296

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES "ACATLAN"

"LA NECESIDAD DE REGULARIZACIÓN Y PARTICULARIZACIÓN DE LOS DELITOS INFORMÁTICOS EN LOS CÓDIGOS PENALES DEL DISTRITO FEDERAL Y EL ESTADO DE MÉXICO."

SEMINARIO TALLER EXTRACURRICULAR

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN DERECHO

P R E S E N T A

FRANCISCO RENATO ALFREDO DE LA PEÑA GONZÁLEZ

ASESOR: LIC. JORGE GUILLERMO HUITRON MÁRQUEZ

NAUCALPAN, DE JUÁREZ EDO. MEX. 2001

AGRADECIMIENTOS

A la Universidad Nacional de México, y en particular a la Escuela Nacional de Estudios Profesionales "ACATLAN", por haberme dado varios de los mas grandes y apreciados tesoros que tengo, gracias por darme los conocimientos necesarios para enfrentar mi vida, por haberme dado muchos de los mejores momentos y amigos que he tenido y por haberme permitido conocer a mi futura esposa.

A mi Madre Sra. Lucina González Molina, por que todo lo que soy y todo lo que tengo se lo debo a ella, por que de ninguna manera mi vida pudo haber sido mejor sin tenerla a mi lado, por que no me alcanzan las palabras para expresar el orgullo y el amor que siento por ella, por que siempre ha dado todo por sus hijos, por que ha sido el mejor ejemplo que pude haber tenido y por que es ella la única responsable de este logro.

A mi novia Yael Vargas Baños, por estar a mi lado, por enseñarme que uno siempre puede ser mejor, por haber cambiado mi vida extraordinariamente, por todo el amor y la felicidad que me ha dado, por aguantarme y por aventurarse conmigo en la odisea mas dulce y maravillosa que he iniciado en mi vida.

A mi Hermana Stella de la Peña González y mi Cuñado Emilio Ramírez Muñoz, por que siempre han estado conmigo, por disfrutar mis alegrías y por sufrir mis problemas como si fueran de ellos y por habernos obsequiado a Mercedes, que ha sido la alegría de nuestra familia.

A todos mis Maestros y en particular a los Lics. Jorge Guillermo Huitron Márquez, Rafael Chaine López, Aarón Hernández López, Moisés Moreno Rivas y Dr. Javier Grandini González, por la paciencia que tuvieron conmigo en el seminario, por haber compartido tantos y tantos conocimientos con nosotros y en particular por haberme permitido conocerlos además de cómo maestros como personas y como amigos.

A mi hermano Oscar Morón López, por que juntos aprendimos que la amistad se puede superar y magnificarse, por que cuando todo falla el sigue aquí.

A todos mis familiares, amigos, amigas, compañeros de trabajo, compañeros de la Universidad y del Seminario, por haberme apoyado, ayudado y sobre todo aguantado, que de verdad, a veces es una tarea muy difícil.

A todos un millón de Gracias.

ANTECEDENTES

ANTECEDENTES DEL TEMA .- el primer antecedente al que deberemos de referirnos lo encontramos, en el año 1949, apenas un año después de que en Estados Unidos, se da a conocer la obra "Cibernética", de Norbert Wiener, obra la cual motiva al juez norteamericano Lee Loeverger a escribir un artículo titulado "El próximo paso", y en la cual por primera vez se utiliza el término "Jurimetría" primer antecedente del actual derecho informático y con lo cual se vislumbraba el surgimiento de una nueva rama del Derecho, encargada de las aplicaciones "cibernéticas" a la información jurídica.

El Juez Loeverger circunscribió la utilidad y fin de la jurimétrica al estudio y la racionalización del Derecho a través de la aplicación de la automatización, elevando inclusive una propuesta de aplicación, limitada únicamente al derecho fiscal.

En esto encontramos brevemente la primera aplicación y antecedente de cómo se intento emplear las nuevas tecnologías al ámbito jurídico.

En 1958, en Francia el jurista, Lucien Mehl, desarrolla el trabajo titulado "Automatización en el mundo legal" exponiendo puntos de vista relativos a lo que se dio en nombrar las "máquinas leyes", calificando las mismas en dos categoría distintas: máquinas documentales y máquinas de consulta.

En 1960, en Washington E. U. A., se da a conocer la primera complicación de leyes federales y estatales referidas a Bases de Datos de los Hospitales, compilación a la cual se le reconoce como la primera base de datos en materia jurídica en la historia, en su momento este trabajo tuvo como finalidad el demostrar la viabilidad de aplicaciones informáticas y su utilidades prácticas en el campo jurídico.

Al principio de los años 60 se dan a conocer los primeros sistemas de tipo comercial destinados a la legislación y la jurisprudencia.

En 1962, en Francia Philippe Dreyfus inventó un termino nuevo: Informatique, uniendo de manera simplificada los términos "información" y "automática""

Para 1963 se publica un artículo, en el que se dan a conocer ideas de gran interés sobre la aplicabilidad de la Cibernética al Derecho; este articulo conocido como el de Knapp (nombre de su autor), no tuvo mayor relevancia ya que fue escrito en checoslovaco; sin embargo este inconveniente fue superado posteriormente al publicar el mismo autor un posterior estudio titulado "Stadd and Reich" publicado en alemán.

Estos antecedentes continúan en Italia, donde encontramos el trabajo de dos juristas de nombres Frosini, escritor del libro titulado "Cibernética,

Diritto e Societá" publicado en 1968 y Mario Losano, quién se encargo de recopilar y publicar todas las notas de la cátedra que impartía denominada "Introducción a la Informática Jurídica".

Este proceso continuo en los sesentas hasta establecer que los bancos de datos que se utilizaban en ese entonces se podían utilizar no solo para almacenar y obtener información de una manera sencilla, sino que algunas actividades jurídicas tales como certificaciones, atribuciones de juez competente, elaboración de sentencias, podían ser realizadas fácilmente auxiliándose de la informática, originándose en consecuencia la Informática Jurídica de Gestión, la cual evoluciono para los años setentas en Informática Jurídica Decisional.

Ya con la aparición de las primera computadoras se introduce la automatización en los estudios de operadores jurídicos (jueces, abogados, fiscales, asesores jurídicos) y las redes de información penetran tempestuosamente en las administraciones públicas.

Este desarrollo continua a pasos agigantados hasta que alrededor del año de 1991, nace la World Wide Web (www por sus siglas, conocida en español como la súper carretera de la información).

Ya el nacimiento del comercio electrónico se sitúa en 1995 precisamente al utilizar el Internet para el desarrollo de negocios y con ello la mayoría de los países del mundo en mayor o menor medida comienzan a legislar respecto al tema.

JUSTIFICACIÓN

En contraparte a los muchos beneficios y adelantos que el desarrollo de la informática aporta a la humanidad, nos encontramos con la inconveniencia que casi siempre acompaña a la solución. Las conductas delictivas y punibles que el gran avance tecnológico ha generado, y que han encontrado un espacio tan prolífico en el campo de la informática.

La tecnología aplicada a la informática se ha desarrollado de una manera tan vertiginosa, que ha dejado muy rezagado al ámbito jurídico mundial y muy en particular aventajo a nuestros legisladores creando lagunas que no han podido ser cubiertas, lo cual es aun más notorio, si tomamos en cuenta que no se ha podido definir uniformemente el concepto de delito informático, situación la cual obviamente será tratada a lo largo del desarrollo de nuestro trabajo.

En los inicios del desarrollo de la Informática y al detectarse las primeras violaciones al derecho intrínseco a ella, se pretendió desarrollar sistemas de seguridad que proporcionaran la inviolabilidad de los mismos (sistema tolerante a fallos, programas antivirus capaces de 'inmunizar' o eliminar el virus del ordenador, claves de acceso con secuencias confidenciales etc.) sin embargo el

desarrollo de estos sistemas de seguridad únicamente han representado un reto, para los delincuentes dedicados a la violación de los mismos, por lo que diversos países se dieron a la tarea de desarrollar el derecho informático, pero en el caso de nuestro país estos esfuerzos han sido limitados ya sea por la creación de leyes demasiado particularizadas hacia un solo tipo de delito o por que los congresos estatales se han encargado de regular su ámbito de competencia sin que exista la comunión necesaria para que se le dé, el carácter de federal a las leyes necesarias.

El tema resulta por demás apasionante ya que el pretender regular los delitos clasificables como informáticos, necesariamente requiere que los encargados de establecer las conductas delictivas y sus correspondientes castigos y medidas de prevención, estén un paso adelante del posible delincuente, tarea por demás difícil ya que, el citado desarrollo informático ha abierto la puerta a conductas antisociales y delictivas, que se manifiestan de formas que hasta ahora no era posible imaginar.

Los sistemas computacionales ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales, merced a algunos individuos sin escrúpulos que traspasando los límites de la seguridad realizan actos ilícitos, lo cual ha generado una gran preocupación por parte de los usuarios de este medio informático, dando como resultado la tarea a la que se han encomendado muchísimas personas, consistente en buscar una solución al problema de la delincuencia informática.

Esta tarea es por demás importante a nivel mundial si se analiza desde el punto de vista del axioma **DELITO QUE NO SE CASTIGA SE REPITE.**

En este orden de ideas y a lo largo del presente trabajo trataremos de establecer las concordancias y diferencias que a lo largo del mundo los organismos judiciales tienen respecto al tema, ya que estas conductas ilícitas en las que se usa la computadora, de un país a otro tienen diferentes denominaciones tales como ***"delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora". "delincuencia relacionada con el ordenador".***

Y por supuesto que se habrán de tomar en cuenta siete puntos básicos que motivan esta investigación y que son características comunes de los delitos informáticos:

- **Tienen como consecuencia primordial el provocar serias pérdidas económicas, a corporaciones publicas y privadas ya que casi siempre producen "beneficios de más de cinco cifras a aquellos que los realizan.**

- **Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.**
- **Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.**
- **Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.**
- **Ofrecen facilidades para su comisión a los menores de edad.**
- **Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.**
- **Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.**

Por otra parte será necesario entrar al análisis denominación y estudio de los diferentes organismos internacionales que se han dedicado a la propuesta de leyes que a nivel mundial regulen y castiguen las conductas delictivas derivadas del desarrollo informático, particularizando por supuesto este tema a nivel de cada nación y en concreto respecto a nuestro país.

En una óptica limitada se podría pensar que nuestro país esta exento de una regulación especial referente a los delitos informáticos, dado el muy pequeño desarrollo tecnológico del que innegablemente adolece nuestra nación, pero si tomamos en cuenta las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las cuales ascienden a un valor superior de mil millones de dólares por concepto de piratería, fácilmente se puede concluir la utilidad de este estudio.

El delito informático ha tratado de ser encuadrado a lo largo del mundo dentro de los delitos y figuras típicas de carácter tradicional, ergo robo, fraude, sabotaje, abuso de confianza etc. Pero la forma de comisión de este tipo de delitos rebasa por mucho el tipo tradicional y las posibilidades del uso ilícito de las computadoras fuera del citado marco tradicional de la comisión de los delitos, pone en grave riesgo los procesos seguidos en contra de los transgresores dada la fragilidad de los autos de formal prisión o de sujeción a proceso siendo esto en gran parte lo que propiciado la necesidad de regulación.

OBJETIVOS

Para lograr tener los elementos suficientes que nos permitan comprender los delitos informáticos y su problemática, se perseguirán los siguientes objetivos.

1.- A fin de preparar el marco histórico del trabajo se detallara el inicio del Internet o World Wide Web así como de las aplicaciones practicas de la informática

2.- Establecer el concepto y marco jurídico teórico y diferentes tipos de los delitos informáticos.

3.- Justificar la necesidad de la regulación penal de los delitos informáticos dada la gravedad de la conducta ilícita en sí, y las implicaciones que trae aparejada.

4.- Proceder al estudio y análisis de los diversos organismos mundiales y ordenamientos legales encargados de la regulación y castigo de los delitos informáticos.

5.- Analizar la situación nacional imperante en cuanto a la prevención regulación y castigo de los delitos informáticos.

6.- Una vez que se hayan realizado los análisis respectivos, y cubierto los objetivos anteriores, elevaremos propuestas para hacer mas seguro el uso de la informática en nuestro país, para prevenir los abusos en ella y en su caso para castigar las conductas delictivas relacionadas con la informática.

HIPOTESIS

Si tomamos en cuenta que en nuestro país, varios ordenamientos legales regulan diferentes tipos de conductas que se pueden tipificar como delitos informáticos, **tenemos que lamentablemente ni en el Distrito Federal ni en el Estado de México se tipifican como delitos las conductas ilícitas relacionadas con el informática su tratamiento prevención o castigo** y que el estado de Sinaloa a través de su Congreso Local ha legislado sobre el tema de *delitos informáticos*, tipificando una amplia variedad de los mismos y estableciendo las sanciones correspondientes. Indudablemente es necesario que con objeto de que se evite un conflicto de competencia entre los congresos locales y el de la Unión, éste ultimo con base en las facultades que la Constitución Federal le confiere, establezca los criterios necesarios para regular prevenir y en su caso castigar lo relacionado a los *delitos informáticos*, estableciendo la jurisdicción federal y local de estos ilícitos.

ANTECEDENTES DE INVESTIGACIÓN AL TITULO.- Al realizar una investigación en las bibliotecas de universidades aledañas a la E.N.E.P. ACATLAN, en busca de antecedente al titulo propuesto, se encontró que el tema como se propone no ha sido desarrollado, la investigación comprendió los siguientes centros educativos: Grupo Sol plantel lomas verdes, Universidad del valle de México plantel Lomas verdes, y Universidad Iberoamericana, y por lo que hace a la biblioteca de la E.N.E.P. ACATLAN, no se encontró Tesis alguna que hiciera referencia al tratamiento de los delitos informáticos en los códigos penales del Estado de México y del Distrito Federal, siendo el común denominador en los trabajos enfocados al derecho informático, La regulación de publicidad en Internet, el desarrollo del E-comerce y la validez de la firma electrónica en diferentes tipos de contratos y actos.

METODOLOGÍA DE LA INVESTIGACIÓN.- la metodología a seguirse será básicamente Bibliográfica y Hemerográfica.

MARCO TEÓRICO.- Constitución y Tratados Internacionales, Tratado de Libre Comercio de América del Norte (TLC), Códigos Penales del Estado de México y del Distrito Federal, Ley Federal del Derecho de Autor, Código Penal Federal.

CAPITULO I
CONCEPTOS GENERALES DEL DERECHO INFORMATICO

1.1.- RESEÑA HISTORICA DEL DERECHO INFORMATICO.

Para iniciar con nuestro estudio quisiéramos tratar el origen del derecho informático o Informática Jurídica su desarrollo y situación actual ya que esto es requisito necesario para establecer el marco de referencia de los delitos informáticos.

Existen muchos y muy distintos conceptos y definiciones aplicables al derecho informático o informática jurídica siendo algunas de las de mayor relevancia los siguientes, en primer lugar tenemos la que nos ofrece el **Dr. Héctor Fix Fierro** la cual establece lo siguiente: "La Informática Jurídica debe entenderse como el conjunto de estudios e instrumentos derivados de la aplicación de la Informática al Derecho, o mas precisamente, a los procesos de creación, aplicación y conocimiento del Derecho" así tenemos que el **Dr. Antonio Pérez Luño,**[1] define al derecho informático como "la aplicación de los sistemas informáticos a las distintas esferas del Derecho, sin embargo debería de añadirse a este concepto el estudio, análisis y aprovechamiento de los recursos que ofrece la informática al quehacer jurídico, mientras que el jurista argentino, **Daniel Ricardo Altmark**[2] (Abogado argentino experto en la materia) define a esta disciplina indicando que: "Derecho Informático es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática".

La Informática esta presente en todas las ramas del Derecho, o mejor dicho es necesaria la presencia del derecho en todas las ramas de la Informática, y la misma como objeto de Derecho, requiere del establecimiento de nuevas reglas jurídicas en materias tales como: el uso, promoción y protección del Software (programas de computación) desarrollado con fines comerciales, adecuar, regular y establecer el valor probatorio del documento y firma electrónica, establecer los medios de defensa de personas físicas y morales para los supuestos de: irrupción, destrucción y propagación de la información contenida en ordenadores públicos y privados y por supuesto lo tendiente a prevenir y castigar los delitos informáticos, por supuesto que lo anterior es una pequeñísima muestra de las soluciones que los estudiosos del derecho informático tienen que aportar a este ámbito.

Lo anterior no resultaría mayor problema si no nos enfrentáramos al hecho de que por lo regular, el desarrollo del derecho informático

---

[1] PÉREZ LUÑO, Antonio-Enrique. "Manual de informática y derecho", Editorial Ariel S.A., Barcelona, 1996, Págs. 69 a 81.

[2] Altmark, D.R. Informática y Derecho: Aportes de doctrina internacional. Volumen 6: Régimen Jurídico de los Bancos de Datos. Buenos Aires 1998.

guarda intima relación con el grado de difusión y desarrollo de la tecnología informática en el país en cuestión y más aún con el tipo de política informática aplicada.

Debido a lo anterior es que encontramos pocas pero muy loables iniciativas en América Latina relacionadas al estudio y desarrollo del derecho informático, como por ejemplo el establecimiento e inclusión dentro del programa de derecho de diversas universidades, de cátedras especializadas en la materia, ya sea en modalidades de cursos regulares o como materias opcionales. Siendo pionera en la difusión de este tema, la Universidad de Buenos Aires, en Argentina.

Mas no debemos pasar por alto a Brasil como uno de los primeros países que en Latinoamérica enfocaron sus esfuerzos por establecer un ordenamiento legal relativo a un régimen especial de protección jurídica del software (programas de computación).

Sin embargo de un modo generalizado en toda Latinoamérica los esfuerzos legislativos, se han centrado básicamente a la búsqueda de soluciones jurídicas tendientes a la protección de los programas de computación y de los derechos de sus autores, esto fácilmente explicable si se toma en cuenta el poder económico de las industrias desarrolladoras de esto programas y la presión que ejercen en los gobiernos de América Latina.

Lo cual ha contribuido también a limitar el desarrollo generalizado de los demás aspectos del derecho informático e inclusive de algunos otro ilícitos que resultan igual o mas preocupantes que el uso ilegal de software.

De esta manera es imposible hablar de un desarrollo igualitario o de prácticas jurídicas homogéneas, ya que en América Latina aun se puede considerar que el derecho informático apenas ha dejado atrás el proceso de gestación, para iniciar muy lentamente su maduración, proceso en el cual resulta preponderante la participación de los estudiosos del derecho para el desarrollo de la legislación y doctrina jurídica que ordene debidamente todas las relaciones jurídicas derivadas de las relaciones usuario-tecnología-derecho.

Sin embargo para entender la situación actual del derecho informático es necesario establecer su antecedentes. Así las cosas el primer antecedente al que deberemos de referirnos lo encontramos, en el año 1949, apenas un año después de que en Estados Unidos, se da a conocer la obra "Cibernética", de Norbert Wiener, obra la cual motiva al juez norteamericano Lee Loeverger a escribir un artículo titulado "El próximo paso", y en la cual por primera vez se utiliza el término "Jurimetría" primer antecedente del actual derecho informático y con lo cual se vislumbraba el surgimiento de una nueva rama del Derecho, encargada de las aplicaciones "cibernéticas" a la información jurídica.

El Juez Loeverger circunscribió la utilidad y fin de la jurimétrica al estudio y la racionalización del Derecho a través de la aplicación de la automatización, elevando inclusive una propuesta de aplicación, limitada únicamente al derecho fiscal.

En esto encontramos brevemente la primera aplicación y antecedente, de cómo se intento emplear las nuevas tecnologías al ámbito jurídico.

En 1958, en Francia, el jurista Lucien Mehl, desarrolla el trabajo titulado "Automatización en el mundo legal" exponiendo puntos de vista relativos a lo que se dio en nombrar las "máquinas leyes", calificando las mismas en dos categoría distintas: máquinas documentales y máquinas de consulta.

En 1960, en Washington E. U. A., se da a conocer la primera complicación de leyes federales y estatales referidas a Bases de Datos de los Hospitales, compilación a la cual se le reconoce como la primera base de datos en materia jurídica en la historia, en su momento este trabajo tuvo como finalidad el demostrar la viabilidad de aplicaciones informáticas y su utilidades prácticas en el campo jurídico.

Al principio de los años 60 se dan a conocer los primeros sistemas de tipo comercial destinados a la legislación y la jurisprudencia.

En 1962, en Francia Philippe Dreyfus inventó un termino nuevo: Informatique, uniendo de manera simplificada los términos "información" y "automática""

Para 1963 se publica un artículo, en el que se dan a conocer ideas de gran interés sobre la aplicabilidad de la Cibernética al Derecho; este articulo conocido como el de Knapp (nombre de su autor), no tuvo mayor relevancia ya que fue escrito en checoslovaco; sin embargo este inconveniente fue superado posteriormente al publicar el mismo autor un posterior estudio titulado "Stadd and Reich" publicado en alemán.

Estos antecedentes continúan en Italia, donde encontramos el trabajo de dos juristas de nombres Frosini, escritor del libro titulado "Cibernética, Diritto e Societá" publicado en 1968 y Mario Losano, quién se encargo de recopilar y publicar todas las notas de la cátedra que impartía denominada "Introducción a la Informática Jurídica".

Este proceso continuo en los sesentas hasta establecer que los bancos de datos que se utilizaban en ese entonces se podían utilizar no solo para almacenar y obtener información de una manera sencilla, sino que algunas actividades jurídicas tales como certificaciones, atribuciones de juez competente, elaboración de sentencias, podían ser realizadas fácilmente auxiliándose de la

informática, originándose en consecuencia la Informática Jurídica de Gestión, la cual evoluciono para los años setentas en Informática Jurídica Decisional.

Ya con la aparición de las primera computadoras se introduce la automatización en los estudios de operadores jurídicos (jueces, abogados, fiscales, asesores jurídicos) y las redes de información penetran tempestuosamente en las administraciones públicas.

Este desarrollo continua a pasos agigantados hasta que alrededor del año de 1991, nace la World Wide Web (W.W.W. por sus siglas, conocida en español como la súper carretera de la información).

Ya el nacimiento del comercio electrónico se sitúa en 1995 precisamente al utilizar el Internet para el desarrollo de negocios.

1.2- HISTORIA DEL SURGIMIENTO DE INTERNET Y SU DESARROLLO EN MÉXICO

La primera pregunta que cualquier persona que no se encuentre familiarizada con Internet o que maneje el mismo en formas relativamente superficial se haría es, ¿que es Internet?

Internet es una gran cantidad de pequeñas redes de computadoras y otras no tan pequeñas que se encuentran interconectadas entre sí, estas redes se encuentran distribuidas por todo el mundo, en la que se puede encontrar información y servicios de todo tipo. Para acceder a esta información se requiere de herramientas que permitan buscar rápidamente la información que se esta buscando a través de todas estas computadoras.

Existen herramientas que permiten el intercambio de correo electrónico con personas en todo el mundo, buscar un archivo o un juego de computadora a través de toda la red, visitar grandes tiendas virtuales en cualquier parte del mundo y realizar compras, consultar las últimas ediciones de las enciclopedias mas prestigiadas, consultar bases de datos públicas, "platicar" con personas en otros lugares acerca de un tema en común o simplemente visitar una cantidad de sitios diferentes sin salir de casa.

En los últimos años se ha echo un gran esfuerzo por hacer más sencilla la búsqueda de información, se han desarrollado interfaces gráficas con las que se pueden realizar las tareas más fácilmente.

Actualmente Internet está formada por aproximadamente mas de treinta millones de usuarios y mas de diez millones de computadoras distribuidas e interconectadas entre sí por todo el mundo con equipo de todas marcas y sistemas operativos tan diferentes entre sí como Unix, OS/2, Novell, o Windows (en sus diferentes versiones) comunicándose entre ellas mediante protocolos como el TCP/IP y algunos otros.

Historia de Internet

Internet fue creada a partir de un proyecto del departamento de defensa de los Estados Unidos llamado DARPANET (Defense Advanced Research Project Network) iniciado en el año de 1969 y cuyo propósito principal era la investigación, desarrollo e implementación de protocolos de comunicación para redes de área amplia (WAN).

Estas investigaciones arrojaron como resultado el protocolo de comunicaciones TCP/IP (Trasmission Control Protocol/Internet Protocol) un sistema de comunicaciones muy sólido y robusto en el cual se integran todas las redes que conforman lo que se conoce actualmente como Internet.

Durante el desarrollo de este protocolo se incrementó notablemente el número de redes locales de agencias gubernamentales y de universidades que participaban en el proyecto, dando origen a la red de redes más grande del mundo, las actividades militares se separaron y se permitió el acceso a la red a todo aquel que lo requiera sin importar de que país provenía la solicitud siempre y cuando fuera para fines académicos o de investigación y que pagara sus propios gastos de conexión, los usuarios pronto descubrieron que la información que se encontraba en la red era muy útil y si cada institución que se conectaba aportaba algo crecería más el acervo de información existente.

Por muy extraño que pueda parecer, no existe ninguna autoridad central que controle el funcionamiento de la red, aunque existen grupos y organizaciones que se dedican a organizar de alguna manera en tráfico y crecimiento de Internet.

Existen tres grupos que tienen un papel muy importante en la organización de Internet, el Internet Archiecture Board (IAB) que son los que controlan los estándares de comunicaciones entre las diferentes plataformas para que puedan funcionar las máquinas y sistemas operativos de diferentes fabricantes sin ningún problema, este grupo es responsable de como se asignan las direcciones y otros recursos de la red. El NIC (Network Information Center) es el grupo encargado de asignar las direcciones y dominios a los solicitantes que desean conectarse a Internet.

Uno de los grupos más importante es el Internet Task Force (IETF) en el cuál los usuarios de Internet pueden expresar sus opiniones sobre cómo se deben implementar soluciones a los problemas operacionales que van surgiendo y como debe cooperar los usuarios para lograrlo.

El enorme crecimiento de Internet comenzó en 1994 cuando compañías con propósitos comerciales comenzaron a conectarse a la red, iniciando una nueva etapa de crecimiento.

Aplicaciones de Internet

Debido al tamaño mundial de la red y la diversidad de empresas, como organismos, instituciones gubernamentales y no gubernamentales, Instituciones educativas, investigadores y personas que se conecten dentro de esta gran telaraña de computadoras; la información ahí almacenada va desde simples paginas personales, pasando por páginas comerciales, lugares que ofrecen diversa información, hasta universidades muy prestigiadas en diversos campos de investigación que presentan estudios realizados por ellos mismos de aspectos tan importantes como el SIDA y diferentes enfermedades que afectan a los seres humanos.

A través de esta misma red de computadoras, se pueden intercambiar mensajes o correos electrónicos con personas tan distantes como sería al otro lado del mundo en cuestión de minutos, con tan solo una llamada local y la dirección electrónica de la otra persona.

Esta gran red de computadoras tiene una gran variedad de usos tanto como el usuario pueda imaginar, solo falta obtener la herramienta necesaria para realizarlo.

Crecimiento de Internet

En fechas recientes ha ocurrido un explosivo crecimiento del tamaño de la red Internet. Hay una cantidad increíble de computadoras interconectadas entre si.

En una encuesta realizada en Enero de 1999, las cifras arrojadas son sumamente interesantes: en Enero existían 20,472.00 servidores conectados a Internet. La estimación hecha en base a dichos datos permite suponer que para estas fechas sea más de 22,000.000 de computadoras las que conformen a Internet. Esta cantidad de máquinas es, por sí mismo, enorme. No obstante, es aun más impresionante el saber que:

La cantidad de computadoras conectadas a Internet se duplica cada seis meses Esto reafirma el crecimiento explosivo de la red.

Nadie puede decir con exactitud la cantidad de usuarios que existen, pero la mayor parte de la personas coincide en el hecho de que hay, al menos, un usuario por servidor.

Se ha extendido el mito de que "hay que estar en Internet", y de que la compañía debe de tener su propio Homepage. También se afirma que Internet es el libro virtualmente infinito y que "todo el saber humano se encuentra en Internet" y el suscrito considera que de no ser así, no dista mucho la época en que esto sea una realidad.

La historia del Internet en México empieza en el año de 1989 con la conexión del Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Monterrey, ITESM hacia la Universidad de Texas en San Antonio (UTSA), específicamente a la escuela de Medicina. Una Línea privada analógica de 4 hilos a 9600 bits por segundo fue el enlace.

Conexiones a BITNET en México

Sin embargo, antes de que el ITESM se conectara a Internet, casi a final de los 80's, recibía el tráfico de BITNET por la misma línea privada. El ITESM era participe de BITNET desde 1986.

Las conexiones se hacían a través de líneas conmutadas. La conexión permanente de esta institución se logró hasta el 15 de Junio de 1987 (a BITNET y posteriormente a INTERNET).

La UNAM se conectó a BITNET en Octubre de 1987.

En Noviembre de 1988 se cambia la conexión permanente que interconectaba equipo IBM con RSCS, a equipos DEC utilizando DECNET. Al cambiar el protocolo se tenía la posibilidad de encapsular tráfico de TCP/IP en DECNET y por lo tanto formar parte de INTERNET.

Al siguiente año, en 1989, se cambió de una a tres líneas. Con ello, se cambió el equipo de interconexión y se incorporaron los equipos de ruteo CISCO. Las conexiones siguieron siendo con la UTSA.

Primeros equipos conectados a INTERNET

La máquina que recibía la conexión de DECNET esa una **Microvax-II** con la dirección 131.178.1.1 (desde Septiembre de 1993 se encuentra fuera de operación en el ITESM, Campus Monterrey). Esta máquina tenía un software que recibía el tráfico de TCP/IP encapsulado en DECNET, lo sacaba y permitía acceder a Internet.

Además de ser el primer nodo de Internet en México, pasó a ser el primer Name server para el dominio .mx.

La UNAM como segundo nodo y su interconexión con el ITESM

El segundo nodo Internet en México fue la Universidad Nacional Autónoma de México, en el Instituto de Astronomía en la Ciudad de México. Esto mediante una conexión vía satélite de 56 Kbps, con el Centro Nacional de Investigación Atmosférica (NCAR) de Boulder, Colorado, en los Estados Unidos de Norteamérica. Por lo tanto, se trataba de una línea digital.

Después de esto, lo que proseguía era una interconexión entre la UNAM y el ITESM (Campus Monterrey), pero lo que funcionó en ese entonces fue un enlace BITNET entre ellos. Claro, usando líneas privadas analógicas de 9600 bps.

El ITESM, Estado de México, se conecta a Internet

El ITESM, en su Campus Estado de México, se conecta a través del Centro de Investigación Atmosférica (NCAR) a Internet. Como la UNAM, obtiene una conexión satelital de 56 kbps, es decir, enlace digital. La función de este enlace es dar servicio a los demás ITESM, diseminados a través de todo el país.

Conexiones posteriores

El ITESM, Campus Monterrey, promovió y logró que la Universidad de la Américas (UDLAP) en Cholula, Puebla y el Instituto Tecnológico y de Estudios Superiores de Occidente (ITESO) en Guadalajara, Jalisco, se enlazaran a INTERNET a través del mismo ITESM.

Aunque sus enlaces eran de baja velocidad, 9600 bps, fue suficiente, en ese momento, para proveer de correo electrónico, transferencia de archivos y acceso remoto.

Debido al crecimiento registrado en Internet, la National Science Fundation en los Estados Unidos, requería de una respaldada red de telecomunicaciones para todos aquellos países que se integraban a Internet, por lo tanto, se tomaron algunas decisiones en México, como la de formalizar el uso de IGRP entre los ruteadores y revisar detalladamente la asignación de ASN (Authonomous Systems).

La Universidad de Guadalajara, obtiene una conexión a Internet con la Universidad de California en los Ángeles. Esta era una línea privada de 4 hilos a 9600 bps. Estaban bajo el dominio de UCLA y con direcciones de IP también de la UCLA.

Las demás instituciones, en ese tiempo, accesaban a Internet por medios conmutados. Tal es el caso de Colegio de Postgraduados de la Universidad de Chapingo, en el Estado de México. El Centro de Investigación en Química Aplicada, con sede en Saltillo, Coahuila. El Laboratorio Nacional de Informática avanzada de Xalapa, Veracruz. Todos ellos se conectaban al ITESM, Campus Monterrey para entrar a Internet.

La Universidad de Guanajuato Precursor de RUTYC en Salamanca, Guanajuato, se enlazaba a la UNAM. El Instituto Tecnológico de Mexicali, en Baja California; se conectaba a la red de BESTNET.

Formación de MEXNET

En este entonces existía un organismo llamado RED-MEX, formado principalmente por la academia, y es donde se discuten las políticas, estatutos y procedimientos que habrían de regir y dirigir el camino de la organización de la red de comunicación de datos de México. Esta debería ser una Asociación Civil.

Es así (después de muchos problemas para reunir a los representantes legales de cada institución) como surge MEXNET, el lugar fue la Universidad de Guadalajara. El Motivo, crear a la asociación civil. El día 20 de Enero de 1992. Los participantes: ITESM, Universidad de Guadalajara, Universidad de las Américas, ITESO, Colegio de Postgraduados, LANIA, CIQA, Universidad de Guanajuato, Universidad Veracruzana, Instituto de Ecología, Universidad Iberoamericana, IT de Mexicali.

Crecimiento del Internet en México

Más tarde, el 1ro. de Junio de 1992, MEXNET establece una salida digital de 56kbps al Backbone de Internet.

El crecimiento de MEXNET fue registrando a usuarios como: U. De G., I.P.N., CINVESTAV, U.A. de C., U. De M. , INAOE, en 1992; UAM, UAG, Universidad Panamericana, CIMIT, UAP, Universidad Autónoma de Chapingo, UAAAN, COMIMSA, UASLP, Universidad Veracruzana, U.A.N.L. y Universidad Autónoma de Puebla entre otros, esto durante 1993.

BAJARED se empieza a formar con las siguientes instituciones educativas, todas ellas de Baja California:

Centro de Enseñanza Técnica y Superior - CETYS.

Centro de Investigación Científica y Educación Superior de Ensenada - CICESE.

Universidad Autónoma de Baja California - UABC.

Colegio de la Frontera Norte - COLEF.

Instituto Tecnológico de Mexicali – ITM

En 1993 el CONACYT se conecta a Internet mediante un enlace satelital al NCAR.

El ITAM hace lo propio el 18 de Enero de 1993.

Es en 1993 cuando la UAM se establece como el primer NAP, al intercambiar tráfico entre dos diferentes redes.

Para finales de 1993 existían una serie de Redes ya establecidas en el País, algunas de ellas:

MEXNET

Red UNAM

Red ITESM

RUTyC, que desaparecería como tal ese mismo año

BAJANET

Red Total CONACYT

SIRACyT, un esfuerzo por agrupar las anteriores

Fue hasta 1994, con la formación de la Red Tecnológica Nacional (RTN), integrada por MEXNET y CONACyT que el enlace creció a 2Mbps (E1). Y es en este año que el Internet se abre a nivel comercial en nuestro país PÍXELNET, ya que hasta entonces, solamente instituciones educativas y de investigación lograron realizar su enlace a Internet.

Durante 1994 y 1995, se consolidaron redes como RTN creando un Backbone nacional y agrupando a un gran numero de instituciones educativas y comerciales en toda la República, desde Baja California hasta Quintana Roo. Se mantuvieron esfuerzos de la Red UNAM y surgieron los ISP's comerciales con más fuerza, los cuales no sólo brindaban conexión a Internet sino servicios de valor agregado, tales como acceso a Bases de Datos públicas y privadas.

CONSOLIDACIÓN DE LOS SERVICIOS DE INTERNET EN MÉXICO

En Diciembre de 1995 se hace el anuncio oficial del Centro de Información de Redes de México (NIC-México) el cual se encarga de la coordinación y administración de los recursos de Internet asignados a México, tales como la administración y delegación de los nombres de dominio ubicados bajo .MX.

En 1996, ciudades como Monterrey, N.L., registran cerca de 17 enlaces E1 contratados con TELMEX para uso privado. Se consolidan los principales ISP's en el país, de los casi 100 ubicados a los largo y ancho del territorio nacional.

En los primeros meses, tan sólo el 2% de los hosts totales (16,000) ubicados bajo .mx tienen en su nombre las letras **W.W.W.**

Nace la Sociedad Internet Capítulo México, una asociación internacional no gubernamental no lucrativa para la coordinación global y cooperación en Internet. Se crea el Computer Emergency Response Team de México

A finales del 96 la apertura en materia de empresas de telecomunicaciones y concesiones de telefonía de larga distancia provoca un auge momentáneo en las conexiones a Internet. Empresas como AVANTEL y Alestra-AT&T ahora compiten con TELMEX.

En 1999 existían más de 250 Proveedores de Acceso a Internet (ISP's) que brindaban sus servicios en el territorio mexicano, ubicados en los principales centros urbanos: Cd. de México, Guadalajara, Monterrey, Chihuahua, Tijuana, Puebla, Mérida, Nuevo Laredo, Saltillo, Oaxaca, por mencionar sólo algunos, algunos de estos inclusive en forma gratuita.

Cabe mencionar que el auge y crecimiento de estos proveedores se estanco a partir de mediados del año pasado debido a la crisis que las empresas punto com han venido sufriendo.

1.3.- ELEMENTOS QUE INTEGRAN EL DERECHO INFORMÁTICO.

La Informática Jurídica o Derecho Informático y sus impulsores han realizado enormes esfuerzos para consolidar esta disciplina como una rama autónoma del Derecho, la cual constituye sin lugar a dudas una de las mas recientes áreas del derecho la cual busca encontrar la convergencia entre el derecho y las nuevas tecnologías; en ese sentido, la Informática Jurídica y el Derecho Informático hasta cierto punto constituyen las áreas de avanzada del Derecho.

A pesar de lo anterior el impacto del esta rama del derecho en las nuevas tecnologías no ha sido tan innovador como pudiera suponerse, ya que la misma se ha visto irremediablemente frenada en su desarrollo al intentar encuadrar su desarrollo en los esquemas tradicionales del derecho, los cuales amen de resultar insuficientes, dados los nuevos tipos y supuestos que la tecnología trae consigo, muchas veces le resultan por demás incongruente, generándose en consecuencia grandes preocupaciones a los especialistas de cada una de las áreas que se encentran comprendidas dentro de la informática,

Después de lo anterior y a estas alturas del estudio podremos establecer una pequeña diferencia entre Derecho Informático e Informática Jurídica, el derecho informático como tal es conjunto de normas enfocado a la regulación y análisis de la Informática, manteniéndose ajeno al desarrollo de la tecnología, pues regula el fenómeno informático, como a lo largo de la historia ha

regulado todas las relaciones de la humanidad (patrimonio, derechos civiles, administrativos, penales, etc.)

Mientras que la Informática Jurídica, se encarga de establecer las posibilidades de uso de la tecnología informática en auxilio del derecho facilitando la manipulación de los inmensos volúmenes de leyes, casos, normas y procesos que de manera natural rebasan las posibilidades naturales de utilización de las mismas, permitiendo mediante el uso de las computadoras el ejercicio mas eficiente de la profesión legal.

Es por esto que en líneas anteriores se señalaba que existe una muy pequeña diferencia entre las dos ascpeciones (derecho informático e informática jurídica) ya que la división citada es equívoca, cosmética, poco útil e ineficiente y lejos de funcionalizar el cambio tecnológico hacía lo medular del fenómeno jurídico, refuerza viejas formas de concebir y operar el derecho

Por lo anterior y a consideración del suscrito el derecho informático esta integrado por los siguientes elementos los cuales en su mayor parte tienen similitud con los elementos tradicionales del derecho en general, pero la modernidad de la disciplina a estudio les da sus propias y especiales características.

1.- El derecho informático es un fenómeno esencialmente humano, el termino esencialmente humano que difiere de la concepción tradicional que establecía "exclusivamente humano", obedece esencialmente a que el desarrollo de la tecnología ha producido inteligencia artificial, la cual en algunos años estará tomando decisiones importantes que podrían afectar a la humanidad de muchísimas formas, es por eso que no se puede limitar la existencia de este elemento como único y exclusivo del hombre.

2.- El derecho informático es un ordenamiento derivado de la razón aplicada a la tecnología, el derecho tradicionalmente reguló y estableció las conductas que a la luz de razonamientos jurídicos requerían de ordenamientos, sin embargo la tecnología que en un principio ayudo al desarrollo y aplicación del derecho, genero nuevas conductas que escaparon a razonamientos tradicionales y han hecho necesario su estudio tendiente a establecer su normatividad.

3.- El derecho informático presupone la libertad del desarrollo y uso de nuevas tecnologías, ya que el establecer bases y lineamientos e incluso sanciones para el desarrollo y uso de la tecnología, establece la libertad de investigación y uso con las limitantes que al derecho de terceros establecido por la materia presupone.

4.- El derecho informático regula la convivencia social de una nueva comunidad global, el desarrollo de la tecnología ha dejado atrás fronteras e inclusive idiomas, ya que en este ámbito los lenguajes de programación, no tienen nacionalidad preestablecida y la habilidad del usuario le permite acceder a

cualquier parte del mundo, de ahí que la convivencia en una comunidad global tiene que estar necesariamente regulada por el derecho informático.

5.- El derecho informático tiene como fin inmediato la regulación de las actividades de los usuarios de las nuevas tecnologías, ya que al ser tantas y tan variadas las actividades que se realizan por medio de la informática es completamente necesario establecer normas mínimas de conducta y uso de la tecnología.

6.- El derecho informático debe ser promulgado por organismos colegiados que integren juristas y especialistas en informática, tratando de vislumbrar avances tecnológicos y su regulación.

7.- El derecho informático es la única rama del derecho que no se ve limitada únicamente por la realidad, ya que lo vertiginoso del desarrollo de este campo obliga a estar un paso adelante de lo existente, tratando de regular inclusive lo proyectado.

Por ultimo y para cerrar este subíndice podemos establecer como elementos del derecho Informático las áreas que el mismo regula, tomando siempre en cuenta que el avance de la tecnología supone la regulación de nuevas áreas que al momento de la elaboración de este trabajo no son del dominio público, así tenemos que el derecho informático regula las siguientes actividades:

COMERCIO ELECTRÓNICO: (E-comerce): Los diversos estudios realizados en torno al tema definen al comercio electrónico como "cualquier forma de transacción comercial en la que las partes interactúan electrónicamente en lugar de por intercambio o contacto físico directo". Dicha definición tan solo resalta una de las características de esta modalidad de comercio ; las relaciones entre las partes se desarrollan en vía electrónica.

Sin embargo, los alcances del comercio electrónico no puede quedar restringidos a las relaciones de compra venta entre las partes a través de medios electrónicos pues tal figura podría confundirse con lo que la doctrina del derecho informático ha definido como "contratación electrónica". El comercio electrónico abarca un amplio espectro tal como lo define el jurista argentino Antonio Millé quien afirma que " Bajo la denominación de comercio electrónico se distingue el basto conjunto de actividades con finalidad mercantil que se desarrolla mediante el uso de sistemas de procesamiento de datos y de comunicación sin que exista un contacto físico directo entre quien oferta un bien o un servicio y quien lo demanda (...) la denominación no cubre solamente actos comerciales directos, como la compra venta o el alquiler, sino también acciones preparatorias o conexas como las de publicidad o mercadeo".

Es decir, el comercio electrónico comprende no solo las ventas o adquisiciones que el empresario y el usuario realizaran a través de Internet, sino que engloba todas las bases del negocio empresarial.

DELITOS INFORMÁTICOS: 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

FIRMA ELECTRÓNICA: En materia de comercio electrónico la tradicional firma manuscrita u ológrafa, que implica la función de autoría de una declaración de voluntad por parte del sujeto que suscribe un documento se reemplazara por una firma digital llave magnética mucho mas segura o de mayor viabilidad técnica que permite comprobar adecuadamente la identidad del auto o emisor de un documento o mensaje, así como también el contenido concreto del mismo y los termino reales en que fue aceptado por el receptor ambos signos, de la firma manuscrita y/o digital identifican a las personas que las emiten y les atribuye a sus titulares el contenido de documentos determinados.

PUBLICIDAD EN INTERNET: Regulación de las campañas cantidades y mensajes de anuncios publicitarios lanzados a la red mediante banners o correos electrónicos directos.

PROTECCIÓN Y ACCESO A LA INFORMACIÓN: El derecho a la información es un concepto doctrinal que supone el estudio y sistematización de las disposiciones jurídicas positivas en materia de información por definición incluye, pero no se agota el estudio de las libertades de información.

El derecho a la información incluye las siguientes materias; libertades fundaméntelas de la información, régimen informático del estado, régimen de las empresas y actividades relacionadas con la información el estatuto de los profesionales de la información, régimen de responsabilidad civil y penal y los derecho de autor.

PROTECCION AL CONSUMIDOR EN INTERNET: rama del derecho informático que se encarga de promover y proteger los derechos de los consumidores en las operaciones efectuadas a través de los medios electrónicos, ópticos o de cualquier otra tecnología pues prevé las obligaciones de los proveedores en este tipo de transacciones pues con ello se garantiza de manera integral los derechos de los consumidores, evitando en todo caso el manejo fraudulento de la información proporcionada y la correcta utilización de los datos aportados.

DERECHOS DE AUTOR RESPECTO A SOFTWARE PROTEGIDO: La Organización Mundial de Propiedad Intelectual, en diciembre de 1996 después de constatar lo precario de la protección jurídica del estatuto jurídico tradicional que la propiedad intelectual otorga a las obras que se comercializan y consultan en Internet, estableció la obligación que lo estados que ratifiquen y firmen la convención de Ginebra sobre derechos de autor deben resguardar

jurídicamente y promocionar la aplicación de medidas de seguridad de la propiedad intelectual (derecho de autor)

REGISTRO Y PROPIEDAD DE DOMINIOS: Rama del derecho informático encargada de establecer la propiedad que respecto a los dominios en Internet tienen los particulares, aspecto de enorme importancia mundial, dado lo elevado de los precios que un dominio extremadamente comercial puede tener en para un comerciante o inversionista en línea.

1.4.- SEGURIDAD JURÍDICA QUE PROPORCIONA EL DERECHO INFORMÁTICO EN EL AMBITO ECONÓMICO DE NUESTRO PAÍS.

El desarrollo de la informática en nuestro país aunque limitado, existe, si bien no gracias al apoyo y desarrollo procurado por nuestro gobernantes, este desarrollo es consecuencia del establecimiento en nuestro país de muchísimas filiales de empresas importantes a nivel mundial que han importado su tecnología para el desarrollo de sus actividades, amen de que la tendencia a la globalización hace que el desarrollo y uso de la tecnología este a la mano de la mayoría de las naciones.

Aunque cabe aclarar que la importancia de la Información es tal que en 1977 se reforma nuestra constitución y se reconoce el Derecho a la Información, adicionando los artículos 6º y 41[3], de para establecer este concepto o garantía individual, política y social.

Ahora bien la informática es parte medular en la mayoría de las actividades comerciales, ya que inventarios, bases y transferencias de datos, firmas de contratos, compra ventas, intercambios, subastas, licitaciones, conferencias, educación a distancia, y muchas actividades mas se realizan mediante la informática, se calcula que únicamente en México se realizan transacciones en línea superiores a los 5 millones de dólares mensuales, cantidad que se multiplica varias veces en mercados con mayor desarrollo tecnológico, en los cuales hay mas facilidad para sus ciudadanos de acceder a estos medios, pero si el valor de las transacciones es alto, el valor de las bases de datos, de los programas de investigación, de las paginas comerciales en la red, de las cuentas bancarias que son manejadas en línea, etcétera, es incalculable.

Por lo tanto el derecho informático tiene la función de proporcionar seguridad al usuario, al desarrollador de programas, al inversionista, la seguridad de que cualquier conducta que pudiera afectar sus intereses será prevista y en su caso castigada, que las controversias que pudiesen surgir por el uso de la informática, serán resueltas por tribunales que se especialicen en la

---

[3] Constitución Política de los Estados Unidos Mexicanos. Editorial Alco Edición 2000 México.2000.

materia o que por lo menos tengan conocimiento de la misma, y en general de proporcionar a la comunidad participante y usuaria de esta tecnología, la certeza de estar en un ambiente regulado alejado de la anarquía reinante en un sistema sin normatividad.

El sistema bancario de cualquier país es fundamental para el desarrollo del mismo y este ha sido uno de los que mayormente se ha enfocado a actualizarse y utilizar los beneficios que la informática le puede proporcionar, así tenemos que las transferencias en línea son cada vez mayores en nuestro país, que las nominas de numerosas industrias e incluso de dependencia gubernamentales son actualmente pagadas y depositadas por medios informáticos, que las firmas de alianzas estratégicas, así como la firma de contratos se verifican en línea, por lo tanto todas estas actividades necesariamente tienen que regularse por el derecho informático el cual si bien norma las conductas, y dirime controversias, tiene como una de sus finalidades principales la prevención de conductas delictivas.

1.5.- FUENTES REALES QUE GENERAN EL DERECHO INFORMÁTICO.

Las fuentes reales son los modos o formas en las que nace el derecho, los procesos de manifestación de las normas jurídicas, en palabras del ***jurista Bonnecase*** "órganos de expresión del derecho".[4]

Estas fuentes se reducen a dos una que se conoce por medio de la razón llamada tradicionalmente "ideales de la justicia" y la otra vinculada a la experiencia llamada "circunstancias históricas".

Los ideales de Justicia, son el fruto de las aspiraciones sociales mas elevadas del espíritu humano, mientras que las "circunstancias históricas" son el conjunto de particularidades a que se halla sometido el hombre por su condición de ser corpóreo, situado en un tiempo y en un espacio determinados,.

Francisco Suárez (1548-1617)[5] apunto que si el hombre fuera puro no tendría necesidad del derecho. Si transpolamos esta idea al derecho informático, tendremos que: si las conductas derivadas del uso de la informática fueran ideales no existiría el derecho informático.

En efecto, es la condición temporal y corpórea del hombre la que lo sitúa en medio del torbellino de los problemas jurídicos, por su cuerpo, el hombre se halla a merced del vaivén de las circunstancias históricas, es decir, de las fuerzas sociológicas y económicas, de los hechos y situaciones de la historia,

[4] VILLORO Toranzo Miguel. Introducción al estudio del derecho México. Ed. Porrua 1988. Pág. 157

[5] VILLORO Toranzo Miguel. Ob.cit. Pág. 157

de las pasiones e influencias humanas. En este orden de ideas tenemos como la fuente real mas directa del derecho informático el siguiente axioma, LAS REALIDADES CONDICIONAN AL DERECHO, así tenemos que la revelación de una nueva realidad, la existencia de conductas y hechos que no se encontraban en las reguladas hasta hace dos décadas, motiva la creación de leyes especiales para ellas y por sobre todo a crear y enfocar una disciplina del derecho que se enfoque básicamente a su estudio.

Sin embargo las condiciones históricas requieren forzosamente de los esfuerzos de la autoridad creadora del derecho enfocándose la misma a llevar las normas creadas al estado mas cercano a lo ideal, siempre cuidando de no caer en la utopía de lo irrealizable, ni en la autocomplacencia derivada de las presiones de la sociedad.

Si bien las dos fuentes reales ofrecen el contenido de las normas jurídicas, estas no se formulan en forma automática, Se requiere, la acción causal de la autoridad, correspondiéndole a esta una elección que busque el punto de equilibrio entre los ideales de Justicia y las posibilidades de regulación de las circunstancias históricas, la elección del contenido de las normas es el momento decisivo del proceso creador del derecho.

CAPITULO II
MARCO JURÍDICO DOCTRINAL DE LOS DELITOS INFORMÁTICOS

2.1.- NATURALEZA DE LOS DELITOS INFORMÁTICOS

A fin de poder establecer la naturaleza de los delitos informáticos será necesario proceder a clasificarlos y podemos comenzar con la clasificación que hace el jurista Mexicano Julio Téllez Valdés quien clasifica a los delitos informáticos en base a dos criterios:

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

2. como fin u objetivo: se enmarcan a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. [6]

María de la Luz Lima: clasifica los delitos electrónicos en tres categorías, de acuerdo a como utilizan la tecnología electrónica:

1. Como método: cuando los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

2. Como medio: en donde para realizar un delito utilizan una computadora como medio o símbolo.

3. Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla. [7]

Jorge Pacheco Klein distingue 5 clasificaciones:

1. Delitos informáticos internos. Ej. : sabotaje de programas.

2. Delitos a través de las telecomunicaciones. Ej. : hacking.

---

[6] TÉLLEZ VALDEZ Julio "Derecho Informático" Editorial Mc Graw Hill 2000 Pag. 105 - 106

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

3. Manipulación de computadoras. Ej. : apropiación indebida, peculado y fraudes informáticos. Es la más vinculada a delitos de cuello blanco.

4. Utilización de computadoras en apoyo a empresas criminales, como el lavado de dinero y la distribución ilícita de drogas.

5. Robos de software (piratería).

En la siguiente clasificación, la cual proponemos después de analizar lo anterior los delitos informáticos se basan en dos criterios: como instrumento o medio, o como fin u objetivo.

a.- Como instrumento o medio

Se tienen a las conductas criminales que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito. Ejemplo: Los falsificadores de tarjetas de crédito, billetes y/o documentación oficial, la cual en nuestro país bien pareciera una profesión bien remunerada, habría que agregar a los equipos que emiten hologramas oficiales de verificación y de tenencias.

b.-Como fin u objetivo

En esta categoría se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Para ejemplificar este criterio fácilmente podemos mencionar tanto a los Crackers como a los Hackers quienes han revolucionado a los programas de seguridad y se han convertido en un filtro más en la efectividad del desarrollo de software especializado.

Sin embargo al ser tan complejas las conductas relacionadas a la informática que pudieran ser consideradas como delictivas, podemos hacer una clasificación mas detallada tomando en cuenta para ello los siguientes puntos: 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 la clase de actividad que implique según los datos involucrados, lo anterior nos lleva a enumerar los delitos informáticos por la naturaleza de su clasificación.

Son conductas criminales de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando y se derivan de los conocimientos que el sujeto activo obtiene en el desarrollo de su profesión.

Son acciones de oportunidad, en cuanto se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

Provocan serias pérdidas económicas, ya que casi siempre producen altos beneficios a aquellos que los realizan.

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

Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

Son muy sofisticados y relativamente frecuentes en el ámbito militar.

Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico y por el desconocimiento del mismo por parte de las autoridades encargadas de la persecución de los mismos.

Una gran parte de ellos son imprudenciales cometidos por personas que desconocen el tipo penal aplicable y no necesariamente se cometen con intención.

Ofrecen facilidades para su comisión a los menores de edad.

Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Haciendo un análisis concreto de las características enunciadas, es importante señalar la urgencia de legislar al respecto de estos delitos teniendo especial cuidado en la prevención de los mismo, vía la difusión masiva de las conductas reglamentadas, a fin de que las personas que cometen estos ilícitos por desconocimiento, conozcan los delitos en que pueden incurrir con sus actuaciones, este trabajo como ya se menciono en el primer capítulo de este ensayo deberá ser realizado por personas que tengan el conocimiento, tanto técnico en materia de computación, como en lo legal, ya que únicamente al integrar las dos disciplinas se podrán aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular.

2.2. ESTUDIO DOGMATICO A LA LUZ DE LOS ELEMENTOS DEL DELITO

Se pueden señalar tres sistemas en la evolución de la concepción analítica que distingue en el delito los elementos acción, tipicidad, antijuridicidad y culpabilidad.

I.- El primer sistema llamado del causalismo natural o sistema clásico esta representado por los sistemas de Franz Von Liszt, Ernest Beling y Gustav Raduch, este sistema imperó durante los primeros años del siglo xx su estilo de pensamiento corresponde al positivismo científico imperante en la segunda mitad del siglo xix y respecto a los elementos del delito consideran:

A: La acción es concebida de un modo puramente naturalista, como innervación muscular, es decir como voluntario movimiento corporal y cambio en el mundo exterior (resultado) unidos por una relación de causalidad. este es el llamado concepto natural de acción.

B: El tipo se concibe como pura descripción del aspecto objetivo del hecho, sin contener predicados de valor (que pertenecen a la antijuridicidad) ni elementos subjetivos (que corresponden a la culpabilidad)

C: La antijuridicidad es un juicio valorativo que recae únicamente sobre el aspecto objetivo del hecho típico, ya que todo lo subjetivo pertenece a la culpabilidad, es decir se valora el hecho típico objetivo en relación con el derecho y si hay contrariedad la conducta es antijurídica (concepción formal de la antijuridicidad)

D: La culpabilidad es concebida como un proceso psicológico que tiene lugar en el interior del mundo anímico del autor por ello concibe a la culpabilidad como el nexo psicológico que liga al autor con el hecho realizado (concepción psicológista de la culpabilidad) la cual se agota en las simples formas de dolo o culpa.

II.- El segundo sistema corresponde al llamado causalismo valorativo o sistema neo clásico y esta representado fundamentalmente por los sistemas de Mezger, Mayer y Sauer (autores alemanes) en este sistema se configura una concepción teleológica del delito en la que todas las características esenciales de la infracción punible aparecen orientadas sobre la idea de valor.

En efecto el anterior sistema de Liszt y Beering que había conseguido imponerse en los primeros años del siglo xx, es sometido a un profundo proceso de transformación cuya culminación puede cifrarse convencionalmente en el año de 1931 en que aparece la primera edición del tratado de derecho penal de Edmund Mezger. formalmente se mantiene el mismo

sistema anterior, pero se transforma sustancialmente el contenido conceptual de los elementos del delito, resultando así que ahora:

A: La acción y la omisión punibles no son puros acontecimientos naturalisticos del suceder externo, sino conceptos referidos a un valor.

En este sentido, acción y omisión son solo aquellos acontecimientos que merecen el calificativo de conducta humana y pueden ser valorados como tal por trascender socialmente (concepto social de acción)

B: El tipo deja de concebirse como una descripción del aspecto objetivo del hecho y se enriquece con elementos normativos y subjetivos, es decir se reconoce que en ciertos casos, la tipicidad de la conducta depende de determinadas valoraciones normativas o de ciertos elementos subjetivos, por ejemplo en el robo se requiere que el apoderamiento recaiga en cosa mueble ajena donde la cosa mueble es un concepto normativo de valoración jurídica y el apoderamiento implica el animo de adueñamiento por lo que este animo es un elemento subjetivo.

C: La antijuridicidad, no se agota en la pura relación de contrariedad entre el hecho y la norma (antijuridicidad formal) sino que ahora se constituye sustancialmente como lesión o puesta en peligro de bienes jurídicos intereses o valores (antijuridicidad material)

D: La culpabilidad ya no es concebida únicamente como nexo psicológico entre el hecho y su autor, sino que se concibe ahora como juicio de valor, así, culpabilidad es reprochabilidad (juicio de reproche personal) las relaciones sicológicas (dolo y culpa) que antes agotaban la culpabilidad pasan ahora a ser presupuestos del juicio de reproche, es decir la culpabilidad es la reprochabilidad de una conducta típica y antijurídica, cometida dolosa o culposamente (concepción normativa de la culpabilidad)

III.- El tercer sistema corresponde a la doctrina finalista cuyo fundador y mas autorizado representante fue Hanz Welzel comenzó a elaborarse esta doctrina en la década de los años treintas del siglo pasado en Alemania, modificando el contenido conceptual de los elementos del delito así como su ubicación sistemática dentro de la teoría del delito en comparación con los modelos usados por los sistemas del causalismo natural y del causalismo valorativo.

para esta teoría la acción humana es ejercicio de la actividad final, la acción se dirige voluntariamente a un fin, por lo que el dolo y la culpa forman parte de la acción.

En tanto que el resultado no es elemento de la acción, permanece fuera de ella.

El Tipo Penal se configura por la unión de acción y resultado y toda vez que el dolo y la culpa forman parte de la acción, resulta entonces que dolo y culpa son elementos del tipo, por lo que este ya no contiene solo elementos objetivos, sino también subjetivos (dolo y culpa) y normativos.

La Antijuridicidad se concibe formal y materialmente y al ser un juicio de valor que recae sobre la acción (y por contener esta al dolo y la culpa) el dolo pasa a ser por tanto el objeto del juicio de antijuridicidad, originándose así una concepción subjetiva de la antijuridicidad que Hanz Welzel califica como injusto personal.

La culpabilidad ya no se integra de dolo y culpa (estos elementos forman parte del tipo por lo que la culpabilidad es la reprochabilidad de una conducta típica y antijurídica que contiene como elementos:

1.- La imputabilidad
2.- El conocimiento potencial de la antijuridicidad
3.- La exigibilidad de una conducta diversa a la realizada.

Las diferencias fundamentales entre las corrientes Causalista y Finalista son:

1.- El contenido de los conceptos.
2.- Su ubicación dentro de la teoría del delito.

EVOLUCIÓN DE LA TEORÍA DEL DELITO

(Resumen)

Causalismo Natural Sist. Clásico	Causalismo Valorativo Sist. Neoclásico	Finalismo
ACCIÓN.- CONCEPTO NATURAL INNERVACIÓN MUSCULAR MOVIMIENTO CORPORAL VOLUNTARIO ESTO SE DESARROLLA DURANTE EL POSITIVISMO QUE DICE QUE EL CONOCIMIENTO VIENE DE LA EXPERIENCIA	ACCIÓN (MESGER Y MAYER) YA NO ES NATURAL SOLO VA A SER ACCIÓN LAS QUE TIENEN RELEVANCIA JCO-PENAL ACCIÓN.- ES UN COMPORTAMIENTO HUMANO VOLUNTARIO ENCAMINADO A UN PROPÓSITO.	ACCIÓN CONSIDERA QUE TODA ACCIÓN ES UNA ACCIÓN FINAL ES DECIR ENCAMINADAS A UN FIN. COMPORTAMIENTO HUMANO VOLUNT.
TIPICIDAD DESCRIPCIÓN DEL ELEMENTO OBJETIVO QUE REQUIERE EL TIPO	TIPICIDAD YA HAY ELEMENTOS SUBJS. OBJETIVO Y VALORATIVOS PERO LOS SUBJETIVOS SON DIFERENTES AL DOLO	TIPICIDAD ADQUIERE OBJETIVOS, SUBJS. Y NORMATIVOS Y ADEMÁS DENTRO DE LOS SUBJETIVOS ENCONTRAMOS EL DOLO Y LA CULPA
ANTIJURIDICIDAD (FORMAL) CONDUCTA CONTRARIA A DERECHO	ANTIJURIDICIDAD SE ACEPTA LA FORMAL Y LA MATERIAL ES ASÍ POR QUE ES CONTRARIA A DERECHO Y POR QUE LESIONA O PONE EN PELIGRO BIENES JURÍDICAMENTE	ANTIJURIDICIDAD TAMBIÉN ES FORMAL Y MATERIAL PERO TAMBIÉN TIENE UNA NATURALEZA SUBJ.

	PROTEGIDOS	POR QUE ANALIZA EL JUICIO DE VALOR DE LA CONDUCTA.
CULPABILIDAD ES UN PROCESO PSICOLÓGICO INTERNO QUE SE AGOTA CON LAS SIMPLES FORMAS DE DOLO Y CULPA	CULPABILIDAD AQUÍ SE REQUIERE PARA DECLARAR CULPABILIDAD QUE EXISTA DOLO + REPROCHABILIDAD	CULPABILIDAD ES LA SIMPLE REPROCHABILIDAD DE UNA CONDUCTA
TEORIA PSICOLOGISTA DE LA CULPABILIDAD	TEORÍA NORMATIVISTA DE LA CULPABILIDAD	

ACCIÓN

La acción es el elemento mas importante de la estructura del concepto de delito, el concepto de acción al evolucionar, ha pasado por la siguientes etapas.

I.- Teoría causal de la acción.

A.- Esta teoría fue expuesta por Franz Von Liszt y actualmente ya no es sostenida, muestra el influjo de la filosofía positivista de fines del siglo xix, este concepto de acción se llama "natural" por que trata de incorporar las leyes causales de las ciencias naturales en el derecho penal.

Para esta corriente la acción es un puro factor de causalidad, acción es la producción de un resultado mediante fuerzas físicas, así según Liszt la acción es una "modificación" en el mundo exterior físico, perceptible material, es decir sensorialmente debido a la tensión corporal en el delito comisivo y al descanso físico en el delito omisivo.

Para el concepto naturalista de acción, esta es una "innervación muscular" es decir, un movimiento voluntario, pero en el que carece de importancia o se prescinde del fin a que esta voluntad se dirige, por lo que bajo esta concepción habría acción comisiva si un sujeto disparaba sobre otro con voluntad de presionar el gatillo sin que fuese necesario tomar en cuenta la finalidad que se proponía para hacerlo, por que esta finalidad no pertenecía a la conducta.

El concepto naturalista de acción también fue sostenido por Ernest Beling, quien caracterizo a la conducta como un comportamiento corporal voluntario.

Como ya se dijo esta teoría trata a la acción como puro factor causal del resultado, sin tomar en cuenta la intención que llevo al sujeto a realizarla, por ello se le define como "un comportamiento humano voluntario que produce una determinada consecuencia en el mundo exterior", es decir, de la acción solo importa si el comportamiento voluntario causo el resultado pero no interesa si la voluntad iba dirigida a ello, ya que esto ultimo es materia de análisis hasta el nivel de la culpabilidad.

Eugenio Raúl Zaffaroni, en su manual de derecho penal establece respecto al concepto natural de acción lo siguiente:

"No obstante, lo cierto es que una conducta sin finalidad carece de voluntad y en realidad quedaba reducida a un simple proceso causal..... la conducta como concepto final no era la conducta humana en su realidad, sino algo diferente, un concepto propio que en sustancia coincidía con el que hasta entonces se había venido fundamentando por el positivismo mecanicista: una conducta era un "hacer voluntario" pero en esta voluntad no había contenido".

En defensa del concepto causal de acción Edmundo Messger señala que la conducta siempre tiene una finalidad solo que la finalidad no se toma en consideración sino hasta llegar al nivel de la culpabilidad y que nada cambia que se le tome en consideración ahí, pues de cualquier forma no se le desconoce dentro de la estructura general de la teoría del delito, argumentando que Zaffaroni considera falso debido a que "si la conducta siempre tiene una finalidad no se esta tomando en consideración a la conducta sino un proceso causal, por ende, dentro de este sistema el núcleo del injusto no será una conducta, sino un proceso causal. esta afirmación es sumamente grave por que contradice la esencia del derecho: lo típico y antijurídico no serán conductas sino procesos causales el derecho no será (para esta concepción) un orden regulador de conductas sino de procesos causales, lo que es absurdo: el derecho no regula "hechos" sino hechos humanos voluntarios, es decir conductas".

CONCEPTO SOCIAL DE ACCIÓN

Una de las criticas mas severas al concepto natural de acción es que trató de incorporar las leyes de la naturaleza al derecho penal, no obstante que la acción es un concepto situado dentro del campo del derecho, incluso un concepto situado dentro del derecho penal (argumento de los seguidores del concepto social de acción)

La teoría social de la acción considera que solo son acciones aquellas que tienen sentido social, es decir, las que trascienden a terceros, formando parte del interaccionar humano, por lo que las que no tienen trascendencia social, esto es que permanecen en el ámbito informal no interesan al derecho penal.

Dentro de este planteamiento también se llega a sostener que solo pueden ser acciones con relevancia penal las que perturban el orden social, por lo que conforme a esta corriente, la acción es la acusación de un resultado relevante socialmente; desde el punto de vista jurídico penal, es la acusación de un resultado típico.

Para esta teoría, la acción, como causacion de un resultado por un factor de causalidad tampoco toma en cuenta el fin que persigue el sujeto activo con su comportamiento voluntario, es decir, la voluntad es dividida en voluntad de movimiento corporal o de la inactividad y voluntad de resultado. la primera es decir la voluntad del movimiento corporal o de la inactividad es la única que forma parte del concepto social de acción. La segunda es decir, la voluntad del resultado, esto es el fin que se persigue con la acción no forma parte de esta sino de la culpabilidad.

Específicamente del dolo, el cual para esta corriente forma parte de la culpabilidad.

Para Zafaronni el que la conducta tenga trascendencia social por perturbar el orden social no es un problema de conducta sino de tipicidad, debido a que no cualquier conducta sino solo la que es típica, lesiona o pone en peligro bienes jurídicamente protegidos.

2.- La corriente finalista de la acción considera que es insostenible el concepto causal de acción, debido a que no es posible que la voluntad de la acción se pueda dividir en una voluntad de solo movimiento corporal y otra voluntad de resultado o fin perseguido, puesto que entonces ello equivale a considerar que la acción es una acción "ciega", es decir sin dirección, sin un fin especifico, cuando en realidad las cosas son finales, puesto que la acción humana siempre es "vidente" esto es, que la acción siempre se dirige a un fin por ello, Hans Welzel considera que "la acción humana es dirección final del suceso causal; la acción es actividad final humana".

Esto significa que en las acciones humanas el hombre antes que realizar una acción, anticipa mentalmente el resultado o fin que se propone y selecciona los métodos que considera adecuados para lograrlo, posteriormente realiza la acción la cual puede o no alcanzar el fin o resultado propuesto es decir, es contingente en ese sentido, al suceso causal (acción, resultado y nexo de causalidad) se le imprime una dirección final, ello es, se dirige a un fin concreto.

Por ello esta finalidad pertenece a la acción y así, la acción es actividad final humana, la corriente finalista considera que si la acción es un comportamiento humano voluntario esta voluntad no se divide como lo estima la teoría causalista, sino que dicha voluntad contiene siempre el fin que se persigue, por lo que si la voluntad tiene como contenido a la finalidad, el dolo o en su caso la culpa siempre serán elementos de la acción y toda vez que la acción es el principal elemento del tipo, resulta entonces que dolo y culpa son elementos del tipo penal.

Una de las criticas mas importantes que se la he formulado a la teoría finalista es que en los delitos culposos la acción no se dirige al fin de la producción de un resultado típico y sin embargo este se produce por lo que entonces ahí no habría acción, lo cual seria un absurdo, frente a esta critica la

corriente finalista explica que si funciona correctamente, el concepto final de acción aún en los delitos culposos, puesto que el sujeto activo realiza una acción cuando mentalmente anticipa el resultado que se propone, por ejemplo, llegar pronto a su fuente de trabajo y para ello, selecciona los medios adecuados para lograrlo, como por ejemplo manejar su vehículo a gran velocidad, pero por un descuido de su parte en el trafico, al seleccionar incorrectamente los medios (conducir su vehículo a gran velocidad), produce el resultado típico que no buscaba, como por ejemplo lesionar a un peatón, en este caso sigue funcionando el concepto final de acción puesto que la actividad humana se encamino a un fin que originalmente era licito y este resultado puede o no alcanzarse y en el ejemplo se advierte que no se consiguió por una inadecuada selección de los medios incumpliendo con ello, un deber de cuidado.

Todo dolo del tipo es una voluntad finalista, pero no toda finalidad es un dolo del tipo.

2.3. CLASIFICACION DEL TIPO MAS COMUN DEL DELITO INFORMÁTICO

Delito Informático

Artículos: 217 Código Penal y de Procedimientos Penales del Estado de Sinaloa, Artículos 211 Bis 1 al Bis 7 Código Penal Federal.

Elemento de Conducta: De Acción.

Bien Jurídico Tutelado: El Patrimonio

Objeto Material del Delito: El Patrimonio

Resultado: Formal y Material

Daño: De Peligro

Núcleo Esencial del Tipo: Usar

Duración: Instantáneo

Forma de Persecución: De Oficio

Elemento Interno: Doloso

Elemento Objetivo: Entrar, Usar

Elemento Subjetivo: Con el fin o Con el Propósito

Elemento Normativo: Lucro, Bienes

Número de Sujetos: Unisubjetivo

Número de Actos: Unisubsistente

Estructura Metodológica: Simple

Ordenación Metódica: Tipo Básica Fundamental

Formulación: Causista Alternativo

2.4.- CONCEPTO DE DELITO INFORMÁTICO

El definir el delito informático resulta relativamente difícil ya que los conceptos básicos así como las definiciones varían de una manera importante de un país a otro, derivado esto desde el idioma utilizado, las frases o expresiones que cambian y se utilizan de un país a otro inclusive en aquellos que hablan la misma lengua, hasta por el desarrollo tecnológico alcanzado por cada país. Esto es notorio al analizar que el delito informático tiene diversas acepciones a lo largo del mundo y solo citando alguna enumeraremos las siguientes:

1.- delitos informáticos, 2.- delitos electrónicos, 3.- delitos relacionados con las computadoras, 4.- crímenes por computadora, 5.- delincuencia relacionada con el ordenador.

No obstante habremos de citar las definiciones y conceptos utilizados por los mas renombrados estudiosos del tema, entre los que orgullosamente se cuenta al jurista mexicano Julio Téllez Valdés de quien y a manera de homenaje transcribiremos su definición en primer termino.

El concepto típico: "los Delitos Informáticos son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin."

El concepto atípico, "los Delitos Informáticos son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin."

Nidia Callegari[8] define al "delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas."

Rafael Fernández Calvo[9] define al "delito Informático" como la realización de una acción que, reuniendo las características que delimitan el

[8] 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. P.115

[9] FERNÁNDEZ Calvo, Rafael. "El tratamiento de llamado "delito informático" en el proyecto de ley Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática" en Informática y Derecho. Pp.1150. Pendiente

concepto de delito, se ha llevado a cabo utilizando en elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española."

María de la Luz Lima[10] 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."

El departamento de investigación de la Universidad de México, señala como delitos informáticos que son "todos aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático.

El italiano Carlos Sarzana,[11] define el Delito Informático como: "cualquier comportamiento criminógeno en que la computadora esta involucrada como material, objeto o mero símbolo."

Jimena Leiva lo define como: "toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma"

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

La delincuencia Informática es definida por el jurista GÓMEZ PERALS[12] como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica

---

[10] María. Ob. Cit.

[11] SARZANA, Carlo. "Criminalità e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2. Ano 1. 1979. Roma,Italia. P.53

[12] GÓMEZ PERALS, Miguel. "Los Delitos Informáticos en el Derecho Español", Informática y Derecho nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi, págs. 481 a 496.

informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

Baón Ramírez[13] define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).

Tiedemann considera que con la expresión "criminalidad mediante computadoras", se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos.

Romeo casabona[14] se refiere a la definición propuesta por el Departamento de Justicia Norteamericana, según la cual Delito Informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución.

Davara Rodríguez[15] al estudiar el tema manifiesta lo siguiente: "No parece adecuado hablar de delito informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito. Ni el Código Penal de 1995 introduce el delito informático, ni admite que exista como tal un delito informático, si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático." Y el jurista citado define el Delito informático como, "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software."

---

[13] BAÓN RAMÍREZ, Rogelio. "Visión general de la informática en el nuevo Código Penal", en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, págs. 77 a 100.

[14] ROMEO CASABONA, Carlos María. "Los llamados delitos informáticos", Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995

[15] DAVARA Rodriguez Miguel Ángel, MANUAL DE DERECHO INFORMÁTICO, Ed. Aranzadi, Pamplona, España, 1997.

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

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

RUIZ VADILLO[16] recoge la definición que adopta el mercado de la OCDE en la Recomendación número R(81) 12 del Consejo de Europa indicando que abuso informático es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos.

Nos parece adecuado mencionar en este subcapítulo el tratamiento que se ha dado al tema en el derecho anglosajón en el que se ha popularizado la denominación de "Computer Crime" mientras que en el derecho germano la expresión "Computerkriminalität" es la que esta mas en boga.

Con lo anterior consideramos que ha quedado establecido el concepto de Delito Informático por lo que pasaremos al siguiente subcapítulo en el que se enlistaran los tipos de delito informático conocidos en la actualidad definiendo cada uno de los mismos.

2.5- TIPOS DE DELITOS INFORMÁTICOS.

Los delitos Informático al estar definidos y clasificados en todos los países del mundo de formas relativamente diferente y al no existir una legislación universal que defina los mismos será necesario iniciar este subcapítulo con la definición que la Organización de las Naciones Unidas aporta, para después enumerar los delitos que pudieran escapar de esta y algunas otras definiciones que utilizan diferentes países y juristas, por lo tanto no se pretende hacer una clasificación con un criterio metodológico propio, sino simplemente apegarnos a los criterios establecidos, enunciando de manera importante los que

[16] RUIZ VADILLO, Enrique. "Responsabilidad penal en materia de informática", Informática y Derecho nº 9,10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996, págs. 443 a 460.

nos parecen mas atinados, pretendiendo con esto dejar establecidas las diferentes modalidades delictivas[17].

1.- Fraudes cometidos mediante manipulación de computadoras.- Estos pueden suceder al interior de Instituciones Bancarias o cualquier empresa en su nómina, ya que la gente de sistemas puede acceder a estos tipo de registros y programas.

2.- La manipulación de programas.- Mediante el uso de programas auxiliares que permitan estar manejando los distintos programas que se tiene en los departamentos de cualquier organización.

3.- Manipulación de los datos de salida.- Cuando se alteran los datos que salieron como resultado de la ejecución de una operación establecida en un equipo de computo.

4.- Fraude efectuado por manipulación informática.- Accesando a los programas establecidos en un sistema de información, y manipulándolos para obtener una ganancia monetaria.

5.-Falsificaciones Informáticas.- Manipulando información arrojada por una operación de consulta en una base de datos.

6.- Sabotaje informático.- Cuando se establece una operación tanto de programas de computo, como un suministro de electricidad o cortar líneas telefónicas intencionalmente.

7.- Virus.- Programas contenidos en programas que afectan directamente a la maquina que se infecta y causa daños muy graves.

8.- Gusanos.- 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 porque no puede regenerarse.

9.- Bomba lógica o cronológica.- Su funcionamiento es muy simple, es una especie de virus que se programa para que explote en un día determinado causando daños a el equipo de computo afectado.

---

[17] 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 York.1994

10.- Piratas Informáticos.- Hackers y Crackers dispuestos a conseguir todo lo que se les ofrezca en la red, tienen gran conocimiento de las técnicas de computo y pueden causar graves daños a las empresas.

11.- Acceso no autorizado a Sistemas o Servicios.- Penetrar indiscriminadamente en todo lugar sin tener acceso a ese sitio.

12.- Reproducción no autorizada de programas informáticos de protección Legal.- Es la copia indiscriminada de programas con licencias de uso para copias de una sola persona, se le conoce también como piratería.

Esta clasificación de la ONU, pretende englobar las conductas criminales en la informática de una manera amplia e incluyente, sin embargo el suscrito considero que aun se pueden aumentar algunas conductas y sobre todo hacer mas particularizadas las definiciones a efecto de lo cual propongo se aumente lo siguiente.

Como complemento al numeral 2.- es muy difícil de descubrir y a menudo pasa inadvertido debido a que el sujeto activo en este caso debe tener conocimientos técnicos concretos de informática.

Mediante los cuales modifica los programas existentes en el sistema de computadoras o inserta 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.

Como complemento al numeral 3.- Manipulación de los datos de salida – (outsider termino anglosajón que refiere a gente de afuera o ajena)

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

Manipulación de los datos de entrada (insiders termino anglosajón que refiere a infiltrador)

Estamos ante un fraude informático, conocido también como sustracción de datos y estamos ante 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.

Respecto al numeral 4.- Fraude efectuado por manipulación informática. (Técnica del Salami)

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

Respecto al numeral 5 .- Falsificaciones informáticas

Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.

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.

Respecto al numeral 6.- Sabotaje informático.

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema

Respecto al numeral 7.- Virus.

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, (oculto en un programa mayor)

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

ping-pong: consiste en un punto que se mueve por toda la pantalla y parece rebotar en los bordes.

Datacrime o virus del viernes 13

Jerusalem estaba destinado para destruir todas las memorias militares y científicas de Israel el 13 de mayo de 1988.

Michelangelo

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

Respecto a este particular es necesario abundar un poco en el estableciendo su ciclo de vida:

Los virus informáticos, de igual modo que los biológicos, tienen un ciclo de vida. En primer lugar hay una creación que se produce cuando una persona con conocimientos de programación, trabaja en su gestación por varias semanas y termina creando un nuevo virus que se encuentra programado para reproducirse rápidamente y hacer daño en algún momento determinado especificado por el programador.

La gestación es con el propósito de futuras reproducciones. Usualmente esto se hace infectando un programa y luego distribuyéndolo por la Red. Al hilo de esto está la reproducción, es decir, su replicación por un largo tiempo antes de que sea activado.

Los virus poseen rutinas de destrucción de datos que se activarán cuando ciertas condiciones sean dadas. Algunos virus se activan en una fecha determinada.

La fase de descubrimiento no se tiene porque producir después de la activación, pero usualmente sucede así. Esto se produce cuando alguien da la noticia de un nuevo virus. Generalmente pasa a manos de la National Computer Security Association (NCSA) que se documenta y luego se distribuye a los diseñadores de antivirus.

Después del descubrimiento, los diseñadores de software modifican sus productos para incluir la detección del nuevo virus. Si los suficientes diseñadores de antivirus son capaces de detectarlo y limpiarlo.

Así como los suficientes usuarios adquieren antivirus apropiado para combatirlo, el virus puede estar cerca de ser extinguido. A pesar de que ningún virus ha desaparecido por completo, algunos han cesado por largo tiempo de aparecer en la comunidad informática.

HISTORIA DE LOS VIRUS:

PEVIO AL SURGIMIENTO DE INTERNET:

Los virus, en sus comienzos, se originaron partiendo de una investigación científica relativa a los conceptos de inteligencia artificial y vida artificial, y hasta el momento en que mentes maliciosas decidieron hacer uso de la idea para causar daños en sistemas informáticos, no eran más que meros experimentos universitarios. En 1950 Jonh Von Neumam desarrolló, por primera vez, el concepto de programas autorreplicantes que son programas que hacen que programas y datos se almacenasen conjuntamente en la memoria y que posibilitaba que ese código fuera alterado.

En 1960, en los laboratorios de Bell, se desarrolla un juego llamado Core Wars (Guerras del Núcleo), en el que dos programas luchaban entre sí por un espacio de memoria común y cuyo vencedor era el que conseguía más memoria. Los programas debían sobrevivir utilizando técnicas de ataque, ocultamiento y reproducción similares a las de los actuales virus informáticos.

En los años 70 se elaboran los primeros programas que se autorreproducían. Aparecieron los primeros gusanos, que, en un principio, no tenían un carácter destructivo sino experimental. La función de los gusanos era generar múltiples copias de ellos mismos a lo largo de una red de ordenadores.

En los año 80 aparecen los primeros virus experimentales y la primera definición de virus informático. En 1985 surgen los virus para MS-DOS y se propagaban por los disquetes. En 1986 aparece el primer virus dañino (Brain) que nació en Pakistán. En 1987 aparecieron los primeros virus que fueron ampliamente difundidos (Charlie, Lehigh y Viernes 13). En 1988 se produjo el primer ataque de un gusano a una red que entonces era ARPAnet, precursora de Internet; este gusano se difundía a través de correo electrónico y la erradicación del mismo costó 1 millón de dólares. Ese mismo año aparecieron ya los primeros programas antivirus. Un año más tarde aparecen virus con nuevas técnicas de ocultamiento y los programas antivirus desarrollan nuevas técnicas: heurística.

EN LA ERA DE INTERNET:

En los 90 prosigue el desarrollo de virus y se introducen nuevos conceptos como la infección rápida. En 1991 surge el primer Kit para la construcción de virus que facilitaba la tarea de crear un virus a cualquier usuario de ordenador medianamente experimentado. A mediados de la década de los noventa se produjeron enormes cambios en el mundo de la informática personal que llegan hasta hoy en día y que dispararon el número de virus en circulación hasta límites insospechados. Si a finales de 1994 el número de virus, según la Asociación de Seguridad Informática (ICSA), rondaba los cuatro mil, en los siguientes cinco años esa cifra se multiplicó por diez, y promete seguir aumentando.

La razón principal de este desmesurado crecimiento es el auge de Internet, que en 1994 comenzaba a popularizarse en Estados Unidos y un par de años más tarde empezaría a generalizarse en el resto del mundo. Para principios del nuevo milenio, la cifra de personas que se conectan a Internet habitualmente se estima en trescientos millones.

Por lo tanto, las posibilidades de creación y de expansión de los virus se han desarrollado hasta límites inimaginables hace tan sólo unos años. En primer lugar, porque los creadores de virus tienen a su disposición toda la información y las herramientas que necesitan para llevar a cabo sus creaciones. También pueden entrar en contacto con otros programadores. Finalmente pueden hacer uso de toda una serie de herramientas cuando desean dar a conocer sus creaciones a un mercado potencial de varios cientos de millones de usuarios.

El correo electrónico es probablemente el medio "estrella" de difusión de virus, aunque hay otras muchas vías mediante las cuales un ordenador puede llegar a infectarse por medio de la red. Los grupos de noticias son un medio que se suele utilizar habitualmente por la facilidad que supone enviar un mensaje con un fichero adjunto infectado a un grupo leído por cientos de miles de personas. La infección está garantizada.

En 1995, tras la aparición de Windows 95, se da el paso a la creación de los virus de macro. Estos virus se han extendido muy fácilmente porque los archivos que los incluyen son, en apariencia, archivos de datos (que, en teoría, no era posible infectar), aunque incluyen las secuencias de comandos de macro que los convierten en otra amenaza más para nuestro ordenador.

En 1999 aparecen los virus de tercera generación, es decir, virus que son capaces de viajar por medio de Internet, que están diseñados para explotar los recursos de la red para llevar una rápida propagación. El primero fue Happy99, pero el más conocido fue el "I Love You" que es un virus tipo gusano que se envía por IRC (Chat) y por correo electrónico. Miles de usuarios se vieron afectados por este virus. Llega al usuario vía e-mail con el asunto "I Love You" y con un fichero adjunto.

La clave de la rápida propagación está en que utiliza la libreta de direcciones del Outlook para reenviarse a todas las direcciones que se encuentran en ella. Las consecuencias de este virus fueron más de 3 millones de ordenadores infectados, con pérdidas de más de 2000 millones de dólares además de otros 6700 millones de dólares de pérdidas por el descenso registrado en la productividad. Este virus, además de borrar archivos en los PCs, afectó a los servidores de correo que sufrieron colapsos por la actividad del gusano.

En el 2000 apareció un nuevo foco de propagación: los teléfonos móviles. El virus se denomina "Timofonica" y, utilizando un mecanismo similar al "I Love You", el virus manda un mensaje a móviles de Telefónica. En noviembre de ese año apareció el virus "Hybris" y que el responsable del antivirus AVP lo califica como el virus más complejo y refinado jamás escrito en la historia de la programación de los virus informáticos. La principal característica de este virus, y también su principal problema, a la hora de detectarlo y de la desinfección es que tiene la capacidad de actualizar su código a través de la red utilizando para ello los grupos de noticias los días de luna llena.

Respecto al numeral 8.- Gusanos.

Se fabrica en 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 porque 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 subsecuentemente se destruirá, puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Respecto al numeral 9.- 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 donde se halla la bomba.

Respecto al numeral 10.- Piratas informáticos. (Mejor conocidos como 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.

Hacker: persona que disfruta explorando detalles de los sistemas programables y aprendiendo a usarlos al máximo, al contrario del operador común, que en general, se conforma con aprender lo básico.

Cracker: aquel que rompe con la seguridad de un sistema. El término fue acuñado por Hacker en 1985, oponiéndose al mal uso de la palabra Hacker por parte de la prensa.

Preaker: arte y ciencia de crackear la red telefónica para obtener beneficios personales (por ejemplo llamadas gratis de larga distancia).

Respecto al numeral 12.- Reproducción no autorizada de programas informáticos de protección legal.

La reproducción no autorizada de programas informáticos 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 modema.

Como delito no contemplado Rutinas cáncer.

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

Como delito no contemplado.- Creación de Puertas falsas.

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

Utilización de llave maestra (Superzapping).

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

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

Planeación o simulación de delitos convencionales utilizando la informática a fin de facilitar la comisión de los mismos (robo, homicidio, fraude, narcotráfico etc).

El listado anterior comprende los delitos conocidos al momento de elaboración del presente así como sus definiciones, por lo que pasaremos al siguiente punto que se deriva de este punto.

2.6.- AMBITO DE COMISIÓN DE DELITOS INFORMÁTICOS.

Para el estudio de este punto habremos de dividir en dos puntos geográficos las posibilidades de comisión de los delitos informáticos.

Por el espacio geográfico en que se planean y estructuran.- Lo anterior se refiere a los delitos en que por sus propias y especiales características, sus consecuencias se ven limitadas a un espectro físico relativamente pequeño y afectan por lo general únicamente al país de residencia del delincuente, teniendo como ejemplo de ellos: la producción ilegal de software, falsificaciones informáticas.

Por el espacio geográfico en él tiene consecuencia.- Lo anterior se refiere a los delitos en que por sus propias y especiales características su comisión tiene consecuencias transfronterizas, ya que su planeación puede llevarse a cabo en un sitio determinado, pero sus consecuencias se podrán reflejar en cualquier lugar del mundo, teniendo como ejemplo de ellos: Bomba lógica o cronológica, creación de virus, Hackers y Crackers.

El ámbito Internacional de comisión de estos delitos informáticos tiene como características, la falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos, ya que dada las diferentes legislaciones de una nación a otra existen conductas tipificadas como delito en algunos países mientras que en otras no es así, por lo tanto existe una ausencia de acuerdos globales en la definición legal de dichas conductas delictivas, y estas deficiencias son el motivo de la falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos

informáticos, por lo que es urgente la armonización entre las diferentes leyes procésales nacionales acerca de la investigación de los delitos informáticos a fin de poder combatir estos delitos, pese al carácter transnacional de los delitos cometidos mediante el uso de computadoras

CAPITULO III

LEGISLACIÓN NACIONAL E INTERNACIONAL REFERENTE A LOS DELITOS INFORMÁTICOS

3.1.- LEGISLACIÓN NACIONAL

En la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática aún no se contemplan los delitos informáticos dejando de lado a los legisladores del estado de Nuevo León pioneros en el tema y al Código Penal Federal . Sin embargo, después de analizar algunas de las leyes de otros países y el Código Penal del Estado citado se podría hacer alguna adaptación al problema de nuestro país, debiendo de considerar que es pertinente recurrir a aquellos tratados internacionales en 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.

Tratado de Libre Comercio de América del Norte (TLC)[18]

Este instrumento internacional firmado por los Gobiernos de México, los Estados Unidos de América y Canadá en 1993, contiene un apartado sobre propiedad intelectual, la 6a. parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

Resulta de vital importancia para este trabajo la presente referencia si observamos que el documento en comento en el párrafo 1 del artículo 1717 titulado Procedimientos y Sanciones Penales de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

---

[18] Tratado de Libre Comercio (TLC) Parte 3. Diario Oficial de la Federación. Lunes 20 de diciembre de 1993.

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.

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 estos consten en medios electrónicos o magnéticos.

Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio, incluso el comercio de mercancías falsificadas.

El Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT), manteniendo su vigencia hasta estos días.

Es de destacarse el hecho de que en este acuerdo, en el artículo 10, relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

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 u, denominada procedimientos penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales además de que, "los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias".

Finalmente, en la parte VII, denominada disposiciones institucionales, disposiciones finales, en el artículo 69 relativo a la cooperación

internacional, se establece el intercambio de información y la cooperación entre las autoridades de aduanas en lo que se refiere al comercio de mercancías de marca de fábrica o de comercio falsificadas y mercancías pirata que lesionan el derecho de autor.

Como se observa, el tratamiento que los dos instrumentos internacionales que se han comentado otorgan a las conductas ilícitas relacionadas con las computadoras es únicamente 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.

Ley Federal del derecho de Autor y Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en materia de Fuero Federal (Derogado)

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.

Es menester analizar la exposición de motivos de esta Ley por lo que trataremos de realizar alguno comentarios respecto a la misma y 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 inició la iniciativa correspondiente, se dijo que la importancia de pronunciarse al respecto era que con dicha iniciativa se atendía la complejidad que el tema de los derechos autorales había presentado en los últimos tiempos lo cual exigía una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión.

Además, se consideró que debido a que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de Derecho 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. En este sentido, consideramos importante detenernos en los artículos 102 y 231 de la presente Ley. 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.

No obstante la redacción limita de sobremanera las acciones que pudieran emprenderse en contra de este delito por lo que como parte de nuestra propuesta en líneas posteriores nos aventuraremos a dar una redacción que incluya los conceptos que de manera general contemplan otras legislaciones

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, fracción II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por esta Ley" y

"Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular".

Según nuestra opinión, la redacción de estas fracciones tratan de evitar la llamada piratería de programas en el área del comercio, permite la regulación administrativa de este tipo de conducta, como una posibilidad de agotar la vía administrativa antes de acudir a la penal, al igual que las infracciones contempladas para los programas de virus.

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 sancionaba con multa de 300 a 3 mil días o pena de prisión de seis meses hasta seis años al que incurriera en este tipo de delitos. Sin embargo, la regulación existente inclusive hoy en día en el Código Penal vigente para el Distrito Federal 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. incluso, la prensa continuamente publica notas en las que informa sobre las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que se remontan a varios miles de 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 enfrentaron juicios administrativos por el uso de programas piratas.

Esto, a la larga podría traer implicaciones de desventaja para México, entre los que podemos citar: la pérdida de prestigio a nivel internacional por el actuar ilícito de empresas cuyo radio de acción no está reducido al ámbito nacional y la pérdida de credibilidad por parte de las compañías proveedoras de programas informáticos, lo que se traduciría en un mercado poco atractivo para ellas 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 por las implicaciones que traería aparejadas, está totalmente justificada su regulación penal.

En otro orden, el Artículo 109 de la Ley citada, 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, al acceso no autorizado a una base de datos de carácter personal 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.

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 facultad 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 TLC y que por tal razón fue necesaria una segunda modificación, en abril del año en curso para incluir la acción de "reproducción".

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.

CÓDIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA.[19]

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos, 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:

I. Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o

II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

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

---

[19] Código Penal y de Procedimientos Penales del Estado de Sinaloa. Editorial. Anaya 1996. México D.F.

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 al delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad y a la información, bien jurídico tan importante para el ser humano como el mismo patrimonio.

CODIGO PENAL FEDERAL

Libro Segundo

Titulo Noveno Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática

Capitulo I Revelación de Secretos

ARTÍCULO 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

ARTICULO 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado publico o cuando el secreto revelado o publicado sea de carácter industrial.

ARTICULO 211 BIS.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicaran sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Capitulo II Acceso Ilícito a Sistemas y Equipos de Informática

ARTICULO 211 BIS 1.- Al que sin autorización modifique, destruya o provoque perdida 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.

ARTICULO 211 BIS 2.- Al que sin autorización modifique, destruya o provoque perdida 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.

ARTICULO 211 BIS 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida 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.

ARTICULO 211 BIS 4.- Al que sin autorización modifique, destruya o provoque perdida 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.

ARTICULO 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 perdida 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 articulo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

ARTICULO 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 articulo 400 bis de este código.

ARTICULO 211 BIS 7.- Las penas previstas en este capitulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

3.2.- LEGISLACIÓN INTERNACIONAL

Una vez que hemos reseñado la legislación nacional referente a delitos informáticos y al derecho informático, pasaremos a citar alguna de las principales leyes que en algunos otros países se han establecido para combatir los delitos informáticos, siendo importante mencionar que esta es mas extensa ya que el desarrollo del derecho informático ha tenido más énfasis en otras latitudes.

A fin de hacer este listado de manera didáctica citaremos las leyes y los cometarios al respecto por países.

Alemania

A partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica en la que se contemplan los siguientes delitos:

Espionaje de datos

Estafa informática

Falsificación de datos probatorios 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.

Alteración de datos, es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.

Sabotaje informático, destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

Utilización abusiva de cheques o tarjetas de crédito.

Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987. Contempla los siguientes delitos:

Destrucción de datos, no solo datos personales sino también los no personales y los programas.

Estafa informática, se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Francia

La Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

Sabotaje Informático. Falsear el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique los documentos informatizados con intención de causar un perjuicio a otro.

Estados Unidos

Estados Unidos en 1994 modificó con el Acta Federal de Abuso Computacional su antecedente, el Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya 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, a los sistemas informáticos, a las redes, información, datos o programas.

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. Definiendo dos niveles para el tratamiento de quienes crean virus:

a.- Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.

b.- Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

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.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

Inglaterra

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

a) Impedir la operación de cualquier computadora; o

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

c) Impedir la ejecución de cualquiera de esos programas, o la confianza en esos datos."

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

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

Holanda.

El 1º de Marzo de 1993 entró en vigencia la **Ley de Delitos Informáticos**, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

España

En el **nuevo Código Penal español** (aprobado por Ley-Orgánica 10/1995, de 23 de Noviembre / BOE número 281, de 24 de Noviembre de 1.995) hay varios artículos íntimamente relacionados con el tema que estamos tratando.

Son los siguientes: *(Nota previa: El concepto de días-multa introducido por el artículo 50 indica que la cuota diaria tendrá un mínimo de doscientas pesetas y un máximo de cincuenta mil pesetas. A efecto de cómputo, los meses son de treinta días y los años de trescientos sesenta días.)*

Artículo 197

1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2.- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en

ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3.- Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4.- Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5.- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6.- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199

1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena

de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

Artículo 201

1.- Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2.- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3.- El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

Artículo 211 (Nota: Tanto este artículo como el siguiente presentan un bonito debate. ¿Se pueden considerar que son de *eficacia semejante* Internet y los medios de comunicación tradicionales? ¿Son *responsables* los administradores de sistema o las empresas propietarias de los servidores?).

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

Artículo 238

Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes

1º.- Escalamiento.

2º.- Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.

3º.- Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras **o descubrimiento de sus claves para sustraer su contenido**, sea en el lugar del robo o fuera del mismo.

4º.- Uso de llaves falsas.

5º.- Inutilización de sistemas específicos de alarma o guarda.

Artículo 239

Se considerarán llaves falsas:

1º.- Las ganzúas u otros instrumentos análogos.

2º.- Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.

3º.- Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.

A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Artículo 248

1.- Cometen estafa los que, con ánimo de lucro, utilizar engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Artículo 255

Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1º.- Valiéndose de mecanismos instalados para realizar la defraudación.

2º.- Alterando maliciosamente las indicaciones o aparatos contadores.

3º.- Empleando cualesquiera otros medios clandestinos.

Artículo 256

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

Artículo 263

El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

Artículo 264

1.- Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:

1º.- Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2º.- Que se cause por cualquier medio infección o contagio de ganado.

3º.- Que se empleen sustancias venenosas o corrosivas.

4º.- Que afecten a bienes de dominio o uso público o comunal.

5º.- Que arruinen al perjudicado o se le coloque en grave situación económica.

2.- La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Artículo 270

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

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

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

Artículo 278

1.- El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2.- Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren , revelaren o cedieren a terceros los secretos descubiertos.

3.- Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 400

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536

La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios

técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

JAPÓN

Una ley aprobada en el Japón en el año 1988, dispuso la imposición de multas de hasta cien mil yens a quien incumpla las regulaciones para la protección de datos o realice otros actos ilícitos relacionados con el procesamiento de datos.

PORTUGAL

La Ley de Protección de Datos Personales Informatizados de 29 de abril de 1991, prevé en también penas de multa y privación de libertad para los que utilicen datos ilegalmente, consigan acceso no autorizado a las bases de datos, realicen interconexiones ilegales y otras conductas.

PERU

DELITOS INFORMATICOS TIPIFICADOS EN EL CODIGO PENAL PERUANO

En el ordenamiento jurídico peruano, se tipifican los siguientes delitos que tienen aplicación directa en el campo informático, y que consideramos están dentro del concepto general de los delitos informáticos :

a) Delito de Violación a la Intimidad.

En este Código Penal está tipificado en el artículo 154 el Delito de violación a la intimidad, y establece que : "el que viola la intimidad de la vida personal y familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios será reprimido con pena privativa de libertad no mayor de dos años. La pena será no menor de uno ni mayor de tres y de treinta a ciento veinte días cuando el agente revela la intimidad conocida de la manea antes prevista".

El artículo 157 del Código Penal en cita precisa que "el que indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida intima de una o más personas será reprimido con pena privativa de libertad no

menor de un año ni mayor de cuatro años. Si el agente es funcionario o servidor público y comete delito en ejercicio del cargo, la pena será no menor de tres años ni mayo de seis e inhabilitación". Las base de datos computarizadas consideramos que están dentro del precepto de "cualquier archivo que tenga datos", en consecuencia está tipificado el delito de violación a la intimidad utilizando la informática y la telemática a través del archivo , sistematización y transmisión de archivos que contengan datos privados que sean divulgados sin consentimiento.

b) Delito de Hurto agravado por Transferencia Electrónica de Fondos, telemática en general y empleo de claves secretas.

El artículo 185 del ordenamiento legal citado establece que aquella persona que "... para obtener provecho, se apodera ilegítimamente de un bien total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Se equipara a bien mueble la energía eléctrica, el gas, el agua y cualquier otro elemento que tenga valor económico, así como el espectro electromagnético".

El artículo 186 segundo párrafo numeral 3 - modificado por la ley 26319- dispone además "la pena será no menor de cuatro años ni mayor de ocho si el hurto es cometido mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas". El delito de hurto agravado por transferencia electrónica de fondos tiene directa importancia en la actividad informática.

El sistema de transferencia de fondos , en su conjunto, se refiere a la totalidad de las instituciones y prácticas bancarias que permiten y facilitan las transferencias interbancarias de fondos. El desarrollo de medios eficientes de transmisión de computadora a computadora de las órdenes de transferencia de fondos ha fortalecido el sistema. Los niveles de calidad y seguridad de las transferencias interbancarias de fondos se han ido acrecentando conforme el avance de la tecnología, no obstante la vulnerabilidad a un acceso indebido es una "posibilidad latente" por tanto además de los sistemas de seguridad de hardware , software y comunicaciones ha sido necesario que la norma penal tenga tipificada esta conducta criminal.

Uno de los medios de transferencia electrónica de fondos se refiere a colocar sumas de dinero de una cuenta a otra, ya sea dentro de la misma entidad financiera o una cuenta en otra entidad de otro tipo, ya sea pública o privada. Con la frase "telemática en general" se incluye todas aquellas transferencias u operaciones cuantificables en dinero que pueden realizarse en la red informática ya sea con el uso de Internet , por ejemplo en el Comercio Electrónico o por otro medio. Cuando se refiere a "empleo de claves secretas" se está incluyendo la vulneración de password, de niveles de seguridad, de códigos o claves secretas.

c) Delito de Falsificación de Documentos Informáticos.

El Decreto Legislativo 681 modificado por la Ley 26612, es la norma que regula el valor probatorio del documento informático, incluyendo en los conceptos de microforma y microduplicado tanto al microfilm como al documento informático. El artículo 19 de esta norma establece que : "la falsificación y adulteración de microformas, microduplicados y microcopias sea durante el proceso de grabación o en cualquier otro momento, se reprime como delito contra la fe pública, conforme las normas pertinentes del Código Penal".

Las microformas que cumplidos los requisitos técnicos (equipos y software certificados que garantizan inalterabilidad, fijeza , durabilidad, fidelidad e integridad de documentos micrograbados) y formales (que procesos de micrograbación sean autenticados por un depositario de la fe pública, por ejemplo el fedatario juramentado en informática) sustituyen a los documentos originales para todos los efectos legales.

En el Código Penal Peruano (C.P.), entre los delitos contra la fe pública, que son aplicables a la falsificación y adulteración de microformas digitales tenemos los siguientes :

d) Falsificación de documentos. "El que hace, en todo o en parte, un documento falso o adultera uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho con el propósito de utilizar el documento, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de dos ni mayor de diez años..." (Artículo 427 del C.P.). Tratándose de microformas digitales su falsificación y/o adulteración son sancionados con la misma pena.

i) Falsedad ideológica "El que inserta o hace insertar , en instrumento público , declaraciones falsas concernientes a hechos que deben probarse con el documento, con el propósito de emplearlo como si la declaración fuera conforme a la verdad, será reprimido si de uso puede resultar algún perjuicio , con pena privativa de libertad no menor de tres ni mayor de seis años.." (Artículo 428 del C.P.). Hay que tener en cuenta que la microforma digital de un documento público tiene su mismo valor, por tanto puede darse el caso de falsedad ideológica de instrumentos públicos contenidos en microformas digitales.

i) Omisión de declaración que debe constar en el documento. "El que omite en un documento público o privado declaraciones que deberían constar o expide duplicados con igual omisión al tiempo de ejercer una función y con el fin de dar origen a un hecho u obligación , será reprimido con pena privativa de libertad no menor de uno ni mayor de seis" (Artículo 429 del C.P.). Para que tenga valor probatorio y efecto legal una microforma digital tiene que cumplir requisitos formales y técnicos. El requisito formal consiste en que debe ser autenticado por depositario de la fe pública (fedatario juramentado o notario) el proceso técnico de micrograbación y que las copias de esos documentos deben ser certificados, por lo cual una omisión de las declaraciones que por ley deben incluirse podría configurar esta figura delictiva.

d) Delito de Fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos.

Puesto que en el patrimonio de la persona están incluidos tanto bienes materiales (hardware) como inmateriales (software, información, base de datos, etc) esta figura delictiva puede aplicarse al campo informático según interpretación del artículo 198° inciso 8 del Código Penal, establece que : "será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años el que, en su condición de fundador, miembro del directorio o del consejo de administración o del consejo de vigilancia, gerente, administrador o liquidador de una persona jurídica, realiza, en perjuicio de ella o de terceros, cualquiera de los actos siguientes : Usar en provecho propio o de otro, el patrimonio de la persona (inciso 8). Esta figura podría aplicarse, en este orden de ideas, tanto al uso indebido de software, información, datos informáticos, hardware u otros bienes que se incluyan en el patrimonio de la persona jurídica.

e) Delito contra los derechos de autor de software.

Con respecto a los delitos contra los derechos de autor de software, debe tenerse en cuenta que "...sobre la naturaleza jurídica y la tutela que apunta el derecho de autor sobre el software hay acuerdo general. Y no puede ser de otro modo, debido a la trascendencia que tiene, dado que la trasgresión de índole penal ala actividad intelectual constituye no sólo una agresión a la propiedad del autor y afecta los intereses de la cultura, sino que conforma también un ataque al derecho moral sobre la paternidad de la obra".

Con la dación del Decreto Legislativo 822, se modificó el Código Penal y se han aumentado las penas, con respecto a la legislación peruana anterior, así tenemos:

I) Que el artículo 217° del Código Penal Peruano establece que "será reprimido con pena privativa de libertad no menor de dos ni mayor de seis años y con treinta a noventa días-multa, el que con respecto a una obra,...o una grabación audiovisual o una imagen fotográfica expresada en cualquier forma, realiza cualquiera de los siguientes actos, sin la autorización previa y escrita de autor o titular de los derechos.

a) la modifique total o parcialmente.

b) La reproduzca total o parcialmente, por cualquier medio o procedimiento.

c) La distribuya mediante venta, alquiler o préstamo público.

d) La comunique o difunda públicamente por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho.

e) La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito.

Aquí se están garantizando bajo la protección los derechos patrimoniales; en los contratos de licencia de uso de software se contemplan el respeto de estos derechos y también en la Ley de Derecho de Autor que anteriormente hemos tratado. La autorización previa y escrita del titular, generalmente en la activad empresarial se instrumenta en una licencia de uso de software.

II) Que el Artículo 218º del Código Penal Peruano dispone que "la pena será privativa de libertad no menor de dos ni mayor de ocho años y sesenta a ciento veinte días-multa cuando:

a) Se de a conocer a cualquier persona una obra inédita o no divulgada, que haya recibido en confianza del titular del derecho de autor o de alguien en su nombre, sin el consentimiento del titular.

b) La reproducción, distribución o comunicación pública se realiza con fines de comercialización, o alterando o suprimiendo, el nombre o seudónimo del autor, productor o titular de los derechos.

c) Conociendo el origen ilícito de la copia o reproducción, la distribuya al público, por cualquier medio, la almacene, oculte, introduzca al país o la saca de éste.

d) Se...ponga de cualquier otra manera en circulación dispositivos, sistemas, esquemas o equipos capaces de soslayar otro dispositivo destinado a impedir o restringir la realización de copias de obras, o a menoscabar la calidad de las copias realizadas; o capaces de permitir o fomentar la recepción de un programa codificado, radiodifundido o comunicado en otra forma al público, por aquellos que no estén autorizados para ello.

e) Se inscriba en el Registro del Derecho de Autor la obra,... como si fuera propia, o como de persona distinta del verdadero titular de los derechos.

Los supuestos tratados en este artículo se refieren tanto a derecho morales como patrimoniales, que por su gravedad (atentar contra el derecho de paternidad, comercializar o distribuir copias ilegales, registrar en forma indebida el software) se amplía la pena hasta ocho años. En la anterior legislación la pena mayor por este tipo de delitos era de cuatro años, actualmente se ha aumentado a ochos años. Estos tipos penales, parten del supuesto que no hay consentimiento o autorización del titular de los derechos para ello; de existir una licencia de uso y cumplirse con sus términos y condiciones, no se tipificaría este delito.

III) Que el Artículo 219º del Código Penal Peruano, establece que :"será reprimido con pena privativa de libertad no menor de dos ni mayor de ocho años y sesenta a ciento ochenta días-multa, el que con respecto a una obra, la difunda como propia, en todo o en parte, copiándola o reproduciéndola textualmente, o tratando de disimular la copia mediante ciertas alteraciones, atribuyéndose o atribuyendo a otro, la autoría o titularidad ajena".

La apropiación de autoría ajena, de reputarse una obra que no es de uno como propia, también se aplica la software, más aún con las opciones tecnológicas para su copia, que incluyen equipos de cómputo, cada vez más sofisticados y el uso de herramientas en Internet.

IV) Que el Artículo 220º del Código Penal Peruano, dispone que: " será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y noventa a trescientos sesenta y cinco días-multa:

a) Quien se atribuya falsamente la calidad de titular originario o derivado, de cualquiera de los derechos protegidos en la legislación del derecho de autor y derechos conexos y, con esa indebida atribución, obtenga que la autoridad competente suspenda el acto de comunicación, reproducción o distribución de la obra, interpretación, producción, emisión o de cualquier otro de los bienes intelectuales protegidos.

e) Si el agente que comete cualquiera de los delitos previstos... posee la calidad de funcionario o servidor público.

Una de las preocupaciones de los creadores de software, al registrar su obra en el Registro Nacional de Derecho de Autor de INDECOPI, es que se tiene que entregar, entre otros requisitos, el programa fuente, se cuestionan que sucede si lo copian sin su consentimiento. Dado que el depósito es intangible, los funcionarios que cometieran estos delitos estarían dentro de este tipo penal y podrían ser pasibles de pena privativa de libertad hasta ocho años.

CHILE

Ley de Delitos Informáticos.

CUBA

Desde 1993 entró en vigor el Reglamento de Protección de Datos y Sistemas Informáticos, así como la articulación nacional de la Comisión de Protección de Datos, que desde el año 1988 viene trabajando en el país y cuyo esfuerzo mereció el reconocimiento del PII-UNESCO al concedérsele a éste en el año 1993, la realización del Proyecto "Laboratorio Latinoamericano de Protección contra Virus Informáticos", institución que hasta la fecha ha formado especialistas del área y ha servido al desarrollo de sistemas autóctonos de protección

informática, así como al diseño e implementación de políticas y estrategias de Seguridad Informática.

COSTA RICA

En el aspecto legislativo sobre el derecho informático, tenemos que existe una propuesta de legislación del recurso del Habeas Data presentada a la asamblea legislativa por iniciativa del señor Diputado Dr. Constantino Urcuyo, proyecto de ley que pretende reformar la Ley de la Jurisdicción Constitucional, con el fin de incorporar dicho recurso del Habeas Data en Costa Rica, el cual resulta interesante debido a que intenta recoger una necesidad sentida de proteger la intimidad, dignidad y autodeterminación de los ciudadanos frente a los retos que ofrece el procesamiento automatizado de datos personales, lo cual a la fecha probablemente ya se encuentre instituido en legal forma.

3.3.ORGANIZACIONES INTERNACIONALES ENFOCADAS A LA REGULACIÓN Y PREVENCIÓN DE LOS DELITOS INFORMÁTICOS.

Dada la importancia del tema a lo largo del mundo se han realizado muchísimos esfuerzos para regular de manera transfronteriza la comisión de los delitos informático, además de que se ha tratado de resumir y ordenar los esfuerzos individuales de los países, a fin de que la aldea global que lo único que no tiene son fronteras cuente con la seguridad necesaria es por eso que este punto se enfoca a hacer un breve listado y descripción de estos organismos citados.

Organización de Cooperación y Desarrollo Económico (OCDE)

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 uso indebido de los programas de computación.

En 1986 la OCDE publicó un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se señalan las normativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1992 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.

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables, así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

LA ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU)

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.

ASOCIACIÓN INTERNACIONAL DE DERECHO PENAL

La Asociación Internacional de Derecho Penal durante un coloquio celebrado en Witrzburgo 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.

ACUERDO GENERAL DE TARIFAS Y ARANCELES ADUANEROS (GATT)

GATT.- Acuerdo de la Ronda Uruguay de Aranceles Aduaneros y Comercio, Art. 10 relativo a los programas de ordenador y compilaciones de datos, serán protegidos como obras literarias de conformidad con el Convenio de Berna para la protección de obras Literarias y Artísticas.

Ciberpolicías.- Tanto NSA, FIRST Forum of Incident Response and Security Teams y CERT Computer Emergency Response Team tienen equipos de especialistas dedicados a la localización de Hackers, defensa frente a sabotajes e intervención en caso de siniestros informáticos. Por otra parte, algunas policías como el FBI y Scotland Yard disponen de unidades especiales para investigar la comisión de delitos a través de la red.

UNESCO (ORGANIZACION DE LAS NACIONES UNIDAS PARA LA EDUCACIÓN LA CIENCIA Y LA CULTURA)

La UNESCO, en sus pronunciamientos relativos a las Autopistas de la Información, ha declarado que "el aumento del acceso a redes y bases de datos interconectadas incrementa el valor de los principios éticos y legales, incluyendo:

La privacidad de la información y el derecho que tiene cada individuo a chequear sus propios datos como derecho humano fundamental.

La lucha contra la piratería internacional y otros delitos.

La protección de los derechos de los creadores de software.

En fecha muy reciente, la propia UNESCO se ha pronunciado en contra del uso que se está dando a estas redes de alcance global para la difusión de pornografía, y el comercio de mujeres, e incluso de niños.

EL CONSEJO DE EUROPA

El Consejo de Europa, ya desde 1973, emitió recomendaciones a los gobiernos de sus estados miembros para tomar precauciones contra todo abuso o mal empleo de la información señalando 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.

PICS (PLATFORM FOR INTERNET CONTENT SELECTION, PLATAFORMA DE SELECCIÓN DE CONTENIDOS DE INTERNET

La norma PICS (Platform for Internet Content Selection, plataforma de selección de contenidos de Internet), que lanzó oficialmente el World Wide Web Consortium.

Constituye un intento de establecimiento de una norma mundial para toda la industria. PICS, que ofrece un "control del acceso a Internet sin censura", está apoyada por una amplia coalición de fabricantes de material y programas informáticos, suministradores de acceso, servicios comerciales en línea, editores y suministradores de contenido. Actualmente se incluye como característica normal en navegadores (browsers) de Internet, como Microsoft Explorer o Netscape 3.0, y también cuenta con el apoyo de una serie de conjuntos de programas de filtrado.

Convención para la Protección y Producción de Fonogramas.

Convención relativa a la Distribución de Programas y Señales.

Convenios de la OMPI.

3.4. PARTICIPACIÓN DE MÉXICO EN EL AMBITO INTERNACIONAL

Al inicializar 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 primer instituto citado siguen siendo vigentes.

En este entendido, cabe mencionar que el Gobierno de México es parte de este acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio (GATT) manteniendo su vigencia hasta nuestros días.

Consideramos que debe destacarse el hecho de que en este acuerdo, en el artículo 10, relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad de acuerdo al Convenio de Berna de 1971 para la protección de Obras Literarias, y que las compilaciones de datos que sean legibles serán protegidos como creaciones de carácter intelectual.

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

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

Finalmente, en la parte VII, denominada disposiciones institucionales, disposiciones finales, en el artículo 69 relativo a la cooperación internacional, se establece el intercambio de información y la cooperación entre las autoridades de aduanas en lo que se refiere al comercio de mercancías de marca de fábrica o de comercio falsificadas y mercancías pirata que lesionan el derecho de autor.

Como 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 de nuestro país.

TRATADO DE LIBRE COMERCIO DE AMERICA DEL NORTE (TLC)

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la 6ª parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.

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.

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.

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.

Lo cual innegablemente pone en riesgo a los mismos de sufrir ataques por parte de delincuentes informáticos.

POLICIA FEDERAL PREVENTIVA, POLICIA CIBERNETICA

Ahora bien aunque no implica participación de México en el ámbito internacional, considero necesario incluir en este trabajo la presentación que la Policía Federal Preventiva hace de la Ciber Policía dedicada a la vigilancia de la Red en nuestro país, a efecto de lo cual se transcriben las siguientes notas periodísticas que al respecto de publicaron en el diario Reforma.

"En el marco de una reunión nacional para la prevención, atención y erradicación del fenómeno del comercio y explotación sexual infantil, que se desarrolló el miércoles pasado en Cancún, el director general de Protección de los Derechos Humanos de la Secretaría de Seguridad Pública, Antonio del Valle Martínez, anunció la creación de la unidad de policía cibernética en México, adscrita a la coordinación general de inteligencia de la Policía Federal Preventiva.

Manifestó que los delitos contra menores se han convertido en un asunto complejo, porque difícilmente la autoridad puede actuar contra los delincuentes que utilizan principalmente medios informáticos para sus actos.

El poder legislativo no lo ha tomado en cuenta, agregó, y las leyes no castigan ejemplarmente a quienes se atreven a dañar a niños y niñas.

En su ponencia, el funcionario dijo que no existe un esfuerzo nacional que combata este tipo de crímenes y las legislaciones locales no son suficientes, lo que ocasiona un desinterés en la investigación policíaca y la consecuente impunidad de los depravadores.

La Unidad de Policía Cibernética, contará con un área específica en materia de investigación de delitos contra menores, y atenderá los casos en que se involucra a menores de edad como población vulnerable.

Además, elaborará el primer banco nacional de datos sobre pedófilos y sobre el modus operandi de bandas de robachicos.

Pero también este grupo tendrá la tarea de realizar operaciones de patrullaje "anti hacker" en el ciberespacio, dijo, como un instrumento para atrapar a los delincuentes que cometen fraude, intrusiones y organizan sus actividades delictivas en la Red.

Finalmente, hará un análisis de la información recolectada en campo, para combatir los delitos que tienen lugar en la Red.

De manera encubierta desplegará operaciones para detectar sitios donde se transmite pornografía infantil y donde un menor puede ser contactado por los delincuentes para, sin escrúpulos, inducirlo a actos inmorales.

En días pasados la policía cibernética logró la identificación de una organización pedófila que opera en Acapulco, Guerrero, agregó el funcionario.

Respecto de sitios de Internet, dijo, algunas organizaciones no gubernamentales han reportado casos de pedofilia, principalmente en comunidades de la Web como Microsoft Network y Yahoo.

Al reunirse con Diputados de la Comisión de Atención a Grupos Vulnerables, Suárez Valenzuela dijo que este tipo de delitos deben ser catalogados como graves y de carácter federal.

Mencionó que la Secretaría de Seguridad Pública constituyó la Policía Cibernética, que tiene como objetivo navegar por la red para identificar, perseguir y detener a todas aquellas organizaciones que operan con pornografía.

El problema, explicó, puede ser tan grande y tan grave como el de que cada día más familias adquieren un equipo de cómputo y tienen acceso a Internet, sin que el acceso a las páginas de estas organizaciones sea restringido.

Agregó que la situación entre los menores de edad es grave, pues dados los ofrecimientos que se les hacen a través de este medio, cada día son más los que caen en sus redes.

De acuerdo con el funcionario, en México existen cerca de 100 páginas en la red, las cuales pueden conectar a un usuario a muchas más a nivel internacional.

En este momento, detalló, existen cerca de 60 elementos de la policía cibernética que de manera encubierta navegan por Internet en busca de sitios que pudieran representar un riesgo para los menores.

Planteó la necesidad de establecer un registro de personas convictas por delitos sexuales violentos y de abuso contra menores, administrado por la PFP y en el cual de manera constante se notifiquen lo cambios de domicilios.

También legislar lo necesario para que la Policía pueda pedir a los proveedores de servicio de Internet los registros usados para cometer actividades delictivas en este medio y para que los jueces acepten como evidencia una prueba "lógica" presentada en cualquier medio magnético.

Suárez Valenzuela propuso la elaboración de convenios bilaterales con los países de donde proviene el mayor número de turistas que buscan tener sexo con menores de edad mexicanos.

Destacó que este punto parte del hecho de que luego que desmembraron una banda que operaba en Acapulco, Guerrero, detectaron que esta tenía enlaces con otras organizaciones que operan en Estados Unidos, Canadá, Holanda, Rusia, Alemania, Australia y algunas naciones de África y Centro América."

"Los crímenes cometidos en agravio de menores a través de una computadora y otros medios han tenido un crecimiento sin precedente en estos tiempos de globalización. Un efecto colateral de lo anterior lo constituye el alarmante incremento de casos -tanto en México como en el mundo- de organizaciones criminales de pedófilos que promueven y transmiten vía Internet la pornografía infantil y la corrupción de menores", señaló.

Al reunirse con Diputados de la Comisión de Atención a Grupos Vulnerables, el funcionario de la Secretaría de Seguridad Pública indicó que, ante esta situación, la dependencia constituyó la Policía Cibernética, que tiene como objetivo navegar por la red para identificar, perseguir y detener a las organizaciones que operan en este ramo.

El problema, explicó Suárez Valenzuela en entrevista posterior al encuentro, puede ser tan grande y tan grave como el hecho de que cada día más familias

adquieren un equipo de cómputo y tienen acceso a Internet, sin que la entrada a las páginas de estas organizaciones esté restringido.

Dijo que la situación entre los menores de edad es grave, ya que los ofrecimientos que se les hacen a través de estos portales cada día son más atractivas por lo que muchos de los niños y adolescentes caen en estas trampas.

"Es muy difícil establecer la proporción del problema, si usted me dice cuántos niños tienen computadora, cuántos niños pueden ingresar a una red de Internet, entonces serían los parámetros para poderlo saber. Es muy difícil explicarlo.

"El problema está tan extendido como lo que tú quieras acceder a cualquier sistema, entrar a una red a navegar y encontrar lo que tú quieras, como buscar un coche, buscar un terreno, lo que tú quieras lo vas a encontrar. Esa es la extensión de este delito", indicó.

De acuerdo con Suárez Valenzuela, en México existen cerca de 100 páginas en la red, las cuales pueden conectar a un usuario a muchas más a nivel internacional.

En este momento, detalló, existen cerca de 60 elementos de la Policía Cibernética que navegan por Internet en busca de sitios que pudieran representar un riesgo para los menores.

"Trabajamos en la computadora diario, diario estamos en ello, la gente está preparándose para poder obtener ese tipo de información, tener acceso a la información, es una gente profesional dedicada días enteros a ese tipo de trabajo, son expertos en sistemas de cómputo", señaló.

"Aquí", continuó, "no necesitamos armas, necesitamos cerebro, papel y lápiz y eso es lo que está haciendo el personal de la Policía Cibernética, ellos están intentan identificar las líneas, los sitios donde tratan de enganchar a los niños o de poderlos involucrar en este tipo de delitos".

Por la gravedad del asunto, y dadas las lagunas existentes en la legislación penal, sobre estos delitos, Suárez Valenzuela propuso a los Diputados establecer las medidas legislativas que permitan federalizarlos y catalogarlos como graves.

Planteó la necesidad de establecer un registro de personas convictas por delitos sexuales violentos y de abuso contra menores, administrado por la PFP y en el cual de manera constante se notifiquen lo cambios de domicilios.

También les pidió "legislar lo necesario" para que la policía pueda pedir a los proveedores de servicio de Internet los registros usados para cometer actividades delictivas en este medio y para que los jueces acepten como evidencia una prueba 'lógica' presentada en cualquier medio magnético.

Del mismo modo, propuso la elaboración de convenios con los países de donde

proviene el mayor número de turistas que buscan tener sexo con menores mexicanos, destacando que este punto parte del hecho de que al desmembrar una banda que operaba en Acapulco, Guerrero, detectaron que esta tenía enlaces con organizaciones que operan en Estados Unidos, Canadá, Holanda, Rusia, Alemania, Australia y algunos países de África y Centro América."

De las anteriores notas se desprende el grado de importancia que los delitos informáticos tienen y que el mismo se ha develado a nuestras autoridades, al grado de obligarlas a establecer este tipo de controles policíacos, es de vital importancia señalar que este esfuerzo, solo vera verdaderos resultados cuando los esfuerzos internacionales se concentren y establezcan las medidas de colaboración necesarias, pues no se debe olvidar que uno de las características de los delincuentes informáticos es que no requieren de estar presentes físicamente en un determinado lugar para cometer ilícitos, la Policía Federal Preventiva deberá coordinar a su policía cibernética, con sus elementos de inteligencia y los de tarea, a fin de que los primeros puedan ubicar en la Red paginas, sitios Web o inclusive portales ubicados en México, así como delincuentes cibernéticos nacionales, a fin de que los últimos puedan ubicarlos físicamente en territorio nacional y se pueda proceder a la detención.

CAPITULO IV
LA NECESIDAD DE REGULAR LOS DELITOS INFORMÁTICOS EN LOS CÓDIGOS PENALES DEL DISTRITO FEDERAL Y EL ESTADO DE MÉXICO

4.1. AMBITO DE COMISION DE LOS DELITOS INFORMATICOS EN NUESTRO PAÍS.

El desarrollo y participación de los delincuentes informáticos en nuestro país, afortunadamente es limitado y el mismo se ha centrado básicamente al uso y reproducción de programas protegidos por el derecho de autor, si bien esto podría parecer estimulante se deberá de tomar en cuenta que esto no se debe a ninguna logro de las autoridades ni a programas encaminados a la prevención, sino a diversos factores que a continuación se detallan:

INICIACION DE PROCESOS.- Respecto a este punto es importante señalar que el único organismo que se ha dedicado a denunciar y a perseguir delitos que se pueden considerar incluidos dentro de los denominados Informáticos es el Instituto Nacional de Protección a los Derechos de Autor, el cual fundamentándose en la ley federal del derecho de autor se ha encargado de perseguir y sancionar a todo tipo de usuarios de programas reproducidos ilegalmente sin importar la magnitud de la empresa u organización de la que se trate, y por supuesto en coordinación con diversos organismos policíacos ha instrumentado operativos tendientes al decomiso de material "pirata" y a la detención de las personas que se encargan de comercializarlo, por supuesto que la actuación de este instituto tiene algunas aristas que han impedido que sus esfuerzos brinden una ambiente de seguridad total o prevención de los delitos que persigue, se afirma lo anterior en virtud de que en la gran mayoría de los operativos realizados únicamente se ha detenido a comercializadores, personas que compran su mercancía a grandes productores de material ilegalmente reproducido y que al ser sujetos a una averiguación previa o a un proceso alcanzan fácilmente su libertas dado lo simple del delito o falta administrativa cometida, también se enfrentan al problema de que cada vez es mas común el hecho de que la mercancía decomisada ostenta claramente leyendas de que la música fue adquirida en formato MP3 por medio de buscadores de este formato en Internet, grabados a discos de audio y reproducidos masivamente en megacopiadores profesionales, por lo tanto como se puede tipificar y castigar como delito una acción que deviene de el download (bajar de la red) de un material que se ofrece gratuitamente, por ultimo se debe de señalar que este instituto no tiene ingerencia sobre otro tipo de delitos informáticos por lo que se reitera su actuación es bastante limitada.

Otro de los factores que limitan la iniciación de procesos es la imagen de las instituciones que los sufren, este punto es hasta cierto punto entendible si se analiza el hecho de hasta que punto se afectaría la imagen digamos, de un banco si se da a conocer en forma pública y masiva el hecho de que una institución de este tipo vío vulnerados sus sistemas de seguridad

informática y que algún Hacker consiguió acceso a sus bancos de datos, cuales serían las consecuencia de un acto de esta naturaleza, cualquier delincuente tradicional al recibir esta información de un delincuente cibernético, podría orquestar un secuestro en contra de las personas que según los estados de cuenta consultados podrían representarles un enorme ingreso económico.

Pero aun mas dañino para la imagen de una Institución bancaria seria el hecho de que algún delincuente empezara a transferir fondos de una cuenta a otra e incluso de una institución a otra utilizando técnicas de triangulación inclusive entre países con lo cual sería prácticamente imposible el seguir la pista de los fondos ilegalmente transferidos, que persona en su sano juicio invertiría en un banco que hiciera público el haber sido victima de un delito así.

Estas son solo algunas de las razones por las que las Instituciones bancarias no denuncian estos ilícitos, pero podemos tener la seguridad de que existen las posibilidades, ya que cada vez aumentan las aseguradoras que implementan programas para asegurar instituciones contra este tipo de eventos.

Solo que estas instituciones no son las únicas en nuestro país que resultan atractivas a los delincuentes informáticos, ¿cuanto vale para las personas su información personal? ¡cualquier cantidad!, que datos extraordinariamente importantes se alojan en las miles y miles de computadoras que funcionan en nuestro país, ¡todos¡ si un Hacker irrumpe en los datos contenidos en una computadora, o si intercepta y copia información enviada vía correo electrónico, en una acción que no requiere violencia y que la mayoría de las veces no deja huella las posibilidades de chantaje se vuelven obvias.

DESCONOCIMIENTO DE LOS DELITOS SU PUNIBILIDAD Y CONSECUENCIAS DE LOS MISMOS.- Muchas veces y como ya lo hemos referido en el análisis de las características de los delitos informáticos el desconocimiento de que una acción conforma un delito, lleva a personas de conducta honorable a cometerlos, ahora bien si el delincuente no tiene conciencia de que cometió un delito como el sujeto pasivo de una conducta criminógena atípica se va a enterar de que fue victima de la misma, y peor aún en el supuesto de que el sujeto pasivo estuviera conciente como denunciaría la misma, si los ministerios públicos encargados de integrar las averiguaciones previas no tiene los conocimientos técnicos necesarios para encuadrar estas conductas.

DIFICULTADES TÉCNICAS PARA DETECTARLOS.- Imaginemos a un delincuente invisible que no deja huellas y el cual va obtener beneficios de sus acciones en formas en que el sujeto pasivo difícilmente se va a enterar y si este lo llegase a hacer no tiene forma de conocer la identidad del delincuente, máxime si nuestro país no cuneta todavía con una ciberpolicia encargada de rastrear y perseguir delincuentes informáticos, con que bases se procede a la denuncia, que seguridad en caso de hacerlo se tendría de que se

castigaría al comisor del delito esta es una de las razones que crean una cortina de humo respecto a las estadísticas de comisión de delitos informáticos.

Desprendido de lo anterior es fácil establecer que el ámbito de comisión de los delitos informáticos en nuestro país no tiene una margen geográfico ya que su comisión puede tener lugar en el Distrito Federal y sus consecuencias tendrían consecuencias en cualquier punto del mundo, pero esto requiere necesariamente que se este hablando de delitos relacionados al Internet, refiriéndonos a delincuentes de la súper carretera de la información, pero respecto a los delitos informáticos que no necesariamente requieren ser cometidos en línea y los cuales casi exclusivamente se refieren a copiado ilegal de programas protegidos por los derechos de autor la dificulta a la que nacemos referencia se refleja en el siguiente artículo en el cual la Secretaría de Gobernación anuncio la creación de una nueva Ciberpolicia que para desgracia de nuestro país a la fecha solo ha quedado en un simple anuncio.

-Cd. de México, México.- México cuenta ya con una policía especial para detectar delincuentes cibernéticos en un tiempo no mayor a 15 minutos, publicó un periódico nacional que citó a fuentes de la Secretaría de Gobernación.

"Los recursos son escasos, el personal todavía lo están seleccionado y el equipo técnico no ha quedado totalmente instalado", apuntó el diario.

La nueva corporación dependerá de la PFP (Policía Federal Preventiva) de reciente creación, y se espera que en pocos meses ya este funcionando totalmente.

Esta policía especial, nació ante la ausencia de mecanismos para detectar a "Hackers" que tienen la capacidad de invadir los sistemas informáticos del gobierno, empresas y particulares.

"Sí, se han vulnerado algunos sistemas. Algunas páginas en Internet de dependencias federales y estatales, han entrado y las han dañado. Tenemos indicios de que han tratado de penetrar algunos sistemas financieros", explicó al medio de comunicación un funcionario.

Incluso, reconoce que probablemente los "Hackers" se introdujeron al sistema informático del gobierno y "ni cuenta nos hemos dado".

Entre los delitos que combatirá está policía cibernética, están el evitar el robo de números de tarjetas de crédito, la sustracción de información oficial, la obtención de donativos para grupos terroristas, la creación de empresas fantasma, pornografía, piratería de música y falsificación de documentos."

Ahora bien ya se ha establecido que los delitos informáticos clasificados por su comisión en línea no se ven limitados por ningún ámbito geográfico, pero los que no requieren esta conexión, si tienen un ámbito geográfico, si tomamos en cuenta que estos delitos se reducen en gran parte a reproducción ilícita de material protegido por derecho de autor y a falsificaciones de documentos, tenemos que en México es el Distrito Federal el lugar en el que el 90% o mas de esto ilícitos se comete, lo anterior se afirma dado que el principal punto de reproducción y comercialización ilícita es la zona de "TEPITO" lugar en el que este materia es distribuido inclusive a Centroamérica, obviando por supuesto que es el centro de dotación de todos los comerciantes de esta mercancía del país y por lo que hace a falsificaciones aunque no es el único lugar, la mayor parte de esta actividad también se desarrolla en el Distrito Federal, merced a la actividad económica que aquí se desarrolla y a la concentración de insumos tecnológicos que se encuentra disponible.

4.2. SUJETO ACTIVO Y SUJETO PASIVO EN LA COMISION DE LOS DELITOS INFORMÁTICOS.

SUJETO ACTIVO.

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

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

Es importante señalar 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 estas aseveraciones pueden y deben ser objeto de un estudio más profundo, que dada la naturaleza de nuestro objeto de estudio nos vemos en la necesidad de limitar sin embargos si podemos señalar alguna características de los sujetos activos de los delitos informáticos.

1.- Poseen importantes conocimientos de informática ya sea por el desarrollo de sus carreras y estudios profesionales o por la natural facilidad que los jóvenes tienen para asimilar conocimientos técnicos computacionales como resultado de su constante acercamiento a la tecnología.

2.- Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible (se los ha denominado delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema).

3.- A pesar de las características anteriores debemos tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

4.- Las opiniones en cuanto a la tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional a nivel informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

5.- Estos delitos se han calificado de "cuello blanco", porque el sujeto que comete el delito es una persona de cierto status socioeconómico y no se requiere ningún tipo de violencia física para su comisión.

La "cifra negra" es muy alta. No es fácil descubrirlo ni sancionarlo, en razón del poder económico de quienes lo cometen y también es importante destacar que los daños económicos son altísimos. Se habla de pérdidas anuales por delitos informáticos y otros tecno-crímenes, que van desde los U.S.D. $100 millones (Cámara de Comercio de los Estados Unidos) hasta la suma de U.S.D.$5000 millones, de acuerdo a un estudio de 1990 hecho por una firma auditora.

Pacheco Klein nos dice: "Otro estudio estimó que sólo el 1% de los robos de computadora son detectados, y quizá sólo un 15 % de ellos sean denunciados. Cuando los delitos informáticos son denunciados y llevados a juicio, muchos de ellos son negociados fuera del juzgado; sólo alrededor del 24 % van realmente a juicio, y alrededor de dos tercios de esos juicios resultan en la absolución y el archivo del expediente."

6.- Un punto importante muy importante es que la opinión pública no considera delincuentes a estos sujetos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario el autor de estos delitos distingue entre el daño a las personas (que es inmoral) y el daño a las organizaciones, porque en este último caso sienten que "hacen justicia", se le ha llamado a este punto de vista el síndrome de Robin Hood.

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 son 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, una 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.

Derivado de lo anterior tenemos que el sujeto pasivo de los delitos informáticos, es la persona o entidad sobre el cual recae la conducta que realiza el sujeto activo. La mayoría de los delitos informáticos no son descubiertos, como ya dijimos, pero es importante destacar que se debe en gran parte a que los mismos no son denunciados, las empresas o bancos tienen miedo al desprestigio y a su consecuente pérdida económica, derivada de la duda que se sembraría en sus ahorradores e inversionistas al darse a conocer el hecho de que sus sistemas de informática resultan vulnerables.

4.3. BIEN JURÍDICAMENTE TUTELADO EN LOS DELITOS INFORMÁTICOS.

Respecto a este particular se habrá de establecer que los delitos informáticos atañen a dos bienes tutelados por las leyes penales estos son el derecho a la información y la protección al patrimonio.

Esto se afirma al tomar en cuenta que una gran parte de los delitos informáticos se enfocan a destruir, inutilizar o privar de bienes patrimoniales a los sujetos pasivos, ya que al hacer una transferencia ilegal de fondos estamos claramente ante un ataque al patrimonio, al igual que lo estamos al momento en que un gusano, un virus o una bomba lógica inutilizan las computadoras personales de miles de sujetos pasivos.

Y que se puede decir del delincuente que hace mal uso de una tarjeta de crédito cuyas características interceptó en la red, sin duda afecta directamente al patrimonio del titular de la misma, no obstante que se aclarase el cargo el detrimento al patrimonio seria en contra de la institución bancaria y en segundo término a la aseguradora de la misma y esto se traduciría en una escalada de gastos para la población en general dados los aumentos en seguro, en consecuencia en servicio y en precios.

Pero el derecho a la información tutelado inclusive por nuestra Constitución también se ve afectado por los delitos informáticos, ya que es practica común entre los delincuentes informáticos el romper barreras de seguridad de diversas bases de datos privadas y gubernamentales, para sustraer información que tenga determinado valor personal para el delincuente.

Es debido a esta bifuncionalidad de bienes jurídicamente tutelados que las leyes que se han creado en México hasta el momento no han resultado lo suficientemente eficaces como para prevenir y combatir los delitos informáticos pues los Códigos Penal del estado de Sinaloa y el Penal Federal se han enfocado ha tutelar el derecho a la información por sobre el patrimonio,

además la existencia de estos dos ordenamientos jurídicos puede crear un conflicto de competencias ya que no se ha establecido perfectamente la calificación de este tipo de delitos, y por lo tanto el estado de Sinaloa puede reclamar el juzgar y castigar a un delincuente informático el cual haya tenido como base de operaciones este estado, a pesar de que le efecto del delito haya tenido lugar en cualquier punto de la Republica o incluso del mundo.

Luego entonces tenemos que el bien jurídico tutelado por el derecho informático y en particular por la regulación de los delitos informáticos es la propiedad y la privacidad de las personas, agredida en forma dolosa.

A efecto de acreditar lo anterior nos permitimos transcribir el articulado referente a esto delitos en los ordenamientos legales en comento.

CODIGO PENAL FEDERAL

Libro Segundo

Titulo Noveno Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática

Capitulo I Revelación de Secretos

ARTÍCULO 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

ARTICULO 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado publico o cuando el secreto revelado o publicado sea de carácter industrial.

ARTICULO 211 BIS.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicaran sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Capitulo II Acceso Ilícito a Sistemas y Equipos de Informática

ARTICULO 211 BIS 1.- Al que sin autorización modifique, destruya o provoque perdida 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.

ARTICULO 211 BIS 2.- Al que sin autorización modifique, destruya o provoque perdida 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.

ARTICULO 211 BIS 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida 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.

ARTICULO 211 BIS 4.- Al que sin autorización modifique, destruya o provoque perdida 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.

ARTICULO 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 perdida 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 articulo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

ARTICULO 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 articulo 400 bis de este código.

ARTICULO 211 BIS 7.- Las penas previstas en este capitulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

CODIGO PENAL DEL ESTADO DE SINALOA

CAPITULO V.

DELITO INFORMATICO

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

I. Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o

Ii. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

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

4.4. PROPUESTA PARA LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN LOS CÓDIGOS PENALES DEL DISTRITO FEDERAL Y DEL ESTADO DE MÉXICO.

Como objetivo fundamental de este estudio y después de analizar diversas propuestas y exposiciones de motivos que en legislaciones de otros países e inclusive en el nuestro se han elevado, es menester establecer los lineamientos que en nuestro muy particular punto de vista se deberán de seguir para la inclusión de un nuevo capítulo en los Códigos Penales del Distrito Federal y del Estado de México, por lo que antes de formular el proyecto debemos de tomar en cuenta los siguientes lineamientos:

1.- Los delitos informáticos deberán de considerarse particularmente agravados, cuando la destrucción, intromisión o acción delictiva se

cometa contra datos pertenecientes a organismos de defensa nacional, seguridad interior o Inteligencia, lo anterior dado los conflictos internacionales que podrían causarse con estos eventos.

2.- El simple hecho de que se accese a una computadora o sistema de computación, o almacenamiento de datos y los mismos no le pertenezcan directamente al intruso, ya sea mediante presencia física o a través de otra computadora, sin autorización del propietario o de un tercero facultado para otorgarla o si estando autorizado, excediere los límites de la misma. Baste para que se configure el tipo penal.

3.- Al establecer lineamientos para la regulación de estos delitos se deberá tomar en cuenta la posibilidad de actuaciones conjuntas con órganos policíacos y legislativos de otros países dadas las características transfronterizas de las conductas.

4.- Se deberá buscar una redacción genérica y previsora que cuente con la facilidad de adaptarse a conductas atípicas o no previstas inclusive al momento de la promulgación, ya que a manera de ejemplo si tomamos en cuenta que a la fecha no hay legislación particularizada en materia civil respecto a la firma electrónica y si el día de hoy se establecen los delitos encuadrables como informáticos, que pasaría el día en que se legalizan las firmas electrónicas y las mismas se comiencen a falsificar, tomando en cuenta que no hay posibilidad de practicar periciales grafoscopicas, grafometricas, grafológicas que pudieran determinar la falsificación

Por lo anterior y basándonos en los lineamientos establecidos proponemos el siguiente modelo de Titulo incluíble en los Códigos Penales para el Distrito Federal y el Estado de México.

TITULO_____ DELITOS INFORMATICOS

ART.1.- Se impondrá la pena de uno a cinco años de prisión al que indebidamente y sin autorización de su destinatario, propietario o autor, **abra, accese o tome parte en una comunicación electrónica, escrita u oral que se este llevando a cabo en tiempo real o que este a disposición de su destinatario, valiéndose de medios electrónicos, computacionales, satelitales, electromagnéticos u ópticos.**

ART. 2.- Se impondrá la pena de uno a cinco años de prisión al que indebidamente y sin autorización irrumpa, use, modifique, inutilice, altere, destruya o provoque perdida de información, almacenada en sistemas o equipos de informática y computación fijos o portátiles, soportes informáticos o bases de datos públicas o privadas.

ART. 3.- La pena prevista en el artículo anterior aumentara de uno a tres años para el evento de que la persona que incurra en la conducta

prevista sea el encargado o responsable de los sistemas, redes o equipos de informática y computación fijos o portátiles, soportes informáticos o bases de datos públicas o privadas o de sus ficheros, programas, códigos, claves de acceso, comandos, electrónicos o telemáticos, archivos o registros, y que preste sus servicios para el afectado o bien sea funcionario o empleado publico

ART. 4.- .- Se impondrá la pena de uno a cinco años de prisión al que indebidamente, sin autorización y valiéndose de, equipos de informática y computación, programas, códigos, claves de acceso, comandos, electrónicos o telemáticos, archivos o registros, irrumpa o accese en sistemas, redes o equipos de informática y computación fijos o portátiles.

ART. 5.- Se equiparara al delito de fraude y se castigara en los mismo términos que al delito citado al que **al que actuando en calidad de usuario sea persona física o moral, intermediario, prestador de servicios, banco, empresa proveedora de información o comercializadora y mediante sus habilidades técnicas o maquinaciones utilice el intercambio electrónico de datos para obtener con engaños ganancias indebidas, dinero, valores, bienes o servicios, adquiriendo, enajenando, transfiriendo, depositando, o dando en garantía productos y servicios de cualquier índole.**

Como redacción alternativa proponemos la utilizada por el Código Penal Español que establece lo siguiente en su artículo tercero:

Artículo 3º. Fraude informático. El que con intención de procurarse a sí mismo o a un tercero un beneficio patrimonial indebido, causare un perjuicio en el patrimonio de otro, operando un proceso de datos incorrecto, configurando incorrectamente un programa de software, empleando adrede datos falsos, incorrectos o incompletos, o a través de cualquier otra intervención o manipulación ilegítima, sin la debida autorización o excediendo la misma, será castigado con pena de dos a seis años de penitenciaría.

ART. 6.- Se impondrá la pena de uno a cinco años de prisión al que difunda en redes de informática y telecomunicaciones servicios que contengan material apto únicamente para mayores de edad, o que puedan afectar la integridad de la familia, o herir la sensibilidad de algún sector de la población, siempre que no se especifique claramente en su página de entrada advertencias respecto al material a difusión y las restricciones para los menores de edad.

ART. 6 bis.- Así como al que difunda por los mismos medios material prohibido por leyes especiales, y tratados internacionales, en los que se utilicen menores de edad o incapaces.

ART. 7.- Se impondrá la pena de uno a cinco años de prisión al que con o sin animo de lucro cree, invente, produzca y difunda programas computacionales, comandos, claves, archivos ejecutables, o cualquier sistema informático, tendiente a la inutilización, modificación o destrucción de sistemas,

redes o equipos de informática y computación fijos o portátiles, soportes informáticos o bases de datos públicas o privadas, o de sus ficheros, programas, códigos, claves de acceso, comandos, electrónicos o telemáticos, archivos o registros.

Se tendrá que tomar en cuenta que para casos que resulten particularmente graves, la aplicación del Código Penal Federal, que aunque limitadamente contempla los delitos informáticos seria conducente y aun mas será necesario el establecer la posibilidad de la intervención de los Tribunales Internacionales en los casos en que los delitos cometidos tengan naturaleza transfronteriza.

Esto es de vital importancia ya que a nivel mundial los delincuentes informáticos (HACKERS) constituyen una gran comunidad con grandes lazos entre si e inclusive tienen códigos de ética tan complicados como los de cualquier otra mafia en el mundo, de hecho en la red es relativamente fácil encontrar documentos, los cuales dan lineamientos básicos a este tipo de delincuentes para poder sortear los inconvenientes de una posible detención, la posible declaración que se deberá hacer ante la autoridad respectiva y las conductas que las fuerzas de orden podrán seguir en esta detención

4.5. GLOSARIO DE TERMINOS INFORMÁTICOS

A medida que la investigación realizada para integrar el presente estudio fue avanzando, descubrimos que el común de los abogados e inclusive de cualquier tipo de profesionistas que no tengan como campo de trabajo la informática, tienen conocimientos muy limitados respecto a esta, y en su gran mayoría se limitan a utilizar los comandos básicos de diversos procesadores de texto, por lo que creímos necesario incluir esta recopilación de términos y definiciones, a fin de hacer más fáciles de comprender a cualquier persona que consulte esta obra, los términos en ella utilizados o los que se va a encontrar en sus acercamientos a la informática.

:-) Este extraño símbolo es una forma en que una persona puede mostrar su estado de ánimo en un medio "frío" como es el ordenador. Representa un "rostro sonriente" y es una forma de "metacomunicación" de las centenares que existen y que van de lo obvio a lo críptico. Este símbolo expresa en concreto "felicidad", pero también "broma" o "sarcasmo".

Ack.- Ver "acknowledgement".

Acnowledgement (ACK).- Acuse de recibo. Un tipo de mensaje que se envía para indicar que un bloque de datos ha llegado a su destino sin errores.

Address (dirección).- Existen tres tipos de dirección de uso común dentro de Internet: "Dirección de correo electrónico" (email address); "IP" (dirección internet);

y "dirección hardware" o "dirección MAC" (hardware or MAC address). Ver también: "email address", "IP address", "internet address".

Advanced Research Projects Agency Network (ARPANET).- Red pionera de larga distancia financiada por ARPA (hoy DARPA). Fue la base inicial de la investigación sobre redes y constituyó el eje central de éstas durante el desarrollo de Internet. ARPANET estaba constituida por ordenadores de conmutación individual de paquetes interconectados mediante líneas telefónicas.

Agent (agente).- En el modelo cliente-servidor, la parte del sistema que realiza la preparación e intercambio de información por cuenta de una aplicación del cliente o del servidor.

Algoritmo.- Conjunto final de reglas determinadas tendientes a resolver un problema a medida de un número especifico de operaciones. Ejemplo: especificación completa de una serie de operaciones aritméticas que permitan el cálculo de valores del seno con una precisión dada.

Alias.- Nombre usualmente corto y fácil de recordar que se utiliza en lugar de otro nombre largo y difícil de recordar.

Anonymous FTP (FTP anónimo).- El FTP anónimo permite a un usuario la captura de documentos, ficheros, programas y otros datos contenidos en archivos existentes en cualquier lugar de Internet sin tener que proporcionar su nombre de usuario y una contraseña ("password").

Utilizando el nombre especial de usuario "anonymous", el usuario de la red superará los controles locales de seguridad y podrá acceder a ficheros accesibles al público situados en un sistema remoto. Ver también: "archive site", "File Transfer Protocol".

Application Program Interface (API).- Conjunto de convenciones de programación que definen cómo se invoca un servicio desde un programa.

Archie.- Sistema para recoger, indexar y servir información dentro de Internet. Las versiones iniciales de "archie" proporcionaban un directorio indexado de nombres de ficheros de todos los archivos de "Anonymous FTP" de Internet.

Las versiones posteriores permiten otros tipos de obtención de información. Ver también: "archive site", "Gopher", "Wide Area Information Servers".

Archive site.- Ordenador que permite el acceso a una colección de ficheros a través de Internet. Un "anonymous FTP archive site", por ejemplo, permite el acceso a dicho material mediante el protocolo FTP. Ver también: "anonymous FTP", "archie", "Gopher", "Wide Area Information Servers".

Attach.- Adjuntar un archivo, enlazar con un servidor.

B

Banco de datos.- Conjunto de datos relativos a un área determinada de conocimientos y organizado para ser ofrecido para consultas de usuarios.

Base de datos.- Conjunto de datos, organizado en vía de su utilización por programas correspondientes a aplicaciones distintas, a efectos de facilitar la evolución independiente de datos y programas.

Backbone (eje central) Nivel más alto en una red jerárquica. Se garantiza que las redes aisladas y de tránsito conectadas al mismo eje central están interconectadas.

Bitnet.- Red de ordenadores de centros docentes y de investigación que ofrece servicios interactivos de correo electrónico y de transferencia de ficheros utilizando un protocolo de almacenaje y envío basado en los protocolos de IBM Network Job Entry. Bitnet-II encapsula el protocolo Bitnet en paquetes IP y depende de Internet para enviarlos a su destino.

Browser.- Navegador.

Bug.- Error de programación.

Bulletin Board System (BBS) (Tablón de Anuncios Electrónico) Ordenador y programas que habitualmente suministran servicios de mensajería electrónica, archivos de ficheros y cualquier otro servicio y actividad que interesan al operador del BBS.

Aunque hasta hace poco los BBSs solían estar en manos de aficionados, existe un número cada vez mayor de BBSs conectados directamente a Internet y muchos BBSs son operados actualmente por las Administraciones Públicas, por centros docentes y de investigación y por empresas: Ver también: "Electronic Mail", "Internet", "Usenet".

Burotica u Ofimática.- Conjunto de técnicas y de medios tendiente a automatizar las actividades de oficina y principalmente, el tratamiento y la comunicación de la palabra, de lo escrito y de la imagen.

C

Campus Wide Information System (CWIS) (Sistema de Información Universitario).- Un CWIS ofrece información y servicios públicos en un centro universitario mediante quioscos informatizados y permite operaciones interactivas mediante quioscos, sistemas informáticos interactivos y redes universitarias.

Habitualmente estos servicios comprenden directorios, calendarios, BBS, bases de datos.

Client (cliente).- Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una estación de trabajo que solicita el contenido de un fichero a un servidor de ficheros es un cliente de este servidor. Ver también: "client-server model", "server".

Client-server model (modelo cliente-servidor).- Forma común de describir el paradigma de muchos protocolos de red. Ver también: "client", "server".

Computadora.- Equipo informático de tratamiento automático de datos que contiene los órganos (o elementos) necesarios para su funcionamiento autónomo.

Congestion (congestión).- Se produce una congestión cuando la carga existente sobrepasa la capacidad de una ruta de comunicación de datos.

Cracker (intruso).- Un "Cracker" es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los "Hackers", y suelen disponer de muchos medios para introducirse en un sistema.

Los Crackers tienden a reunirse en pequeños grupos cerrados muy secretos que no se relacionan con la enorme y abierta policultura que define a los Hackers; la mayoría delos verdaderos Hackers los consideran como una forma de vida separada y mas baja.

Cyberspace (Ciberespacio).- Término creado por William Gibson en su novela fantástica "Neuromancer" para describir el "mundo" de los ordenadores y la sociedad creada en torno a ellos.

D

Dark – side hacker .- Hacker malicioso o criminal. Referencia a Darth Vader "seducido por la fuerza del lado oscuro.

Data Highway (autopista de datos).- La autopista de datos es una malla continua de redes de comunicaciones, bases de datos y productos de electrónica de consumo capaz de poner ingentes cantidades de información al alcance de los usuarios. Ver también: "NII" y "GII".

Datos.- Representación de una información bajo una forma convencional destinada a facilitar su tratamiento, Según la ley canadiense de 1985 sobre delitos informáticos, "dato" señala la representación de informaciones o de conceptos que son preparados o lo han sido de manera que puedan ser utilizados en una computadora.

Distributed database (base de datos distribuida).- Conjunto de depósitos de datos que ante el usuario aparece como una base de datos única. Un ejemplo esencial en Internet es el "Domain Name System".

Domain Name System (DNS) (Sistema de Nombres de Dominio).- El DNS un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de estos.

El estilo de los nombres de "hosts" utilizado actualmente en Internet es llamado "nombre de dominio".

DSL (digital subscriber line o "línea digital por subscripción").- A medida que en los países industrializados se instalan líneas telefónicas que permiten conexión de alta velocidad a Internet, oirá usted cada vez más hablar de DSL. Escuchará también el término XDSL, que designa cualquier variante de la norma DSL, como asimismo ADSL, que quiere decir "línea digital asimétrica por suscripción".

Una conexión DSL a Internet tiene una amplitud de banda considerablemente mayor que la de una conexión con un módem análogo.

E

E-mail.- Sistema mediante el cual un ordenador puede intercambiar mensajes con otros usuarios de ordenadores (o grupos de usuarios) mediante redes de comunicación. El correo electrónico es uno de los usos más populares de Internet.

Electronic Frontier Foundation (EFF) (Fundación de la Frontera Electrónica) Fundación norteamericana creada para tratar todos los temas sociales y legales derivados del impacto social del uso cada vez más extendido de los ordenadores como medio de comunicación y de distribución de la información.

F

FAQ (Frequently Asked Question) Abreviatura de "Preguntas más frecuentes".

File transfer (transferencia de ficheros).- Copia de un fichero desde un ordenador a otro a través de una red de ordenadores. Ver también: "File Transfer Protocol".

File Transfer Protocol (FTP) (Protocolo de Transferencia de Ficheros).- Protocolo que permite a un usuario de un sistema acceder, y transferir a y desde, otro sistema de una red. FTP es también habitualmente el nombre del programa que el usuario invoca para ejecutar el protocolo. Ver también: "anonymous FTP".

Flame (desahogo).- Opinión sincera y/o crítica sobre algo o alguien, expresada de forma franca y apasionada en un mensaje de correo electrónico. Suele ir precedida de un aviso (FLAME ON).

Surgen guerras de desahogo (Flame Wars) cuando alguien empieza a desahogarse con otro por haberse desahogado sin razón. Ver también: "Electronic Mail".

G

Gateway.- Hoy se utiliza el término "router" (direccionador) en lugar de la definición original de "gateway". Es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero operativas diferentes. Ver también: "mail gateway", "router."

GB (gigabyte).- Un gigabyte es una medida de la capacidad de la memoria de una computadora. Un gigabyte equivale a mil millones de bytes o un millón de kilobytes. La capacidad del disco duro - el dispositivo donde usted guarda programas, cartas y documentos en su computadora - se mide hoy en gigabytes. Los mayores se aproximan actualmente a los 100 GB de capacidad.

GHz (gigahertz).- Es la abreviatura que marca hoy en día el ritmo del progreso, gracias a los "chips" electrónicos fabricados por el gigante Intel o su competidor Advanced Micro Devices (AMD

Un Gigahertz quiere decir básicamente "mil millones de ciclos por segundo" y es utilizado para expresar la velocidad a la cual una señal electrónica circula por un microprocesador. Tanto Intel como AMD tienen microprocesadores de 1 GHz. Y esto es rápido. Un chip de 1 GHz puede procesar mil millones de instrucciones por segundo.

Global Information Infrastructure (Infraestructura Global de Información).- Es el nombre que se le ha dado a la autopista de datos que cubrirá todo el planeta.

Gopher (Gopher).- Un servicio de distribución de información que ofrece colecciones jerarquizadas de información en Internet.

Gopher utiliza un protocolo simple que permite a un cliente Gopher acceder a información desde cualquier servidor Gopher que esté accesible, proporcionándole un único "espacio Gopher" (Gopher space) de información.

Están disponibles también versiones de dominio público para cliente y servidor. Ver también: "archie", "archive site", "Wide Area Information Servers".

H

Hacker.- Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores.

Este término se suele utilizar indebidamente como peyorativo, cuando en este último sentido sería más correcto utilizar el término "cracker".

Host (sistema central).- Ordenador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP.

Host address.- Ver: "internet address"

Host number (número de sistema central).- Ver: "host address"
Hostname (nombre de sistema central).- Nombre dado a una máquina. Ver también: "Fully Qualified Domain Name".

I

Información.- Elemento de conocimiento susceptible de ser representado con ayuda de convenciones para ser conservado, tratado o comunicado. Para el Ministerios Francés de Economía y Finanzas la información es así considerada como el contenido semántico de un dato. Toda vez que el término es comúnmente empleado en lugar de dato, por ejemplo en la expresión "soporte de información"

Informática.- Ciencia del tratamiento Racional, particularmente por máquinas automáticas, de la información considerada como el soporte de conocimientos humanos y de comunicaciones en los aspectos técnicos específicamente aplicables al tratamiento de datos efectuado por medios automáticos.

Internet (internet).- Si bien "internet" es una red, el término "internet" se usa habitualmente para referirse a un conjunto de redes interconectadas mediante direccionadores (routers). Ver también: "Internet", "network".

Internet address (dirección internet).- Dirección IP que identifica de forma inequívoca un nodo en una red internet. Una dirección Internet (con "I" mayúscula) identifica de forma inequívoca un nodo en Internet. Ver también: "internet", "Internet", "IP address".

Internet Relay Chat (IRC) (Charla Interactiva Internet).- Protocolo mundial para conversaciones simultáneas ("party line") que permite comunicarse por escrito entre sí a través de ordenador a varias personas en tiempo real.

El servicio IRC está estructurado mediante una red de servidores, cada uno de los cuales acepta conexiones de programas cliente, uno por cada usuario.

Interoperability (interoperabilidad).- Capacidad de comunicación entre diferentes programas y máquinas de diferentes fabricantes.

J

Java.- Lenguaje desarrollado por Sun para la elaboración de aplicaciones

exportables a la red y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores.

Javascript.- Programa escrito en el lenguaje Java incluido dentro de una página HTML, que es interpretado por la aplicación cliente, normalmente un navegador Web (Browser). Ver también: "WWW", "browser", "HTML", "Java".

Joint Photograph Expert Group (JPEG) (Unión de Grupos de Expertos Fotográficos).- Ademas, formato gráfico con compresión con perdidas que consigue elevados ratios de compresión creado por este grupo.

JPEG Ver: "Joint Photograph Expert Group".

L

LAN.- Ver: Local Area Network

Lenguaje de programación.- Conjunto definido de caracteres y reglas de gramática asociada, fijadas de manera formal ue permiten expresar sin ambigüedad los programas.

Local Area Network (LAN) (Red de Area Local).- Red de datos para dar servicio a un área geográfica máxima de unos pocos kilómetros cuadrados, por lo cual pueden mejorar los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 millones de bits por segundo).

M

Mail gateway.- Máquina que conecta entre sí a dos o más sistemas (incluso diferentes) de correo electrónico y transfiere mensajes entre ellos. A veces, la transformación y traducción pueden ser muy complejas.

Microprocesador.- Procesador miniaturizado donde todos sus elementos están conjuntados en un solo circuito integrado.

MP3.- se ha convertido en sinónimo de música digital, y por buenas razones. En el nombre de un archivo, MP3 es la extensión o sufijo (la parte después del punto en un nombre como micanción.mp3) usado el MPEG nivel 3, una norma de codificación de sonido que se hace cada vez más popular.

Multimedia (multimedia) Material digital que combina texto, gráficos, imagen fija y en movimiento, así como sonido.

N

Network (red).- Una red de ordenadores es un sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

Network Information Center (NIC).- (Centro de Información de la Red).- Una NIC ofrece información, asistencia y servicios a los usuarios de la red.

P

Packet (paquete).- La unidad de datos que se envía a través de una red.

Packet Internet Groper (PING) (Búsqueda de Direcciones de Internet).- Programa que se utiliza para comprobar si un destino está disponible. El término se utiliza también coloquialmente: "Haz un "ping" al "host" X a ver si funciona".

Packet switching (conmutación de paquetes) Paradigma de comunicaciones mediante el cual los paquetes (mensajes) son dirigidos entre sistemas centrales, sin que exista una ruta ("path") previamente definida.

Protocol (protocolo).- Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes.

Q

Queue (cola) Conjunto de paquetes en espera de ser procesados.

R

Router (direccionador) Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento. Ver también: "gateway".

S

Signature (firma).- Mensaje de tres o cuatro líneas situado al final de un mensaje de correo electrónico o de un artículo de Usenet que identifica al emisor. Las firmas con más de cinco líneas suelen estar muy mal vistas.

Simple Mail Transfer Protocol (SMTP).- Protocolo definido en STD 10, RFC 821, que se usa para transferir correo electrónico entre ordenadores.

Es un protocolo de servidor a servidor, de tal manera que para acceder a los mensajes es preciso utilizar otros protocolos.

Sneaker.- Una persona contratada para romper la seguridad de un sistema, como un método para probarla.

T

Telnet.- Telnet es el protocolo estándar de Internet para realizar un servicio de conexión desde un terminal remoto. Tiene opciones adicionales.

Token ring (Red en anillo).- una red en anillo es un tipo de lan con nodos cableados en anillo. Cada nodo pasa constantemente un mensaje de control ("token") al siguiente, de tal forma que cualquier nodo que tiene un "token" puede enviar un mensaje. Ver también: "local area network".

U

UNIX-to-UNIX copy (UUCP) (Copia de unix a unix) inicialmente se trataba de un programa que se procesaba en el sistema operativo unix y que permitía a un sistema unix enviar ficheros a otro sistema unix a través de línea telefónica.

Hoy el término se utiliza sobre todo para describir la amplia red internacional que utiliza el protocolo uucp para enviar noticias y correo electrónico.

URL (uniform resource locator).- Aunque no es nueva en el mercado consumidor, esta abreviatura se presta a veces para confusiones. URL es el término oficial de la dirección de un recurso (archivo o página Web) en Internet.

V

Video-on-demand (Televisión a la carta).- Servicio asíncrono de televisión que provee al usuario el acceso a material de vídeo almacenado de forma digital en servidores remotos.

Virus.- programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan.

W

W3.- Ver: "World Wide Web"

WAIS.- Ver: "Wide Area Information Servers"

Warez dood.- Individuo dedicado a obtener software comercial, eliminar las protecciones anticopia y distribuirlos de manera gratuita en la red.

White pages (páginas blancas).- Internet mantiene diversas bases de datos que contienen información sobre usuarios tal como direcciones electrónicas, números de teléfono y direcciones postales.

Estas bases de datos pueden ser examinadas a fin de obtener información sobre determinadas personas. Su nombre viene de que su finalidad es similar al de las guías telefónicas. Ver también: "WHOIS".

Wide Area Information Servers (WAIS) (Servidores de Información de Area Amplia).- Servicio de información distribuida que permite hacer preguntas en lenguaje simple, la búsqueda indexada para obtener información con rapidez y un

mecanismo de "retroalimentación de relevancia" que permite que los resultados de una búsqueda inicial repercutan en búsquedas subsiguientes. Ver también: "archie", "Gopher".

World Wide Web (WWW or W3).- Sistema de información distribuido, con mecanismos de hipertexto creado por investigadores del CERN en Suiza. Los usuarios pueden crear, editar y visualizar documentos de hipertexto. Sus cliente y servidores puede accederse fácilmente.

Worm (gusano).- Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos están especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en "ACM Communications" (Marzo 1982).

El gusano de Internet de Noviembre de 1988 es quizás el más famoso y se propagó por sí solo a más de 6.000 sistemas a lo largo de Internet.

Y

Yellow Pages (YP) (Páginas amarillas).- Servicio utilizado por administradores UNIX a fin de gestionar bases de datos distribuidas en una red.

Z

ZIP.- Formato de fichero comprimido. .

CONCLUSIONES

A manera de conclusiones de nuestro estudio tenemos lo siguiente:

1.- Los delitos informáticos son acciones en que el sistema informático es el objeto del delito, y serian solucionables por un esquema de figura que se implantara en nuestro código penal vigente.

2.- La realidad demuestra que las conductas ilícitas provenientes de esta nueva criminalidad, pueden quedar impunes en algunos casos, o ser muy difíciles de calificar en otros, a falta de previsiones legales vigentes

3.- Deben determinarse conductas prohibidas en forma clara y precisa, estableciéndose las sanciones aplicables al caso concreto.

4.- La tipicidad y la prohibición de la analogía en materia penal, imponen la necesidad de establecer una tipología especial delictiva, que enmarque todas las posibles actividades de los delincuentes informáticos

5.- Debe evitarse el encuadrar estas nuevas conductas delictivas en las figuras penales típicas tradicionales.

6.- Es de vital importancia cubrir el vacío legal existente referente a los delitos informáticos.

7.- En el momento de promulgación y entrada en vigor de un nuevo capitulo que regulara los delitos informáticos, este hecho deberá ser anunciado de manera extensa a la población concientizandola respecto a los particulares del mismo.

8.- Existe una notable ausencia de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.

9.- Es necesario abatir la falta de especialización de las policías, Ministerios Públicos y funcionarios judiciales en el campo de los delitos informáticos.

10.- El derecho informático deberá ser instituido como materia obligatoria en todas las escuelas de derecho de las universidades públicas y privadas del país.

11.- La forma de persecución de los .Delitos Informáticos deberá ser por querella.

BIBLIOGRAFIA

LIBROS

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

PORTE PETIT CANDAUDAP, Celestino. APUNTAMIENTOS DE LA PARTE GENERAL DE DERECHO PENAL Ed. Porrúa S.A. México. 1993

AMUCHATEGUI REQUENA Irma G. DERECHO PENAL Ed. Harla S.A. de C.V. México 1993.

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

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

TELLEZ Valdes, Julio. Derecho Informático. 2ª. Ed. México. Ed. Mc Graw Hill 1996. Pp.103-104.

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

CONSENTINO, Guillermo et Al :"Tras los pasos de la Seguridad Perdida :Delitos Informáticos". En Revista Iberoamericana de Derecho Informático Nº 25. Mérida, España. UNED. 1998.

DAVARA, Miguel Angel : "Derecho Informático". Editorial Aranzandi España, 1993.

TIEDEMAN, Klaus : "Criminalidad mediante Computadoras". En Poder Económico y Delito. Editorial Ariel S.A. Barcelona 1985.

TELLEZ VALDES, Julio : "Derecho Informático". Segunda Edición. Editorial McGraw-Hill. México 1997.

NUÑEZ PONCE, Julio César : "Software : Licencia de Uso, Derecho y Empresa". Fondo de desarrollo Editorial de la Universidad de Lima. Lima, 1998.

LEDESMA, Julio C.:"Derecho Penal Intelectual" Ed. Universidad. Buenos Aires, Argentina. 1992. Págs. 194

RIOS ESTAVILLO Juan José "Derecho e Informática en México" Instituto de Investigaciones Jurídicas de la UNAM México 1997

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

HEMEROGRAFIA

"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 reformas a la Ley sobre Derechos de Autor y el Código Penal", El Universal, México, martes 29 de abril de 1997.

LINKS Y PAGINAS WEB CONSULTADAS

http://fundesco.es/seminarios/actasloslgv.html

http://www.mundolatino.org/i/derecho/delitos.htm

http://www.jurisweb.com/buscador/index.htm

http://info.juridicas.unam.mx/

http://guia.hispavista.com/Ciencias_Sociales/Derecho/Internacional/

http://www.derechoinformatico.com/

http://www.lawinfo.com/index.html

http://www.reforma.com.mx

http://www.monografias.com

http://www.noticias.com

INDICE