfr. INSTITUTO DE INVESTIGACIONES JURÍDICAS, Enciclopedia Jurídica Mexicana, editorial Porrúa, UNAM, Tomo II, Primera Edición, México 2002

programa de computadora o datos contenidos en la misma; no es interceptar es romper, dañar un sistema de seguridad informática, si eso es lo que quisieron decir los legisladores al respecto, además de que los programas de computadora se deben de reglamentar como piratería ya que solo un experto puede romper los candados de seguridad que tiene un disco original sobre cualquiera de ellos, además no necesariamente se necesita estar en base o en red para que se cometan este tipo de conductas.

Debería de ser de carácter federal para que se le aumentara la pena corporal de acuerdo a las conductas hechas a los ofendidos, ya sea que se adhieran conductas a los tipos penales; por ejemplo en el fraude al que por algún medio informático, cibernético, o por sistemas móviles, pueda alterar, modificar, trasladar, mover fondos, y todas aquellas acciones encaminadas a que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero.
En el Código Civil Federal, señala que el consentimiento expreso de la voluntad puede manifestarse de manera verbal, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología o por signos inequívocos.[47]

Sin embargo este tipo de medio electrónico como ya hemos tratado anteriormente puede ser manipulado, y es donde entra el conflicto de la regulación de este tipo de conductas y de ahí la importancia de que el Estado promueva la regulación de ello.

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

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

[47] Cfr. TELLEZ VALDÉS, Julio. Derecho Informático. 3ª Edición, Editorial Mc Graw Hill. P.p., 211.

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 derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.

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

Aún cuando la infracción se circunscribe al área del comercio, permite la regulación administrativa de este tipo de conductas ilícitas, como una posibilidad de agotar la vía administrativa antes de acudir a la penal. Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, artículo 424, fracción IV del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal del que se infiere la sanción al uso de programas de virus. 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 derechos de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los delitos informáticos el bien jurídico serían por ejemplo el de la intimidad, patrimonio, etcétera.

5.1.3. JURISPRUDENCIA.

En este punto cabe recalcar, que la Jurisprudencia en México sobre delitos informáticos, medios electrónicos, comercio electrónico y demás relativos, es nula ya que nos dimos cuenta en nuestra investigación que, por cuestiones de legislación y la falta de ésta en este campo, cabe resaltar que nuestro país esta en pañales a comparación con los demás países que contemplan estos hechos como ilícitos, además que no puede haber lagunas en las leyes al respecto por lo mismo.

5.2. ANÁLISIS COMPARATIVO ANTE LAS LEGISLACIONES.

Los delitos informáticos constituyen una gran laguna en nuestras leyes penales, así pues, el derecho comparado nos permite hacer una lista de los delitos que no están contemplados en el Código Penal Federal y que requieren análisis urgente por parte de nuestros académicos, penalistas y legisladores. Por lo tanto, en este apartado se verá que países disponen de una legislación adecuada para enfrentarse con el problema sobre el particular:

5.2.1. INTERNACIONALES.

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico penales; de ello surge la necesidad de adoptar medidas legislativas. Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo, se deben tomar en cuenta las medidas adoptadas por ciertos países; aunque para fines de esta investigación, se tomará nada más en cuenta aquellas medidas o leyes que no se contraponga con nuestra legislación mexicana.

5.2.1.1. ALEMANIA.

Como ya se había mencionado, en el capítulo tercero, se analizo detenidamente cada una de las leyes más notables para efectos de legislación relacionada con la informática, como la Ley contra la Criminalidad Económica, en la que contempla los siguientes delitos: Espionaje de datos, Estafa Informática, Falsificación de datos probatorios, Uso de documentos falsos, Alteración de Datos, Sabotaje Informático (punible la tentativa), esta solución fue adoptada en países escandinavos y en Austria, en Alemania se han introducido un número altamente alto de nuevos preceptos penales.

5.2.1.2. AUSTRIA.

En esta legislación, se contemplan los siguientes delitos:

a) Destrucción de datos: Es este artículo contempla datos personales, los no personales y nóminas.

b) Estafa informática: Se sanciona a que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos por actuar sobre el curso del procesamiento de datos.

5.2.1.3. FRANCIA.

En este país las cosas cambien un poco, se refieren a delitos como tales, pero realizados en formas poco convencionales, tal es el caso de el Fraude Informático, Acceso fraudulento a un sistema de elaboración de datos, en este precepto se sanciona tanto el acceso al sistema como al que se mantenga en el y aumenta la

sanción cuando existe la agravante como la supresión o modificación de datos contenidos en el sistema.

Otro delito que en el Código Penal Francés se perdigue es el Sabotaje informático, a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos. La Destrucción de Datos, se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás, introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o transmisión. El Código en cuestión, contemplan a las personas que proceden o que manden proceder a la realización de cualquiera de los delitos tratados anteriormente, como agravantes, de las cuales tienen penas que van desde 3 meses hasta cinco años, y con multas que van desde 2,000.00 a 2,000,000.00 euros.

A comparación con las dos legislaciones anteriores, sentimos que es la más completa.

5.2.1.4. ESTADOS UNIDOS.

En 1994, se adoptó el Acta Federal de Abuso Computacional; con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un caballo de Troya, etcétera y en que difieren de los virus la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas, esta ley es un nuevo adelanto por que esta directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión

de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

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

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

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

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

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era de aumentar la protección a los individuos, negocios, y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las

computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias, gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Sería un avance espectacular para nuestra legislación que adoptara un sistema parecido a causa del avance de la Tecnología, con la legislación francesa y estadounidense se podría complementar muy bien.

5.2.1.5. CHILE.

Cuenta con una ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993, la cual en sus cuatro numerales menciona: Artículo 1°.- "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo". Artículo 2°.- " El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".[48]

Artículo 3°.-"El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado". Artículo 4°.-" El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado"[49].

---

[48] http://www.monografias.com/trabajos12/tsinnom/tsinnom2.shtml, 24 de Febrero del 2004.
[49] http://www.monografias.com/trabajos12/tsinnom/tsinnom2.shtml, 24 de Febrero del 2004

5.2.1.6 ITALIA

En un país con importante tradición criminalista, como Italia, nos encontramos tipificados en su Código Penal los siguientes delitos[50]:

- Acceso Abusivo. Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso a aquél sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.

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

- Introducción de virus informáticos. Es penalmente responsable aquel que cree o introduzca a una red programas que tengan la función específica de bloquear un sistema, destruir datos o dañar el disco duro, con un castigo de reclusión de hasta dos años y multas considerables.
- Fraude Informático.- Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un injusto beneficio, ocasionando daño a otro. También se entiende como tal la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en ellos contenidos o pertenecientes a ellos, cuando se procure una ventaja injusta, causando daño a otro. La punibilidad de este tipo de delito es de meses a tres años de prisión, más una multa considerable.

---

[50] www.alfa-redi.org/ upload/documento/110801--20-6-LA%20AUTORIA%20MEDIATA%20(PATRICIA%20COTRONE) 21 de Marzo del 2004.

- Intercepción abusiva.- Es un delito que se comete junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. Asimismo, es la intercepción fraudulenta, el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público, mediante cualquier medio, de la información, de esas publicaciones; este delito tiene una punibilidad de 6 meses a 4 años de prisión. Asimismo, se castiga el hecho de realizar la instalación de equipo con el fin anterior.-

- Falsificación informática. Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. En este caso, se presupone la existencia de un documento escrito (aunque se debate doctrinariamente si los documentos electrónicos o virtuales pueden considerarse documentos escritos). En este caso, la doctrina italiana tiene muy clara la noción de "documento informático", al cual define como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.

- Espionaje Informático.- Es la revelación del contenido de documentos informáticos secretos, o su uso para adquirir beneficios propios, ocasionando daño a otro.

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

- Abuso de la detentación o difusión de Códigos de acceso (contraseñas).

- Violación de correspondencia electrónica, la cual tiene agravantes si causare daños.

5.2.1.7 PORTUGAL

Por su parte, la Constitución de la República Portuguesa, hace mención sobre la utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976, y la cual menciona[51]:

Artículo 35: " Utilización de la Informática. 1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización. 2. La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos. 3. Queda prohibida la atribución de un número nacional único a los ciudadanos.

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

La legislación y regulación sobre los delitos informáticos en otros países, constituye un gran avance para países como en el nuestro que no tienen una legislación al respecto, por lo anterior, no se va ha realizar una crítica a las anteriores disposiciones legales, ya que cada país contempló dichas normas de acuerdo a sus necesidades propias, como se puede observar en líneas precedentes, (ya que algunos países se enfocaron propiamente a proteger el derecho a la privacidad. y a la propiedad intelectual, o como el que disponga de informaciones nominativas y haga un mal uso de ello; otros tantos a proteger al patrimonio de las personas afectadas como en los fraudes informáticos etcétera). Más sin embargo como se

[51] http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap4.htm, 14 de Abril del 2004.

mencionó con anterioridad, nos ayudan y nos dan la pauta para que nuestros legisladores contemplen las figuras delictivas de "delitos informáticos", de acuerdo a nuestra realidad.

5.2.2. NACIONALES.

En México, Internet no se ha regulado de manera expresa, como tampoco en el resto de los países latinoamericanos. Su uso gira en torno a cierto Código Ético y la tendencia Institucional es que será un fenómeno "autorregulable".

A pesar de los índices de crecimiento del uso de la computadora y de Internet, México enfrenta un problema social consistente en lo que denominamos "analfabetismo informático", del cual el Poder Legislativo no está exento, por lo que muchos congresistas no entienden el concepto y la estructura de Internet. Asimismo, nos atrevemos a afirmar que tanto los jueces como los magistrados que forman parte del Poder Judicial tienen hoy día la misma carencia. Es difícil prever el pronunciamiento de los tribunales federales o de la Suprema Corte de Justicia Mexicanos en un caso cuya resolución se base esencialmente en un conflicto por el uso de Internet, por lo cual no se tiene conocimiento de la existencia de tesis ni jurisprudencia algunas que se refieran a los medios electrónicos en general y a Internet en especial.

Como se mencionó es un Código Ético el que puede regular la conducta de los usuarios, mas sin embargo, existe en nuestro país una regulación administrativa sobre las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos, en este sentido, se considera pertinente recurrir a aquellos tratados internaciones de los que el Gobierno de México es parte en virtud de que el artículo 133 Constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

5.2.2.1. CÓDIGO PENAL FEDERAL, ESTUDIO DEL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL PARA LOS ESTADOS UNIDOS MEXICANOS.

Dentro de este apartado se mencionarán las deficiencias del Código Federal Penal vigente en México; para empezar el título de Acceso ilícito a sistemas y equipos de informática, cabe mencionar que a los legisladores en turno, deberían hacer mención a que se referían a un sistema y a un equipo de informática, por que un sistema es muy amplio, deberían haber especificado acerca de las redes, computadoras caseras, de oficina, portátiles, redes de bancos, públicas privadas. Etcétera.

En el artículo 211 bis 1, que es donde comienza el capítulo, a la letra dice ..."al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad..."; sentimos que es muy restringido en cuanto las acciones que cometen, solo identifica el destruir, modificar, o provoque pérdida de información, sin embargo, en el desarrollo de esta investigación, nos damos cuenta que es mas complejo de lo que parece, por que falta mencionar muchas actividades que un hacker o un cracker hace, por ejemplo, en Estados Unidos específicamente el 7 de Febrero del 2000, bloquearon Yahoo.com, el sitio más visitado de la red; durante horas no pudieron usar el correo electrónico, participar en subastas, leer noticias ni consultar ninguna información, para la tarde el hacker en cuestión tenía el control de más computadoras de las universidades y las estaba usando para paralizar otros sitios importantes como Buy.com y eBay.com que dejo a muchos usuarios a media subasta, el ataque a Internet se producía a velocidad de la luz. El sitio de CNN desapareció dos horas y Amazon.com dejó de funcionar una. En la mañana del miércoles, los corredores de la casa de bolsa E*TRADE Financial tuvieron que suspender las transacciones cuando se bloquearon sus servidores, Los expertos en seguridad cibernética les llamaron a estos ataques "denegación distribuida de Servicio" (DDoS, por sus siglas en inglés) cada ataque provocaba que muchas

empresas dejarán de ganar millones de dólares por que los usuarios no podían ingresar a sus sitios en la red.[52]

En el párrafo anterior nos damos cuenta que las acciones encaminadas e describir el tipo penal es muy limitado ante lo que puede hacer un hacker.

Otra de las cosas que debemos cuestionar, es el mecanismo de seguridad, si bien es cierto que a veces muchas veces en las empresas, en el gobierno, en las casas entre muchas más, solo sabemos utilizar las computadoras de una manera básica, como se va a instalar un mecanismo de seguridad, además que solo protege la ley a los equipos de informática protegidos, y los demás no. En este orden de ideas se mantiene la propuesta, que es urgente y necesario la tipificación de los delitos informáticos dentro del Código en cuestión.

Así, podríamos citar cada uno de los artículos contenidos y en cada uno de ellos se observa la falta de interés que tienen nuestros legisladores ante la tecnología que avanza día con día a nuestro alrededor, y que desgraciadamente no todas las personas estamos capacitadas para evitar un problema tan latente, y por consecuencia que en nuestra vida cotidiana es tan necesaria la computadora y la ley no protege a las personas que la utilizan, y todo lo que enmarca que son datos, sistemas, redes, fuentes de trabajo que dependen de ello.

El siguiente artículo demarca las personas que tengan acceso a sistemas gubernamentales, el que sigue a las instituciones financieras, sin embargo, no manifiesta otras hipótesis, solo la que si trabajas para algunas de estas posibles se agravará la pena, pero sigue teniendo el mismo tipo penal ya analizado en los párrafos que anteceden a este; por lo consiguiente estamos totalmente de acuerdo que aunque han permitido el acceso a información, y que se necesitan algunos requisitos, seguirán los problemas.

---

[52] Cfr. GORDON MEEK, James. "Hacker al ataque"en Selecciones Reader´s Digest. Marzo del 2003. México. P.p.95-104.

5.2.2.2. LEY FEDERAL DE DERECHOS DE AUTOR.

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

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 derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.

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

Aún cuando la infracción se circunscribe al área del comercio, permite la regulación administrativa de este tipo de conductas ilícitas, como una posibilidad de agotar la vía administrativa antes de acudir a la penal. Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, artículo 424, fracción IV del Nuevo Código Penal para el Distrito Federal en Materia de Fuero Común y para toda

la República en Materia de Fuero Federal del que se infiere la sanción al uso de programas de virus. 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 derechos de autor, en el que el bien jurídico a tutelar es la propiedad intelectual, lo que limita su aplicación debido a que en los delitos informáticos el bien jurídico serían por ejemplo el de la intimidad, patrimonio, etcétera.

5.2.2.3. CÓDIGO PENAL PARA EL ESTADO DE SINALOA.

El único estado de la República que contempla en su legislación los delitos informáticos es el Estado de Sinaloa. Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos informáticos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo. "Delitos contra el Patrimonio"

Capítulo V. Delito Informático.

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

> **"1.- Use o entre a una base de datos, sistemas 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 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, sistemas o red. Al responsable del delito informático se le impondrá una pena de seis meses a dos años de prisión o de noventa a trescientos días de multa."

En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado. Consideramos que se ubicó el delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícito, 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.

Por lo anterior, es necesario que en nuestro Estado, también exista una conciencia sobre la necesidad de legislar en este aspecto, creando el tipo penal adecuado a estas conductas antisociales, lo cual sería, un freno eficaz para su comisión. Tal vez porque aún no se han visto en gran escala los estragos que pueden ocasionar estos tipos de conductas, y porque mucha gente aún no se ha incorporado al mundo de la telecomunicación, nuestros legisladores se han quedado al margen en cuanto a este aspecto.

5.2.2.4. CÓDIGO DE PROCEDIMIENTOS PENALES PARA EL ESTADO DE SINALOA.

Es menester de esta investigación mencionar que dentro del problema es el procedimiento. ya que es imposible determinar donde ocurrió el delito, sin en cambio es probable que con la tecnología se pueda decir quien lo hizo, ya que materialmente no se podría definir un sistema o una base de datos, así como lo señala el artículo 13 del Código de Procedimientos Penales para el Estado de Sinaloa, que a la letra menciona:

"Cuando haya varios jueces de la misma categoría o se dice en qué lugar se cometió el delito, es competente para conocer el que haya prevenido"

Para que no haya ninguna intervención de incompetencia, la propuesta real es tipificar los delitos informáticos dentro del ámbito federal, ya que no hay un espacio material ni una certeza jurídica dentro de los medios electrónicos o informáticos que existen actualmente, además que el Estado, como ya lo hemos visto tiene la facultad para expedir leyes penales junto con sus penas para no violar las garantías individuales, tal es el caso de los artículos señalados.

5.2. PROPUESTA POR LA NECESIDAD DE TIPIFICAR LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL FEDERAL

A lo largo de este capítulo, vimos las legislaciones de otros países; sin embargo, aunque podemos tomar el ejemplo, la situación de México no es tan crítica, es solo la falta de legislación, la necesidad estriba en que debe contemplar el Código Penal Federal de los Estados Unidos Mexicanos, de acuerdo a la Tecnología que se tiene en el país, de acuerdo a las necesidades de las Instituciones de crédito, las empresas, las redes caseras, sistemas de búsqueda, páginas de las diferentes dependencias de gobierno.

El título de este trabajo denota materia federal, cabe mencionar que un hacker puede, como ya vimos, triangular la información, una explicación mas detallada de esto; es cuando la persona en cuestión se encuentra físicamente en Monterrey, y puede engañar al sistema que cibernéticamente está en Cancún Quintana Roo, y esta traspasando un dinero de una cuenta del Distrito Federal a Reynosa, es muy engañoso el espacio informático y el cibernético, sin en cambio, debemos empezar con una iniciativa para reformar el Código Penal Federal de México, además de que avanzamos jurídicamente, empezamos a evolucionar en cuanto a estar en vanguardia ante otros países que son tercermundistas como nos han catalogado.

Además de que debemos estar preparados a los avances, y que podemos ser atacados en cuestiones personales, ya que si observamos en el primer capítulo tratamos sobre los antecedentes de los hackers empezaron cuando se inventó el teléfono, con esto damos a entender que si lo pudieron hacer ante un sistema tan rudimentario como de ese entonces, pueden llegar a buscar formas más complejas como las que se manejan ahora.

Por Internet, en las páginas de los hackers, además de darte trucos para entrar a paginas establecidas por grandes emporios, te facilitan virus, bombas, caballos de Troya, entre muchas cosas que te dan para que ataques a otras personas por simple maldad, es por esto que es urgente, y necesario regular esto de manera federal; existe otro problema que empiezan a tratar de bloquear los avanzados teléfonos móviles, que ahora ya tienen acceso a la red por vía satelital, y además de esto, los Crackers piden información que otros usuarios dan tan fácilmente, por ejemplo las tarjetas de teléfonos celulares, están investigando como romper la seguridad de la red de Telcel, para poder ingresar crédito a los teléfonos celulares.

Propuesta que tenemos es la de tipificar la regulación de los delitos informáticos, y que la población que utiliza el Internet, las computadoras, las personas que tienen redes, sistemas de bancos, de gobierno, grandes redes de Universidades, que es la mayoría de las personas que viven en este país, estén enteradas de los alcances de la Tecnología. Es necesario mencionar que aunque se tipifique la regulación de los delitos informáticos, aun quedan cosas por hacer, como dar solución a como se indagarán estos delitos, quienes son las personas calificadas para esto, y el como podemos informar a toda la población con el problema que nos aqueja, pero la regulación y la tipificación de los mismos es un avance jurídico, y con algo debemos empezar.

C O N C L U S I O N E S

PRIMERA.- A lo largo de esta investigación, nos damos cuenta que la informática es un medio de subsistencia de la vida cotidiana y para nosotros se ha vuelto una necesidad; por la multiplicidad de cosas que se pueden realizar en ella, desde algunas operaciones sencillas, planos, cuentas, bitácoras, cartas, currículos entre muchas otras más: se menciono la diferencia entre las tareas de cálculo y gestión, y como consecuencia de esto de desarrollaron los aparatos y herramientas para la realización de éstas, hasta llegar a las computadoras, que trajeron consigo una ciencia para ayudar al hombre y la sociedad, que es la informática; de esto se desprende que con ayuda de la herramienta que ahora utilizamos, se han implementado maneras de cometer delitos de una manera por medio de un medio electrónico, llamado internet.

SEGUNDA.- Dentro de las computadoras existen las caseras y grandes redes, por ejemplo las de los bancos, dependencias del gobierno, etcétera; viendo el lado bueno de ello comentaremos el lado malo, que son las personas que intervienen, modifican, destruyen, contaminan entre otras cosas, la información establecida en las computadoras, caseras, o en las redes dentro de nuestro país, a estas personas se les denominan hackers, Crackers, husmeadores, entre otros, dependiendo su actividad, que ya precisamos.

TERCERA.- La importancia de la tipificación de los delitos informáticos dentro de la legislación de los Estados Unidos Mexicanos, se deriva de la realidad que vive nuestro país, el avance tecnológico, y que la falta de regulación dentro de la

legislación mexicana, se hondaría más en el tema pero en esta investigación, se limita a la tipificación de la regulación de los delitos informáticos dentro del país.

CUARTA.- Muchos de los autores consultados dentro de este trabajo de investigación, se limitan a reconocer la existencia de delitos informáticos, dan clasificaciones, y todo esto, pero podemos hacer algo más de acuerdo con sus definiciones acorde con el fin primordial del tema, varias legislaciones de diferentes países, hacen leyes especialmente para Delitos informáticos, una de las cosas que proponemos, es que dentro de cada tipo penal, se aumente la agravante que de por medio informático, cibernético, u otro similar ya sea de banda ancha o de fibras ópticas, cometa un delito, es decir, que por ejemplo en el Código Penal Federal para los Estados Unidos Mexicanos, en su artículo 386, menciona la descripción y los elementos por los que se conforma el delito de Fraude y las penas que se seguirán atendiendo al monto del valor de lo defraudado, y en el artículo que precede menciona las hipótesis o supuestos en los que incurre el probable responsable, a nuestro punto de vista faltaría al que engañe por medio de un medio electrónico, cibernético, por medio de satélite, comunicaciones móviles, fibra óptica, banda ancha o demás, engañe y saque provecho del error en que otra persona se encuentre; se haga de una cosa ilícitamente o alcanza un lucro indebido.

QUINTA.- Para que este tipo de conductas no se quedaran impunes y sean más fáciles de encuadrarlas a un tipo penal más específico, y que de acuerdo con el Maestro Cesar Augusto Osorio y Nieto, en su obra "Delitos Federales" que menciona sobre el poder penal del Estado, que es la facultad y el deber de emitir normas jurídicas que tipifiquen conductas delictivas y proceder a la aplicación de tales normas a este caso en concreto, sancionando con la pena correspondiente a los

infractores de mencionados preceptos, y que tiene como finalidad la mejor convivencia social.

SEXTA.- Brindar seguridad jurídica para el uso de la información; la tipificación de los delitos cometidos con l uso de herramientas informáticas, la protección de los derechos de autor, propiedad industrial, el uso de la informática, debemos contar con un marco legal, completo y coherente que de confianza.

SÉPTIMA.- La determinación de acceso a Internet de contenido nacional, en español, en proyectos tendientes con el analfabetismo informático y a propiciar la promoción a la cultura tecnológica.

OCTAVA.- Puede, en un momento dado, connotarse un poco confusa la tipificación de los delitos informáticos, por que poseen pocos los conocimientos informáticos, sin embargo con este trabajo se delimita muy bien las conductas que pueden tomar de base para lograrlo.

NOVENA.- La falta de cultura informática es un factor determinante en la sociedad, por lo que se requieren mayores conocimientos en tecnologías de la información para permitir tener un marco de referencia aceptable para el manejo de dichas soluciones.

DÉCIMA.- Plantear un reto a los profesionales de la informática para realizar esfuerzos encaminados a robustecer los aspectos de seguridad e integridad de la información.

DÉCIMO PRIMERA.- Crear consciencia sobre los actos que tenemos todos los usuarios de internet a no creer, ayudar y ser atacados fácilmente por estos navegadores del Internet.

BIBLIOGRAFÍA

- BEER, Stafford. Cibernética y Administración. México, 1965, página 21

- DEL PONT K., Luis Marco y NADELSTICHER Mitrania, Abraham, Delitos de cuello blanco y reacción social, Instituto Nacional de Ciencias Penales. México. 1981.

- DUFFY Tim, Introducción a la Informática, traductor Eduardo de la Calle, Grupo Editorial Iberoamericana S. A. de C. V., México, Distrito Federal. Pp. 1-3.

- GARCÍA MAYNES Eduardo. Introducción al Estudio del Derecho. Editorial Porrúa. México 1999, 50ª Edición. P.p. 322.

- HANCE, Olivier. Leyes y Negocios en Internet. México. De. Mc Graw Hill Sociedad Internet. México. 1996.

- HERNÁNDEZ Claudio. Hackers Los piratas del Chip y de Internet. Página 86. (Sin Pie de Imprenta)

- INSTITUTO DE INVESTIGACIONES JURÍDICAS, Enciclopedia Jurídica Mexicana, editorial Porrúa, UNAM, Tomo II, Primera Edición, México 2002.

- INSTITUTO DE INVESTIGACIONES JURÍDICAS, Enciclopedia Jurídica Mexicana, editorial Porrúa, UNAM, Tomo IV, Primera Edición, México 2002

- FIX- ZAMUDIO, Héctor. Metodología, docencia e investigación jurídicas, Editorial Porrúa. Novena Edición. México 2001.

- MIR PUIG S (Comp.) Delincuencia Informática. Promociones y Publicaciones Universitarias. Barcelona, 1992.

- OSORIO Y NIETO, César Augusto. Delitos Federales, Editorial Porrúa, México 2003, Sexta Edición, pp. 3.

- TELLES VALDÉS, Julio. Derecho Informático. 2ª Edición. México. Ed. Mc Graw Hill. 1996. Pp 103-104.

- TELLES VALDÉS, Julio. Derecho Informático. 3ª Edición. México. Ed. Mc Graw Hill. 2003. Pp 211.

- ZAVALA, Antelmo. "El impacto social de la informática jurídica en México". Tesis. México. UNAM. 1996.

LEGISLACIÓN.

- Constitución Política de los Estados Unidos Mexicanos. Editorial Porrúa 139ª Edición. México. 2002.

- Tratado de Libre Comercio (TLC). Parte 3. Diario Oficial de la Federación. Lunes 20 de Diciembre de 1993.

- Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal. Reformas hasta el 20 de Enero de 1997.

- Ley de Vías Generales de Comunicación. Colección Porrúa. Editorial Porrúa. 23ª Edición. México 1993.

- Nuevo Código Penal para el Distrito Federal. Editorial Porrúa. México. 2004.

- Legislación sobre propiedad industrial e inversiones extranjeras. Colección Porrúa. Editorial Porrúa 19ª Edición. México. 1995.

- Ley Federal del Derecho de Autor. Diario Oficial de la Federación. Martes 24 de Diciembre de 1996.

- Código Penal del Estado de Sinaloa. Editorial Anaya. México.1996.

- Código de Procedimientos Penales del Estado de Sinaloa. Editorial Anaya. México.1996.

- Exposición de Motivos de la Comisión de Justicia de la Cámara de Diputados Doc. 184/LVI/96 (I. P. O. Año III) DICT. Durante el análisis de la Ley Federal de Derecho de Autor.

- Exposición de Motivos de la Comisión de Justicia de la Cámara de Diputados Doc. 223/LVI/97 (I. P. O. Año III) DICT. Que contiene el proyecto de Derecho por el que se reforman la fracción III del artículo 231 de la Ley Federal de Derecho de Autor, así como la fracción II del Artículo 424 del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal.

ECONOGRAFÍA.

- CALLEGARI, Lidia. "Delitos informáticos y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Boliviana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985. p. 115.

- FERNÁNDEZ Calvo, Rafael. "El tratamiento de llamado "delito informático" en el proyecto de Ley Orgánica del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática) en informática y Derecho, pp. 1150.

- GORDON MEEK, James. "Hacker al ataque" en Selecciones de Reader´s Digest. Marzo del 2003. México. Pp. 95-104.

- LIMA DE LA LUZ, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Editorial Porrúa. No 1-6. Año L. Enero-Junio 1984. pp. 100.

- SARZANA, Carlo. "Criminalitá e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Año 1. Italia. P 53.

- NACIONES UNIDAS. Revista Internacional de Política Criminal. Manual de las Naciones Unidas sobre Prevención del Delito y Control de Delitos Informáticos. Oficina de las Naciones Unidas en Viena. Centro de Desarrollo Social y Asuntos humanitarios. Nos. 43 y 44. Naciones Unidas, Nueva Cork. 1994.

- NACIONES UNIDAS. Prevención del Delito y Justicia Penal en el contexto del Desarrollo, realidades y perspectivas de la cooperación internacional. Documento de trabajo preparado por la Secretaría (A/CONF. 144/5). Octavo Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente. La Habana, Cuba, 27 agosto-7 septiembre 1990.

- NACIONES UNIDAS. Octavo Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente. La Habana, Cuba, 27 agosto-7 septiembre 1990. Nueva York, Naciones Unidas 1991.

- Primer Congreso Internacional de Delitos Cibernéticos. España. 1982.
- "Tratado de Libre Comercio", Novedades, México, jueves 20 de agosto de 1992.
- ICONOMIA, "Incurrieron TAESA y Muebles Dico en delitos informáticos", La Jornada, México, sábado 12 de abril de 1997.
- "Tarjetas superfraudes". El Sol de México Mediodía. México, lunes 21 de abril de 1997. Primera plana.
- "Aprobó el Senado reformar a la Ley sobre Derechos de Autor y el Código Penal", El Universal, México, martes 29 de abril de 1997.
- http://www.wipo.int/about-wipo/es/dgo/pub487.htm, 03 de febrero del 2004.
- http://www.apc.org/espanol/rights/lac/docs.shtml?-1-"privacidad", 24 de febrero del 2003.
- http://www.kpmg.com.ar/services_fraud.html, 23 de marzo del 2004.
- http://es.gsmbox.com/news/mobile_news/all/3689.gsmbox, 22 de marzo del 2004.
- http://www.geocities.com/ruben_apg/abacoalordenadorelectronico.htm, 17 de Octubre del 2003.
- http://www.geocities.com/ruben_apg/losprimerosanos.htm, 22 de Diciembre del 2003.

- http://orbita.starmedia.com/fortiz/LasTelecomunicaciones/Tema01HistoriaDeLasTelecomunicaciones.htm, 29 de diciembre del 2003.
- http://www.funcionpublica.gob.mx/ocde/, 27 de Marzo del 2004.
- http://www.aaba.org.ar/bi180p43.htm, 1 de Abril del 2004.
- http://assembly.coe.int/, 5 de Abril de 2004.
- http://www.dpi.bioetica.org/softnotas3.htm, 3 de Abril del 2004.
- http://www.aadat.org/delitos_informaticos20.htm, 2 de Abril del 2004.
- www.htmlweb.net/seguridad/tesis/Cap4.pdf, 6 de Mayo del 2004.
- www.stj-sin.gob.mx/Delitos_Informaticos2.htm, 8 de Marzo del 2004.
- www.usm.edu.ec/eticainformatica/estado%20arte/cap%20II%20%20regimen_juridico.PDF, 13 de Enero del 2004.
- http://www.monografias.com/trabajos12/tsinnom/tsinnom2.shtml, 24 de Febrero del 2004.
- www.alfa-redi.org/upload/documento/110801LA%20AUTORIA%20MEDIATA%20(PATRICIA%20COTRONE), 21 de Marzo del 2004.
- http://www.tribunalmmm.gob.mx/biblioteca/almadelia/Cap4.htm, 14 de Abril del 2004.
- http://www.libardo.50megs.com/DELINFOI_A.htm, 30 de Abril del 2004.

- http://www.presidencia.gob.mx/biblioteca/almadelia/Cap4.html, 14 de Abril del 2004.

- www.omc.onu.sa/es/html, 15 de Febrero del 2004.

- www.camaradediputados.gob.gob.mx, Enero del 2003.

- www.monografías.com/trabajos12/tsinnom2.shtml, 24 de Febrero del 2004.