155

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGÓN

REFORMAS AL CÓDIGO PÈNAL PARA EL DISTRITO FEDERAL, PARA LEGISLAR Y CREAR EN DICHO ORDENAMIENTO EL TITULO VIGÉSIMO SÉPTIMO DENOMINADO "DELITOS INFORMÁTICOS"

T E S I S

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN DERECHO

P R E S E N T A :

CARLOS GARDUÑO DOMÍNGUEZ

ASESOR:
LIC. JUAN JESÚS JUÁREZ ROJAS

México 2001

D E D I C A T O R I A

INTRODUCCIÓN

CAPÍTULO I
GENERALIDADES DE LOS DELITOS INFORMÁTICOS

CAPÍTULO II
TIPOS DE DELITOS INFORMÁTICOS

CAPÍTULO III
ANALISIS COMPARADO EN MATERIA DE DELITOS INFORMÁTICOS

CAPÍTULO IV
LA TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL PARA EL DISTRITO FEDERAL.

INTRODUCCIÓN

En los inicios del siglo XXI, el uso de los ordenadores, computadoras personales, interconexiones a redes y sistemas telemáticos se incrementan día a día de manera considerable ya sea en la esfera personal, industrial, gubernamental y de mercado, otorgando a la humanidad grandes beneficios.

Este desarrollo en las tecnologías informáticas se caracteriza, sin duda por su considerable dinamismo, sin embargo, no es inmune a las conductas delictivas y antisociales que se manifiestan de forma inimaginable. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de cometer delitos de tipo tradicional, en formas no tradicionales.

Este trabajo pretende estudiar las conductas dolosas que pueden presentarse con el uso de las computadoras, lo que nos conducirá a destacar la imprescindible intervención de la ciencia jurídica para castigar este tipo de conductas, las cuales dañan directamente el patrimonio de las personas y el derecho a la intimidad, por mencionar a algunos.

Dichas conductas pueden ser comprendidas dentro del tipo penal del delito produciéndose una informatización de un ilícito tradicional. A estos delitos les llamaremos delitos informáticos.

Por lo tanto son varias las cuestiones a resolver por la doctrina, como concepto, tipología y clasificación de los delitos informáticos, el bien jurídico que se protege, los sujetos involucrados, el perfil criminológico, la internacionalización de las conductas típicas, por mencionar algunas.

Resulta necesario entonces, arribar a una definición de informática para en una etapa posterior, continuar en el camino que nos llevará a una acabada noción de informática jurídica, derecho informático y, como consecuencia, a los delitos informáticos.

Asimismo nos referiremos a la categoría de delitos informáticos reconocidos por las Naciones Unidas y que han sido aceptados por la mayoría de la doctrina especializada.

Se analizará en el desarrollo de este trabajo la legislación que regula penalmente las conductas ilícitas relacionadas con la informática, pero, que aún no contemplan en si los delitos informáticos. En este entendido, considero pertinente recurrir al Código Penal del Estado de Sinaloa, ante la importancia que tiene el

Congreso Local de dicho Estado de haber legislado sobre la materia de delitos informáticos.

Posteriormente, señalaré los países que disponen de una legislación adecuada para enfrentarse con este problema en particular, estableciendo las medidas adoptadas en las legislaciones penales para sancionar y prevenir los delitos informáticos.

En este orden de ideas, el autor habrá de conducir su trabajo hasta la propuesta para prevenir y sancionar este tipo de conductas, sugiriendo la inclusión de un título especial en el Código Penal para el Distrito Federal denominada " Delitos Informáticos".

Lo anterior con el propósito de evitar que la ausencia de figuras concretas que se pudieran aplicar en esta materia, permitiera que ciertos hechos quedaran impunes ante la ley, o bien obligaría a los tribunales a aplicar preceptos que no se ajustan a la naturaleza de los mismos.

CAPÍTULO I

GENERALIDADES DE LOS DELITOS INFORMÁTICOS

1.1. ANTECEDENTES

LA REVOLUCIÓN TECNOLÓGICA Y LA INFORMACIÓN.

La era de las comunicaciones, la materialización de la idea del mundo como una aldea global, el cyberespacio, las cyberculturas, y el impacto de las tecnologías de la información han implicado una transformación en la forma de convivir en sociedad.

Dentro de este marco de transformación, el cambio producido por el mal uso de la informática ha hecho que surjan nuevas conductas merecedoras del reproche social que, sin embargo, no siempre son fáciles de tipificar. Así, han surgido modalidades delictivas relacionadas con la informática.

En primer lugar, ciertas figuras típicas convencionales han comenzado a realizarse mediante el empleo de las Tecnologías de la Información, es decir, ha comenzado a ser utilizada la informática como un medio de comisión específico.

Dichas conductas pueden ser comprendidas dentro del tipo penal del delito, produciéndose una informatización de un ilícito tradicional. A estos delitos les llamaremos delitos computacionales, informáticos, electrónicos, etc.

Pero además han surgido nuevas conductas, impensadas por el legislador de hasta hace medio siglo, que por su especial naturaleza no admiten encuadrase dentro de figuras convencionales informatizadas sino que es necesario que se creen nuevos tipos. Son estos nuevos delitos a los que llamaremos con propiedad: "Delitos Informáticos".

Ahora bien, si deseamos seguir la tendencia del derecho comparado a evitar una "inflación penal", es decir, un crecimiento desmedido del Derecho Penal que vaya contra la tendencia hacia la reducción de la esfera punitiva, debe entenderse que no toda conducta impropia relacionada con la informática merece el carácter de delito informático.

Primero, sólo serán delitos los que se tipifiquen como tales en virtud del principio de legalidad.

Segundo, es conveniente que sólo las conductas más graves y preferentemente dolosas, se castiguen penalmente, dado el carácter de " última ratio", de último recurso de la pena dentro del sistema de control social, es decir, que solo una vez que las medidas sancionadoras civiles y administrativas han sido descartadas, las sanciones serán las penales.

Por lo tanto, son varias las cuestiones a resolver por la doctrina, como: concepto, tipología y clasificación de los delitos informáticos, el bien jurídico que se protege, los sujetos involucrados, el perfil criminológico, la internacionalización de las conductas típicas, por mencionar algunas.

El vertiginoso avance de la tecnología, modifica día a día, y a un ritmo cada vez más acelerado, la sociedad en que vivimos.

Las conductas del hombre han variado sustancialmente como consecuencia de los cambios científicos y tecnológicos, motivo por el cual la forma en que trabajamos*, nos comunicamos, nos relacionamos con otros individuos y nos desenvolvemos en la vida de relación, varían de tal manera en que los hacíamos algunos años atrás.

Palabras como computadora, fax, módem, software, Internet, hardware, correo electrónico, por solo mencionar algunas, han pasado a configurar parte de nuestro vocabulario diario.

---

*Un ejemplo de esto lo constituye el teletrabajo o trabajo a distancia, en el cual la persona trabaja desde su casa para una empresa. Se asegura que se trata de una tendencia consolidada, como producto de la cual, en los próximos años será cada vez mayor la cantidad de gente que trabajará desde sus hogares, lo que permitirá, entre otras cosas, un importante ahorro de tiempo y viajes. "Trabajar desde la casa", por Viviana Romero, en Magazine Semanal, año 3 No. 150, págs. 6 a 9.

Nos encontramos con ejemplos cotidianos de alguna determinada tecnología que si bien podría haber constituido un capítulo en un libro de ciencia-ficción en la época de nuestros padres, hoy está al alcance de nuestras manos.

Prueba de ello lo constituye el extraordinario avance con relación a la energía nuclear y solar, la informática, la robótica, la telemática, la biotecnología y la ingeniería genética.

Es por ello que hoy parece difícil imaginar donde está situado el límite entre lo posible y lo utópico o irrealizable, pues se va perdiendo lentamente la capacidad de asombro ante lo novedoso. El multimillonario empresario de la industria del software, Bill Gates, ha manifestado: "No creo que haya nada exclusivo en la inteligencia humana. Todas las neuronas del cerebro operan en forma binaria y creo que podremos reproducirlas en una maquina"[*]. También resultan impactantes sus proyecciones acerca del fenómeno informático.[*]

---

[*] Revista Noticias Número 1048, 25 de enero de 1997, pág. 75; Buenos Aires, Argentina.

[*] "La computadora se convertirá en una increíble herramienta para todo público. Esa visión dista de haberse concretado. Una PC no escucha lo que usted dice, no puede hablarle, no aprende. Quiero decir que todavía es algo bastante limitado. Consagraré mi vida al futuro y están en camino novedades apasionantes y la ley de Moore sostiene que, básicamente las computadoras duplican su eficiencia cada dos años. Ese es un hecho.", El emperador Bill Gates, Revista LA NACIÓN, número 1445. 16 de marzo de 1997 Pág. 25. Buenos Aires, Argentina.

Señala Alterini que la era de la sociedad industrial a llegado a su fin, quizás el 6 de agosto de 1945 cuando el hombre demostró haber dominado la fisión nuclear o quizás el 20 de julio de 1969, cuando arribó a la Luna.

Ha comenzado una nueva etapa en la historia; se trata de una era designada como tecnológica, tecnotrónica, postindustrial, neoindustrial, superindustrial, postmoderna, de la información de muchas otras maneras posibles[1].

Sin perjuicio de ello pareciera que los términos más utilizados para referirse a este nuevo período histórico son: *Era tecnológica o de la información,* éste último debido a la creciente importancia de la misma, a punto tal que se le considera una nueva forma de poder y al mismo tiempo un sector de la economía en sostenido crecimiento.

Vivimos en una sociedad tecnológica, cuya protagonista es la computadora y en donde la informática es considerada como un fenómeno técnico que ha producido un impacto económico, social y legal tan amplio como pocos otros acontecimientos tecnológicos en la historia de la humanidad.

---

[1] ALTERINI, Atilio Aníbal, Desmasificación de las relaciones obligaciones en la era postindustrial, en L. L. 1989-C-955.

El futuro estará marcado por la presencia siempre creciente y cada vez más compleja de la informática y de la cibernética en todo el quehacer del hombre. La película "**La Red**"[2] describe con un cierto tinte fatalista - en un tono pesimista o simplemente apresurado en el tiempo, pero no por ello sin dejar un mensaje que llama a la reflexión, cómo la informática a la par de los progresos puede convertirse en una fuente de inseguridad ciudadana; en un estado de permanente sospecha acerca de sí algo es real o no.

Parece estar orientado en una misma dirección que la novela de George Orwell titulada "1984" en la que - siguiendo el comentario que de ella hace Vittorio Frosini -[3], el escritor inglés brinda la profecía de un futuro que no quiere ver realizado, un mundo dominado por la tecnocracia, es decir, por una clase dirigente que dispone de los instrumentos de dominio de la mente humana y poblado por la clase más extensa de los proletarios sometida a la primera que se encuentra excluida de la participación activa en el control de la mente, compuesta por nuevos ilotas.

Si hablamos de la sociedad de hoy como una "sociedad de la información", corresponde en primer lugar intentar un acercamiento hacia un concepto del término información. Vittorio Frosini la define como "la capacidad de acumulación,

[2] LA RED, Dirección: Irwing Winkler, intérpretes: Sandra Bullok, Jeremi Northan y Dennis Miller; COLUMBIA TRISTAR - HOME VIDEO, LK-TEL, VIDEOVISA S.A. DE C.V..
[3] FROSINI, Vittorio, Informática y Derecho, trad. Por Guerrero y Allerra Redín, Editonal Temis S.A., Bogota Colombia 1988, Pág. 27.

elaboración y distribución de la experiencia humana por medio de un lenguaje que puede ser oral, mímico o simbólico, es decir, que puede valerse de las facultades humanas del oído, de la vista o de la abstracción".[4]

Por su parte Pierre Catalá entiende por información "todo mensaje comunicable a otro por cualquier medio, haciendo referencia también a la existencia de un derecho sobre la información que puede entrar en conflicto con el derecho a la información, propio de un estado de derecho en el cual se reconoce el pluralismo de la información y la libre investigación científica".[5]

En apretada síntesis, pero sin renunciar a la claridad, expone Frosini, cómo la civilización del hombre comienza con el intercambio de informaciones entre ellos y como va evolucionando con el correr del tiempo. En un primer momento el mensaje se brindaba en forma directa, inmediata e individual, luego se extiende al grupo y posteriormente a un grupo cada vez más amplio.

"La invención del lenguaje figurativo representa un paso importante pues a través del signo, luego escritura el mensaje se plasma en la roca y se separa del hombre

[4] Ibídem, Pág. 29.

[5] CATALÁ, Pierre, Ebauche d'une theorie juridique de l'information, Recueil Dalloz Sirei, 16° Cahier, Chronique, 1984 citado en: CORREA NAZAR ESPECHE, CZAR de SALDUENDO, BATTO, Derecho informático, Ed. De Palma Buenos Aires 1994, Pág. 288

para transformarse en cosa, lo que permite comunicar a los presentes con los ausentes y a los vivientes con los muertos que les habían precedido y con lo vivientes que les seguirán. El paso más importante lo marca la aparición de la escritura impresa con caracteres móviles sobre papel, permitiendo la aparición de la prensa diaria."[6]

Lo que aquí se pretende dejar en claro es que la información no es algo nueva sino que por el contrario, existe desde tiempos remotos y ha servido al hombre, entre otros propósitos para alertar a su semejante sobre los peligros que los acechaban, indicarle donde buscar alimento, difundir a otro sus ideales y/o las noticias de la ciudad, etc.

Lo que ocurre es que hoy la información se presenta con caracteres propios que realzan su importancia en el esquema de la sociedad. Su cantidad, variedad, rapidez de circulación, necesidad de la misma en cuanto a toma de decisiones y por último la posibilidad de su tratamiento automático constituyen las piedras fundamentales en las cuales se asientan este extraordinario fenómeno.

[6] FROSINI, Vittorio, Ob. Cit. Págs. 29 y ss.

"Se ha dicho que si la economía del siglo XIX estuvo dominada por el desarrollo de las fuentes de energía, la del siglo XX y más particularmente su segunda mitad se caracterizará en la historia económica como el siglo de la información."[7]

"La comunicación humana, luego de la fase oral, escrita manual y escrita impresa, a alcanzado su cuarta fase de desarrollo: la de la comunicación tele transmitida (radio, televisión, ordenador) superando todo los límites de tiempo y espacio, es por ello que ha dado origen al sector cuaternario de la economía. El sector de la información que se agrega a los tres anteriores (agricultura, industria, servicios."[8]

EL FENÓMENO INFORMÁTICO.

Resulta necesario entonces, arribar a una definición de informática para una etapa posterior, continuar en el camino que me llevará a una acabada noción de informática jurídica, derecho informático y como consecuencia a los delitos informáticos.

Daniel Ricardo Altmark brinda una serie de conceptos que revelan la amplitud de su contenido y así sostiene que ha sido definida como: *"la disciplina que estudia el fenómeno de la información y la elaboración, transmisión y utilización de la*

[7] TOUBOL, Frédérique, El software: Análisis jurídico, trad. De Luis Moisset de Espanés, Zavalia, Buenos Aires, 1990, pág 11.

información principalmente aunque no necesariamente con la ayuda de ordenadores y sistemas de telecomunicaciones como instrumentos, y en una definición aún más amplia como "la aplicación racional y sistemática de la información para el desarrollo, económico, social y político."[9]

También cita - el autor mencionado -, el concepto adoptado por el Centre de Recherches informatiques et Droit des Facultes Universitaires de Namur, al decir que " *Son los aspectos de la ciencia y la tecnología específicamente aplicables al tratamiento de la información y en particular al tratamiento automático de datos*".

En un sentido similar Elías P. Guastavino entiende por informática: *"El tratamiento automático de la información a través de elaboradores electrónicos basados en las reglas de la cibernética"* y define a esta última como *"la rama de la ciencia que estudia los sistemas de control y especialmente de auto - control en organismos y máquinas."*[10]

En este marco de informatización de la sociedad, la tecnología de la información impacta en la vida del hombre no solo en el ámbito informático dado su utilidad en la actividad económica en general sino también en el aspecto cultural y en las relaciones sociales y políticas de los individuos.

---

[8] FROSINI, Vittorio, Ob. Cit.; Pág. 21.
[9] ALTMARK, Daniel Ricardo, La etapa precontractual en los contratos informáticos, en Informática y Derecho, Volumen 1°, Ed. De palma, Buenos Aires, Argentina, 1987, Pág. 6.

Este avance científico, que ha posibilitado múltiples y valiosas aplicaciones en la vida moderna también posee una contracara que lejos de ocultarse debe ser estudiada para evitar sus efectos nocivos.

Por un lado constituye una seria amenaza que posibilita el ensanchamiento de la brecha existente entre países con distintos niveles de desarrollo, en este caso concreto entre los países con un alto grado de civilización tecnológica y aquellos más retrasados, los cuales por la falta de desarrollo informático pasan a ser objeto de una nueva forma de dependencia.

El tema ha sido tratado con profundidad por CORREA, NAZAR ESPECHE, CZAR de ZALDUENDO, BATTO, señalándose: " Que el desafío es, ante todo, de orden político, pues requiere que cada país tome una posición frente a este revolucionario fenómeno y opte por alguna de las diversas alternativas que objetivamente abren las condiciones tecnológicas y económicas en que aquél se desenvuelve."[11]

---

[10] Responsabilidad Civil y otros problemas jurídicos en computación, La Rocca, Buenos Aires Argentina, 1987, Pág. 25.
[11] Ob. cit. Pág. 1.

También analizan los autores mencionados la asimetría Norte - Sur, haciendo referencia a la disparidad existente en el acceso a la informática entre los países del Sur, que recién despiertan a este fenómeno, y los del Norte, que son los principales beneficiarios del fenómeno informático.

Incluyen como anexo del capítulo primero de su obra el informe de la Comisión Nacional Informática* de Argentina, del cual trasladaremos a modo de resumen algunos fundamentos del objetivo de definir una política nacional en materia de informática y tecnologías asociadas.

El reconocimiento del potencial que la tecnología informática y electrónica ofrece para el mejoramiento económico y social del país, a través de aumentos de productividad y de calidad en la producción de bienes y servicios y la mejora en las condiciones de trabajo en el acceso a la cultura y en la integración de sus distintas regiones.

El avance tecnológico acentúa las diferencias que separan a los países ricos de los pobres, anticipan nuevas formas de división internacional del trabajo y ponen crecientemente en cuestión el ejercicio de la soberanía política y económica.

* La citada comisión fue creada 621/84, presidida por el Secretario de Ciencia y Técnica e integrada por Representantes de varios ministerios y organismos gubernamentales de Argentina.

Crear el contorno de políticas económicas, tecnológicas y científicas aptas para favorecer el nacimiento de una industria informática y electrónica, dinámica, innovadora o independiente, único camino para alcanzar una autonomía tecnológica y la capacidad propia de decisión a las que el país aspira.

EL DERECHO Y LOS CAMBIOS SOCIALES. *

A esta altura ya es posible advertir la trascendencia actual y el impacto que la informática a tenido y tendrá en tiempos venideros en toda organización social, ya sea en el ámbito económico, político, cultural y jurídico.

Dada la irrupción del fenómeno en todos los ámbitos de la vida de una sociedad es evidente que el mismo no puede quedar al margen del control del derecho que regula y da las directivas de la actividad humana y las relaciones sociales.

El desafío para los hombres del derecho consiste en aprender estos cambios sociales y buscar las soluciones adecuadas para las cuestiones no reguladas o con una regulación deficiente en el sistema legal vigente.

---

* "Los juristas deben vivir con su época si no quieren que esta viva sin ellos. O acompañan los cambios o estos dejarán a la vera a los juristas" (JOSSERAND) "Al reconocer cosas nuevas, es evidente la necesidad de vivificar el derecho estimado como equitativo durante tanto tiempo" (ULPIANO, LIBRO I TITULO IV, Ley Segunda)

Sostiene Goldenberg Isidoro H., que este desfase entre los instrumentos normativos y la realidad normada no es algo novedoso, por el contrario constituye una constante en la historia del derecho, por continua y vertiginosa movilidad de los hechos sociales que la norma debe regular.

También afirma que no existe área de la juridicidad "que haya permanecido incólume ante el impacto tecnológico y que la incidencia del mismo no se verifica sólo en el derecho privado sino que se proyecta hacia las restantes disciplinas jurídicas y también a otras ciencias del campo cultural como la antropología, la sociología y la economía".[12]

Resulta oportuno mencionar aquí algunas conclusiones elaboradas por la Doctrina en la Décimo Segundas Jornadas de Derecho Civil (UNIVERSIDAD NACIONAL DEL COMAHUE, San Carlos Bariloche, Argentina, 1989), en la comisión número ocho "Impacto tecnológico y manifestación social en el derecho privado" a saber:

- En la actual era tecnológica son gravitantes en el medio social tres poderes; el científico - técnico, el de los medios masivos de comunicación social y el jurídico.

[12] GOLDENBERG, Isidoro H., Impacto Tecnológico y Manifestación social en el Derecho Privado, en L. L. 1989 E-872.

- El Derecho debe jugar un papel protagónico como agente activo de los cambios sociales.
- Las transformaciones producidas a raíz de los avances científicos y técnicos deben estar guiadas a la mejor condición del hombre, afianzar, su libertad.

La informática, al igual que la ciencia y la técnica son intrínsecamente neutrales, de allí que no pueda ser calificada como buena o mala que traiga consigo y por sí sola el progreso total o el caos absoluto; si no que deba apreciarse no en forma aislada sino en su propio contexto, integrándola con la finalidad con la que se emplea apreciando en el caso concreto los pro y los contra de su utilización.

Es, en definitiva, un instrumento, una herramienta, *"... no es un fin en sí mismo sino un medio para realizar determinados objetivos."*[13]

En la primera relación no se puede desconocer la interferencia de la economía en la elaboración de derecho y tampoco concebir a este último como un instrumento dócil e independiente al servicio de los intereses económicos.

En la segunda ocurre algo similar y nos encontramos ante la necesidad de lograr un equilibrio, ya que el derecho no puede hacer oídos sordos y desconocer los avances tecnológicos y sus consecuencias en la sociedad, pero tampoco conviene

subordinar la regla jurídica a los mandatos de los descubrimientos, experimentos o posibilidades que se abren camino a partir de la revolución tecnológica.

Este punto de equilibrio puede hallarse en las palabras de Goldenberg: "*Es necesario aprehender las mutaciones con sentido valioso orientándolos hacia una civilización no alentada, en la cual la ciencia y la tecnología se subordinen las auténticas necesidades y aspiraciones creadoras del individuo para que realizando sus latentes reservas espirituales pueda desempeñar el papel protagónico en la historia.*"[14]

INFORMÁTICA Y DERECHO.

En las relaciones entre informática y derecho podemos vislumbrar por una parte como la informática se acerca al mundo del derecho para tomar un nuevo campo de acción, la información jurídica y en el otro sector, el derecho penetra en el mundo de la informática para enfrentar los problemas que de ella se deriven, necesitados de una adecuada regulación.

---

[13] PALAZZI, Pablo Andrés, Virus informáticos y responsabilidad penal en el L. L. 1992-E-1122.
[14] GOLDENBERG, Isidoro H., Ob. Cit. Pág. 873.

En un primer momento hacia la década de 1970 el interés se centraba en las nuevas posibilidades de investigación y aplicación práctica que la informática ofrecía a los operadores del Derecho.

Con posterioridad la atención se fue desplazando sobre las nuevas perspectivas de elaboración doctrinal de los institutos jurídicos surgidos del nuevo mundo social de las computadoras "la importante y compleja problemática que el fenómeno informático acarreaba".[15]

Podemos decir que dentro de la vinculación entre la ciencia jurídica y la ciencia del tratamiento automático de la información, surgen dos sectores perfectamente delimitables, como producto de que cada una toma a la otra como objeto de estudio dentro del respectivo ámbito de actuación que a ellas compete. Esto da lugar al nacimiento de la informática jurídica y el derecho informático.

INFORMÁTICA JURÍDICA.

Para Elías P. Guastavino, la informática jurídica surge "cuando se aplican los instrumentos informáticos a los fenómenos del Derecho; se refiere a la informática

[15] FROSINI, Vittorio, Ob. Cit. Pág. 136.

como avanzado medio técnico que proporciona auxilio y servicio a las diversas actividades relacionadas con el Derecho."[16]

En sentido coincidente puede ser definida como el ámbito de la informática al servicio del derecho, es decir: "como instrumento que en el ámbito del derecho permite optimizar la labor del abogado como el jurista y el juez."[17]

Esta aplicación concreta de la información se traduce en distintas formas de captar su utilidad, lo que ha dado lugar a la subdivisión en distintas especialidades; informática jurídica documentaría e informática jurídica de gestión e informática jurídica decisional.

INFORMÁTICA JURÍDICA DOCUMENTARIA.

Con el correr del tiempo se va haciendo cada vez más difícil el conocimiento completo y actualizado de la legislación no sólo por parte de la población en general sino también por los abogados y funcionarios encargados de crear y aplicar el derecho.

[16] Ob. cit. Pág. 26
[17] ALTMARK, Daniel Ricardo, ob. cit. Pág. 7

Para los operadores del derecho, la situación deviene aún más complicada cuando se precisa recabar datos sobre doctrina o jurisprudencia de algún tema en especial.

Es necesario ante esta situación recurrir a la valiosa aportación de la informática jurídica documental, que nos permitirá, con el auxilio de las técnicas de tratamiento electrónico de la información, proceder a la selección de los datos. (Legislación, jurisprudencia, doctrina.) "A ser almacenados para su posterior recuperación por el jurista, al proceso de programación que permita el ingreso y modificación de documentos para su posterior consulta y la necesaria uniformación del lenguaje, que permita la correcta búsqueda de los documentos componentes de la base de datos."[18]

En suma, la informática jurídica documental tiene como objetivo el reemplazo de los métodos tradicionales de tratamiento de la información - en la actualidad ineficaz -, por sistemas informáticos que permitan el ingreso, archivo y recuperación de datos de interés para la ciencia jurídica.

Un ejemplo en México de este punto es el software denominado IUS - 6 y últimamente Jurisprudencia 2000 producido y distribuido por la Suprema Corte de

Justicia de la Nación y el acceso al servidor de la misma en la dirección electrónica http://www.scjn.gob.mx.

INFORMÁTICA JURÍDICA DE GESTIÓN.

La informática jurídica de gestión consiste en: " funciones de colaboración técnica y administrativa para las tareas jurídicas, para lo cual deben diagramarse y programarse distintos tipos de sistemas informáticos que contemplen las necesidades del usuario en relación con los problemas que desea resolver." [19]

La importancia de la informática jurídica de gestión, puede observarse por su aplicación, fundamentalmente en dos ámbitos.

Primeramente en la informatización de las oficinas judiciales, sobre todo en lo concerniente a sus tareas administrativas; y en segundo lugar, en la automatización del trabajo profesional del abogado, permitiéndole organizar adecuadamente su estudio jurídico.

Esta específica aplicación de la informática al Derecho que estamos desarrollando pareciera hacerse cada vez más necesaria, razón por la cual empezamos a descubrir su utilidad ya que su aplicación "... *no sólo permitirá optimizar la labor del abogado, el jurista y el juez, sino que jerarquizará su accionar al despejarles el*

[18] FROSINI, Vittorio y ALTMARK, Daniel Ricardo, Ob. Cit. Pág. 8,136.

camino para centralizar su tarea en los niveles superiores de la creación y la decisión".[20]

INFORMÁTICA JURÍDICA DESICIONAL.

La informática jurídica en este ámbito denominado como descicional, se basa específicamente en Sistemas expertos, "... *los que a partir de ciertas informaciones son capaces de resolver ciertos problemas en un ámbito específico, mediante la simulación del razonamiento humano*"[21].

El jurista italiano Antonio Martino nos explica que: " ésta parte de la informática jurídica comienza a ocuparse del campo de la toma de decisiones de los operadores jurídicos, con el auxilio de los sistemas expertos, no siendo necesario que el sistema tome la decisión, puede ser simplemente - como generalmente lo es - una ayuda a la decisión que se puede dar en varios planos y en varios ámbitos." [22]

DERECHO INFORMÁTICO.

---

[19] GUASTAVINO, Elías P. , Ob. Cit. Pág. 29
[20] ALTMARK, Daniel Ricardo, Ob. cit. Pág. 11.
[21] Ibidem Pág. 12.

Es el turno ahora, de abundar en algunos aspectos relativos al segundo aspecto que señalábamos dentro de la relación informática y Derecho, en el cual éste último toma a la primera como objeto de su saber y la alcanza con su regulación.

El avance de la informática en la sociedad produce, como es lógico, importantes efectos en las relaciones entre los individuos que la componen y por ende en las relaciones jurídicas.

Ante esta situación se impone al derecho la necesidad de estudiar estas nuevas relaciones y proceder a la elaboración de respuestas y soluciones jurídicas acordes a los cambios que estamos experimentando.

Con toda claridad a dicho Jorge Bekerman que: "cuando el fenómeno técnico provoca hechos nuevos, como en este caso, es necesario emprender el camino de su recepción en el campo del deber ser."[23]

Altamark Daniel Ricardo esboza un concepto de *Derecho informático* sosteniendo que *"es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática."*[24]

---

[22] MARTINO, Antonio, La informática jurídica hoy, en "Revista del derecho industrial", N 21, Pág. 566, Ed. De palma, citado por ALTMARK, Daniel Ricardo, Ob. Cit. Pág. 12.
[23] Bases de Datos y Bancos de Datos. ¿Producto o servicio?, en L. L. 1990 - C- 942.
[24] ALTMARK, Daniel Ricardo, Ob. cit. Pág. 18.

En una misma orientación aunque agregando a la definición un elemento teleológico y un tinte más descriptivo Carlos Alberto Parellada lo define como: "*el conjunto de normas, reglas y principios jurídicos que tiene por objeto evitar que la tecnología pueda conculcar derechos fundamentales del hombre; que se ocupa de la regulación de lo relativo a la instrumentación de las nuevas relaciones jurídicas derivadas de la producción, uso y comercialización de los bienes informáticos, así como de la transmisión de los datos.*"[25]

1.2. CONCEPTO DE "DELITOS INFORMÁTICOS"

Aún no es fácil conceptualizar a los delitos informáticos por su novedad, variedad y complejidad. La doctrina no se apoya en un parámetro claro y común desde el cual comenzar los intentos de definición. No obstante, trataremos de despejar algunas confusiones habituales que nos permitan esbozar un concepto de delito informático, a nuestro juicio, apropiado.

El *delito informático* implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales

[25] PARELLADA, Carlos Alberto, Daños en la actividad judicial e informática desde la responsabilidad profesional, Ed. Astrea, Buenos Aires, 1990, Pág. 219, citando en dicha definición a Guastavino, responsabilidad civil y otros problemas jurídicos en computación, COCCA, Aldo. El derecho: programador de la informática, J.A., 1983-III-681, Cap. IV. Pág. 27;

como robos o hurto, fraudes, falsificaciones, perjuicios, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

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

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que **Julio Téllez Valdés** señala que *"no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún."* [26]

Para **Carlos Sarzana**, en su obra Criminalità e tecnologia, los crímenes por computadora comprenden *"cualquier comportamiento criminógeno en el cual la*

[26] Derecho Informático 2ª Ed. México, Ed. Mc Graw Hill 1996 pág.103.

computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo." [27]

Nidia Callegari define al *delito informático* como *"aquel que se da con la ayuda de la informática o de técnicas anexas."* [28]

Rafael Fernández Calvo define al *delito informático* como *"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el "Título 1" de la* Constitución Española." [29]

María de la Luz Lima dice que el *"delito electrónico "* en un sentido amplio es *"cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las*

[27] "Criminalitá e Tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Ano 1 1979. Roma, Italia Pág.53

[28] "Delitos Informáticos y Legislación" en Revista de la Facultad de Derecho y ciencias politicas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 Julio-Agosto-Septiembre de 1985, Pág.115.

[29] "El tratamiento del llamado delito informático en el proyecto de ley orgánica del Código Penal: Reflexiones y propuestas de la C.L.I. (Comisión de Libertades e Informática) en Informática y Derecho.Pág.1150

computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin." [30]

Julio Téllez Valdés conceptualiza al *delito informático* en forma típica y atípica, entendiendo por la primera a *" las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin"* y por las segundas *"actitudes ilícitas en que se tienen a las computadoras como instrumento o fin."* [31]

El profesor **Miguel Ángel Davara**, brinda como definición de delito informático la siguiente: *"la realización de una acción que reuniendo las características que delimitan el concepto de delito sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"*[32]

María Cinta Castillo y Miguel Ramallo definen que Delito informático es: " toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizadas en las actividades informáticas "[33]

Por su parte, Lilli y Massa afirman que la locución " Delito Informático", puede entenderse en un sentido restringido y otro amplio.

---

[30] "Delitos electrónicos" en Criminalia, México. Academia Mexicana de Ciencias Penales. Ed Porrúa. No. 1-6. Año L. Enero - Junio 1984 Pág.100
[31] Ob. cit. Pág. 104
[32] "Derecho Informático" Ed. Aranzadi, Panamá, 1993 Pág.319

"En su concepto de estricto sentido, comprenden los hechos en que se atacan elementos puramente informáticos (independientemente del perjuicio que pueda causarse a otros bienes jurídicamente tutelados y que eventualmente puedan concurrir en forma real o ideal); mientras que en su concepto amplio "abarca toda acción típicamente antijurídica y culpable para cuya consumación se utilizó o se afecta una computadora ó sus accesorios"[34]

Estas definiciones deben ser precisadas para no inducir a error, ya no todo ilícito en que el se emplee una computadora como medio o instrumento para su consumación tendrá tal carácter, ya que puede tratarse de una figura típica tradicional informatizada a la que llamamos delito computacional.

Eso sí, aclaremos que no puede afirmarse que todo delito en que interviene una computadora como medio, es un delito informático o un delito computacional, pues el uso que se le dé, debe ser el normal de acuerdo a su naturaleza. Por ejemplo, no sería un delito computacional las lesiones que se causen a una persona golpeándolo con un monitor o un teclado.

---

[33] Citado por Riquert, Marcelo A; " Derecho Penal e Informática: Una aproximación genérica a su ardua problemática", periódico económico tributario, año V, Número 144,.Buenos Aires; Argentina. Pág. 2
[34] Ob. Cit. Pág. 3

Por lo tanto, una primera conclusión que nos llevará a un concepto de delito informático es excluir de la definición a los delitos computacionales.

Ahora bien, teniendo claro que buscamos conceptualizar las conductas ilícitas nuevas, cometidas generalmente a través de equipos computacionales, pero en donde el elemento central no es el medio de comisión sino que es el hecho de atentar contra un bien informático, se hace necesario destacar que no todos los bienes informáticos son objeto de estos delitos.

Los sistemas de tratamiento automatizado de la información se basan en dos grandes tipos de soportes, el físico y el lógico.

Así, por una parte, los bienes informáticos que tienen relación son el soporte físico conforman el hardware, es decir los equipos, que son bienes corporales muebles como el procesador o la unidad central de proceso y los dispositivos periféricos de entrada y salida, como por ejemplo, el monitor, el teclado, la impresora, un escáner, etc.

En cambio, por la otra, existen bienes intangibles que constituyen el soporte lógico del sistema o software. Dentro de él están los datos digitalizados (es decir, transformados a un lenguaje computacional basado en un sistema binario o de base 2, en donde sólo existen dos cifras, los ceros y los unos), que se ingresan a la computadora para que sean procesados y puedan constituir información.

Además, encontramos otros bienes informáticos como los programas computacionales, que son un conjunto de instrucciones para ser usadas directa o indirectamente en una computadora a fin de efectuar u obtener un determinado proceso o resultado.

Pues bien, no todos los bienes computacionales son objeto de delitos informáticos. Contra el hardware o soporte físico se cometen delitos convencionales o delitos computacionales (si se usa como instrumento a la computación), pero no delitos informáticos, es decir, figuras nuevas no encuadradas en las ya existentes.

Si los equipos computacionales son bienes tangibles, corporales, muebles no hay inconveniente para que se cometan en su contra los tradicionales delitos de Robo, fraude o daño en propiedad ajena.

De esta forma, descartamos la incorrecta idea que algunos autores sostienen con relación a calificar como delitos informáticos al robo de una computadora o el robo de un cajero automático, los incendios intencionales y atentados terroristas en contra de una central de computación, por ejemplo.

Es más, incluso empleando como medio de comisión a las tecnologías de la información no estamos en presencia de un delito informático, sino de un delito computacional.

Por ejemplo, el introducir un " virus físico o destructivo", que altere el funcionamiento del sistema exigiéndolo más allá de sus capacidades logrando un sobrecalentamiento que acarrea que se quemen el disco duro, la tarjeta de video o el monitor, es un delito de daños convencional informatizado o delito computacional.

Hay autores que clasifican estas conductas destinadas a destruir los elementos físicos del sistema dentro del sabotaje informático.

Ellos justifican la penalización de tales conductas como delitos informáticos, basados en la desproporción que existe entre el valor de los equipos y el perjuicio que implica la destrucción correlativa; en la impunidad de los autores favorecida por la detectabilidad del ilícito bastante tiempo después; y por la gran dificultad que presentan para valorar la real cuantía del daño producido en atención al valor del material destruido.

Si bien reconocemos que estas son características que se pueden dar cada vez que se atenta contra un sistema de tratamiento de información, en ningún caso son elementos que justifican un tipo penal distinto al delito de daños.

Sin duda, la información que se perderá en este tipo de atentados tiene un valor estratégico muchas veces no comparable con el valor económico del hardware, sin embargo, esto también ocurre cuando se atento contra archivos, registros,

bibliotecas o museos circunstancias que el legislador no considera suficiente como para crear un "delito bibliotecario" por ejemplo, pero sí reconoce su importancia incluyéndolo dentro del delito de daños.

En este caso, si la protección que otorga este delito convencional no es suficiente, debería mejorarse el tipo o la pena y no crear un delito específico nuevo.

Finalmente, ¿ acaso el insertar un clip en el mecanismo de las computadoras para causar cortos circuitos eléctricos, verter café, soluciones de sal y agentes de limpieza cáusticos sobre el teclado y en otros periféricos, arrojar humo, spray para el cabello y otros gases dentro del mecanismo, provocar temperaturas extremas calentando partes de la computadora mediante cigarrillos merecen calificarse de manera distinta a un delito de daños en propiedad ajena?.

Creemos que no y por ello damos segunda conclusión para llegar al concepto de que el delito informático no atenta contra el hardware sino que contra el soporte lógico.

¿Por qué el atentar contra el soporte lógico puede ser calificado como delito informático? Porque la especial naturaleza de los datos digitalizados y de los programas computacionales, su carácter intangible, no le permite al delito tradicional cubrirlo haciendo necesaria la creación de un delito nuevo.

Precisamente el profesor chileno Renato Jijena Leiva sostiene esta postura. Es más, piensa que la especial naturaleza de los programas computacionales no les permite estar ni siquiera incluidos en una clasificación tan general como la de cosas corporales e incorporales.

Si definimos a los programas computacionales como un conjunto de instrucciones para ser usadas en una computadora, no podrán ser percibidas por los sentidos, y por ende, no son cosas corporales.

Y tampoco consisten en meros derechos, es decir, no son cosas incorporales.

Se trataría de meros impulsos electromagnéticos que se transmiten a través de circuitos electrónicos no perceptibles por los sentidos del hombre, ya que lo que se observa en un monitor es el resultado obtenido con el procesamiento electrónico de las instrucciones.

Como consecuencia de ello, por ejemplo, penalmente no se podría cometer delitos patrimoniales de robo, al copiar ilegalmente un programa computacional, puesto que no sería ni un documento ni una cosa corporal mueble.

Al ser intangibles e inmateriales no se pueden aprehender físicamente, es más, al copiarlos ilegalmente no le son privados en forma permanente a la víctima del delito.

Sólo una nueva figura delictiva, es decir, un delito informático, podría sancionar penalmente tales conductas.

Por lo tanto, la definición que consideramos más apropiada para los delitos informáticos es: *"toda conducta que revista características delictivas, es decir, sea atípica, antijurídica y culpable y atenté contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del empleo de las tecnologías de la información y el cual se distingue de los delitos computacionales o tradicionalmente informatizados".*

Esta idea es compartida por el autor más prestigioso de Europa con relación a los delitos informáticos, el profesor alemán Ulrich Sieber, quien los define como *"todas las lesiones dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente."* [35]

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

[35] Citado por CORREA, Carlos M. Derecho Informático, Ed. De Palma, Buenos Aires Argentina, 1987, Pág. 296

En este orden de ideas, en el presente trabajo se entenderán como *"delitos informáticos"* ***todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.***

Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes en México debido a que la legislación se refiere al derecho de autor, propiedad industrial e intelectual, sin embargo, deberá tenerse presente que la propuesta final de este trabajo tiene por objeto la regulación penal de aquellas actitudes antijurídicas que estimamos más graves como último recurso para evitar su impunidad.

1.3SUJETOS EN LOS DELITOS INFORMÁTICOS.

SUJETO ACTIVO

Las personas que cometen los *"Delitos Informáticos"* son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son

hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

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

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

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los *"delitos informáticos"*, estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano **Edwin Sutherland**[36] en el año de 1943.

[36] Citado por TELLEZ, Valdés, Julio. Ob. Cit. Pág.98

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

Asimismo, este criminólogo estadounidense dice que tanto la definición de los "delitos informáticos" como la 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.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil 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 tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Por nuestra parte, consideramos que a pesar de que los "*delitos informáticos*" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objetos de un estudio más profundo, que dada la naturaleza de nuestro objeto de estudio nos vemos en la necesidad de limitar.
De lo anterior podemos concluir que será sujeto activo, con relación a los delitos informáticos cualquier persona física con conocimientos suficientes y especiales en materia informática que realice la conducta típica.

SUJETO PASIVO

En primer término tenemos que distinguir que *sujeto pasivo ó víctima del delito es el titular del Bien Jurídico tutelado y quien resiste la conducta del sujeto activo del delito,* **es decir 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 estos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; La falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática, se requiere en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz

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

1.4 BIEN JURÍDICO TUTELADO.

Es el valor o interés jurídico protegido, ya sea individual o social, que se pretende proteger a través del tipo penal, el cual puede ser el honor, el derecho a la intimidad, el patrimonio de las personas, la fe pública, la seguridad, la información, etcétera. Se puede plantear en extremos factibles que incluso la vida o la integridad física pueden llegar a ser bienes jurídicamente tutelables al sancionar tipos informáticos.

1.5 MEDIOS DE COMISIÓN.

Las tecnologías de la información han facilitado la aparición de nuevas conductas que, con independencia del mayor o menor reproche social generado, han obligado a los países avanzados a adaptar sus legislaciones para dar cabida a modalidades comisivas que no existían hace unos años.

El auge del Internet ha ayudado a difundir las técnicas utilizadas, de manera que pueden encontrarse webs especializados en cada una de las "disciplinas", en los que tanto los aficionados como los más expertos pueden encontrar manuales de instrucciones, esquemas y programas.

Con el término "hacking" nos referimos, en este caso, a la técnica consistente en acceder a un sistema informático sin autorización. Entendemos que existe autorización cuando el sistema está conectado a una red pública y no dispone de un control de acceso mediante el uso de identificadores de usuario y passwords o clave de acceso.

Al hablar de "cracks" nos referimos a los programas o rutinas que permiten inutilizar los sistemas de protección establecidos por el titular de los derechos de propiedad intelectual sobre una aplicación informática. Dentro de los numerosos tipos de crack existentes, destacan los que permiten seguir utilizando un programa de demostración (Demo o sharware) una vez superado el período de prueba establecido. También existen cracks que eliminan la llamada del programa a una llave electrónica, disco llave o número de serie.

Finalmente, en el concepto "phreaking" entrarían las técnicas de fraude en materia de telefonía analógica y digital. Uno de los métodos más utilizados en su día fue el de las denominadas "cajas de colores", que emitían distintas frecuencias, en función del resultado perseguido. Por ejemplo, las cajas azules utilizaban la frecuencia de 2600 hercios empleada por los operadores telefónicos para efectuar llamadas sin cargo.

Ahora es importante hacer notar que cada ciertos ciclos el derecho penal se ve superando por la realidad. Realidad que indica su desactualización como protector social y la necesidad de una reforma. Es aquí donde los códigos y esto vale para todos se vean superados por las circunstancias del hecho.

Las nuevas modalidades delictivas no son solamente formas sentidas por la sociedad como criminógenas, también forman parte de aquel concepto las nuevas modalidades de comisión de delitos anteriores, como el robo que por diferentes razones sea difícil perseguir penalmente, por citar solo un caso, un fraude es un fraude se haya cometido con papel o con un ordenador.

A continuación expondremos sobre algunas de las más modernas conductas no sancionadas por la ley sobre los sujetos que las cometen y que son entendidas como delitos y a sus perpetradores como delincuentes, más allá de las disposiciones legales que existen sobre la punibilidad de esa conducta.

HACKING

La palabra "hacking" proviene del inglés "hack" que significa "hachar" y es el término que se utilizaba para describir la manera en que los técnicos telefónicos arreglaban las cajas descompuestas: a golpes.

Se denomina "hacking" en la jerga informática a la conducta de entrar a un sistema de información sin autorización, es decir, violando las barreras de protección establecidas.

El sujeto que realiza esa actividad es llamado hacker, muy raras ves se le conoce su nombre verdadero y en muchos casos actúa y firma en grupo.

La actividad de hackear un sistema puede tener diferentes finalidades y alcances. Así en la mayoría de los casos el romper el sistema o eliminar los pasos de seguridad de un sistema tiene por objeto ver, fisgonear el contenido y la información protegida, otras veces extraer copias de la información y muy raramente destruir o cambiar los contenidos de la información.

Respecto de esta última situación, es decir, las entradas ilegales que tienen por objeto destruir un sistema, a esto se llama cracking y a los sujetos que lo realizan se los identifica como crackers. Esta es una expresión idiomática que se puede traducir como quebrar, es decir vencer las barreras de seguridad y romper lo que hay detrás de ellas.

En cualquiera de ambos casos, lo caracteriza las andanzas de los sujetos es su entrada ilegal al sistema, entendiendo el concepto de entrada ilegal como la entrada de toda aquella persona que no tiene las claves de acceso (password) o no las ha conseguido por los medios legales.

PHREAKING.

La actividad de phreacking es sin duda la más común de todas las llamadas actividades ilícitas informáticas.

Sin embargo es aquí donde se denota con máxima claridad las dificultades que se presentan al intentar dar una única definición de delitos informáticos. El phreacking es considerado un delito informático por la generalidad de los autores en la rama. El phreaking es la actividad de obtener ventajas de las líneas telefónicas a los efectos de no pagar los costos de comunicación. Es decir que básicamente se trata de encontrar el medio para evitar pagar el uso de la red telefónica ya sea pública o privada, digital o inalámbrica.

Dentro de esta categoría se engloban las tarjetas de monteo, las blue box, etc.

Pero adviértase que para estas actividades raramente se usa la Computadora Personal, salvo para coordinar o elaborar los chips de tarjeta, esta actividad es esencialmente extra computadora personal, telefónica, y se utiliza más bien en electrónica y no de ingeniería en sistemas.

Esta simple sutileza no parece ser advertida por demasiados estudiosos del derecho que engloban a todas las actividades, es como confundir el robo de ganado con el robo de camiones de ganado.

Ello no quita que tales actividades están emparentadas, pues si se revisa la red se observa que allí donde hay páginas de tipo under conviven los hackers y los phreaker sin inconvenientes y coadyuvándose los unos a los otros.

CARDING

Se llama carding a la actividad de cometer un fraude con un número de tarjeta de crédito.

Este concepto que parece simple tiene hontanares de cuestión, primero no todo fraude con tarjeta de crédito se transforma en carding, si se roba o se encuentra una tarjeta y es utilizada por otra persona que no es su titular, ello no es carding es solo un fraude.

El carding consiste entonces en usar un número de tarjetas de crédito ya sea real o creado de la nada mediante procedimientos digitales para realizar compras a distancias por Internet y efectuar pagos.

El nivel de seguridad en Internet para realizar transacciones económicas no son bueno, por ello existen fugas de información, muchos usuarios de la red ponen su número de tarjetas de crédito para hacer compras, estos números son captados por otras personas que los reutilizan para hacer más compras sin ser los titulares de la tarjeta.

A esta actividad debe agregarse la de generar números válidos de tarjetas de crédito para luego usarlos en compras a distancia.

Cuando una empresa de tarjetas asigna una tarjeta numerada a un usuario lo hace a través de un sistema automatizado de creación de números aleatorios. Por ello basta usar el mismo sistema para crear números válidos.

El carding es sin duda la actividad más riesgosa de todas las entendidas como delitos informáticos, pues si se quiere recibir lo que se compró, hay que ordenar que lo manden a algún sitio, he ahí el problema: a que sitio pues; Quien compró con un número de tarjetas que no era suyo, se arriesga a que lo descubran y al ir a recoger el o los productos, lo arresten.

CAPÍTULO II

TIPOS DE DELITOS INFORMÁTICOS

2.1 DIVERSAS CLASIFICACIONES DE LOS DELITOS INFORMÁTICOS.

A) Delitos tradicionalmente denominados informáticos

A pesar de que el concepto de delito informático engloba tanto los delitos cometidos contra el sistema, como con los delitos cometidos mediante el uso de sistemas informáticos, cuando hablamos del ciberespacio como un mundo virtual distinto a la "vida real", me refiero al delito informático como aquél que está íntimamente ligado a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información, etc.

Incluyo también dentro de este capítulo los actos que sólo constituirían una infracción administrativa o la vulneración de un derecho no tutelado por la jurisdicción penal, pero que en algunos países pueden llegar a ser delito.

Dentro de este tipo de delitos o infracciones podríamos destacar:

a) Acceso no autorizado:

El uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito informático, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave;

b) Destrucción de datos:

Constituye los daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático no disponen en algunos países de preceptos que permitan su persecución;

c) Infracción de los derechos de autor:

La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio en el ámbito jurisprudencial. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line o de un sysop respecto a las copias ilegales introducidas en el sistema. Mientras un tribunal condenó a un sysop porque en su BBS había imágenes scaneadas de la revista Play boy, en el caso "La Macchia", el administrador del sistema fue hallado no responsable de las

copias de programas que albergaba su BBS. El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a un "upload" de un programa o fichero que infrinja los derechos de autor de terceros;

d) Infracción de las bases de datos Copyright de:

No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información;

e) Interceptación de e-mail:

En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

f)Fraudes electrónicos:

La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría

todos los requisitos del delito de fraude, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador;

g) Transferencias de fondos:

Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático. A pesar de que en algunas legislaciones y en sentencias aisladas se ha asimilado el uso de passwords y tarjetas electrónicas falsificadas al empleo de llaves falsas, calificando dicha conducta como robo, existe todavía una falta de uniformidad en la materia.

B) Delitos convencionales

Al hablar de delitos convencionales me refiero a todos aquellos que tradicionalmente se han venido cometiendo a lo largo de la historia del hombre sin el empleo de medios informáticos y que con el auge de los sistemas informáticos se han reproducido también en la red de la información "Internet".

Entre los que se encuentran:

- **Espionaje.**
- **Espionaje industrial.**
- **Terrorismo.**
- **Narcotráfico.**
- **Robo.**
- **Falsificación de documentos.**
- **Fraude electrónico.**
- **Otros delitos:** Las mismas ventajas que encuentran en Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

C) Como señala el Profesor Dávara Rodríguez los delitos informáticos han sido clasificados de acuerdo al fin que persiguen de la siguiente manera:

"1. Manipulación en los datos e informaciones contenidos en los archivos o soportes físicos informáticos ajenos;
2. Acceso a los datos y utilización de los mismos por quien no está autorizado para ello;

3. Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas;
4. Utilización del ordenador y/o los programas de otra persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro;
5. Utilización del ordenador con fines fraudulentos y;
6. Agresión a la intimidad mediante la utilización y procedimiento de datos personales con fin distinto al autorizado."[37]

D) Otra clasificación de estas conductas catalogadas como delitos informáticos, es la que ofrece Uhirich Sieber, destacándolas de la siguiente forma:

"1. Fraude por manipulaciones de una computadora contra un sistema de procedimiento de datos;
2. Espionaje informático y robo de software;
3. Sabotaje informático;
4. Robo de servicios;
5. Acceso no autorizado a sistemas de procesamiento de datos, y
6. Ofensas tradicionales en los negocios asistidos por computadora." [38]

[37] DAVARA, Rodriguez Miguel Ángel. Ob. Cit Pág. 323
[38] Citado por CORREA, Carlos M. Ob. Cit. PÁG. 296

E) En varios estudios realizados por la Federación de los Estados Unidos de América, se han concretado manifestaciones de los llamados delitos informáticos o "computer-crime", como lo son:

"1. Introducción de los datos falsos en el sistema y manipulación de datos;
2. Uso no autorizado de instalaciones y elementos físicos de los sistemas informáticos, y
3. Atentados contra el patrimonio mediante computadoras." [39]

F) La clasificación existente en coincidencia con el Código penal del Estado Nacional de Panamá es el siguiente:

I. Delitos económicos vinculados a la informática: Fraude mediante manipulaciones contra los sistemas de procesamiento de datos, Espionaje Informático y robo (hurto) de software; sabotaje informático; Apropiación de servicios, Acceso no autorizado a los sistemas informáticos; Fraude fiscal informático

II. Ofensas por medios informáticos contra los derechos individuales de la persona: atentados contra la intimidad y privacidad.

[39] GUTIERREZ, Francés, Ma. Luz . "Fraude informático y estafa" Ministerio de Justicia, Secretaría General técnica, Madrid, España 1991, Pág. 62

III. Ataques por medio de la informática contra intereses supraindividuales: atentados contra la seguridad nacional; atentados contra la integridad de los procedimientos basados en la informática y en los procesamientos de datos, atentados contra la legitimación democrática de las decisiones parlamentarias vinculadas a los ordenadores.

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

1. Como instrumento o medio:
    - Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito;
2. Como fin u objetivo:
    - En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física." [40]

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

"1. Los que utilizan la tecnología electrónica como método,

2. Los que utilizan la tecnología electrónica como medio y

3. Los que utilizan la tecnología electrónica como fin.

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

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

Como fin.- conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla." [41]

I) Autores como Carlos Sarzana menciona que estos ilícitos pueden clasificarse: "en atención a que producen un provecho para el autor y provocan un daño contra la computadora como entidad física y que procuren un daño a un individuo o grupos, en su integridad física, honor o patrimonio, nosotros preferimos clasificarlos en atención a dos criterios: como instrumentos o medio, y como fin u objetivo.

Como instrumento o medio:

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

---

[40] Ibidem.

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

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

c) Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etc.)

d) " Robo " de tiempo de computadora.

e) Lectura, sustracción o copiado de información confidencial.

f) Modificación de datos tanto en la entrada como en la salida

g) Aprovechamiento indebido o violación de un código para penetrar a un sistema de instrucciones inapropiadas (esto es lo que se conoce en el medio como el método del "Caballo de Troya".

h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la "técnica de salami".

i) Uso no autorizado de programas de cómputo.

j) Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas, a fin de obtener beneficios, tales como "consulta a su distribuidor".

k) Alteración en el funcionamiento de los sistemas, a través de los cada vez más temibles "virus informáticos".

---

[41] LIMA, de la Luz, María, Ob. Cit. Pág. 85

l) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

m) Acceso a áreas informatizadas en forma no autorizada.

n) Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo.

En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

a) Programación de instrucciones que producen un bloqueo total al sistema;

b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

d) Atentado físico contra la máquina o sus accesorios, discos, cintas, terminales, etc..

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

f) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje (pago de rescate etc.)"[42]

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

Tipos de delitos informáticos reconocidos por Naciones Unidas

La categorización y clasificación de los fenómenos tiene siempre un aspecto pedagógico, pues a través de las mismas se puede apreciar con mayor nitidez las diferencias y relaciones que existen entre los sujetos sometidos a la comparación.

Nos referiremos aquí a las categorías de delitos informáticos reconocidas por las Naciones Unidas y que ha sido aceptada por la mayoría de la doctrina especializada. Naciones Unidas distingue tres tipologías de delitos informáticos, a saber:

"1.- Fraudes cometidos mediante manipulación de computadoras.
Entre estos se encuentra la manipulación de datos de entrada y salida y la manipulación de programas. En cada caso, lo que se trata es de colocar datos falsos en un sistema u obtener los datos del sistema en forma ilegal.

[42] Sarzana, Carlos. Ob. Cit. Pág. 34

2.- Falsificaciones informáticas.

En este punto se trata de usar las computadoras como elemento para falsificar entradas, dinero, tickets o cuentas bancarias.

3.- Daños a datos computarizados.

Aquí se ubican los virus, las bombas lógicas, los gusanos, accesos no autorizados, etc. Se trata, en general, de programas que de una u otra forma, dañan la información de un sistema determinado." [43]

Otra clasificación tradicional propuesta por el profesor alemán Klaus Tiedemann y compartida por Uhirich Sieber, hacen hincapié en la necesidad de distinguir entre los delitos informáticos de carácter económico (cuando se produce un prejuicio patrimonial) y los que atentan contra la privacidad (mediante la acumulación archivo y divulgación indebida de datos contenidos en los sistemas de datos informáticos.

Fraudes cometidos mediante manipulación de computadoras.

Manipulación de los datos de entrada

Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de

descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

La manipulación de programas

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

Manipulación de los datos de salida

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de

---

[43] Riquert, Marcelo A., Ob. Cit, Pág. 2.

adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática

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

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 basándose en 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.

Daños o modificaciones de programas o datos computarizados.

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. Las técnicas que permiten cometer sabotajes informáticos son:

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.

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. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica

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

Acceso no autorizado a servicios y sistemas informáticos

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Piratas informáticos o hackers

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

Reproducción no autorizada de programas informáticos de protección legal

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de

las redes de telecomunicaciones modema. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un *delito informático* debido a que el bien jurídico a tutelar es la propiedad intelectual.

2.3 DELITOS INFORMÁTICOS EN OTROS PAÍSES

ESPAÑA

Delitos Informáticos legislados en el Código Penal español.

El llamado Código Penal Español del siglo XXI incorpora nuevos bienes jurídicos que van a ser objeto de tutela a partir de ahora, al tiempo que refuerza bienes jurídicos tradicionales que se trasladan al nuevo ámbito jurídico del ciberespacio.

La polémica generada en todo el mundo por la aprobación en Estados Unidos, de la Comunications Decency Act, declarada inconstitucional en junio de 1996, nos obliga también a abordar el tema de los menores de edad, como víctimas potenciales de delincuentes que se aprovechan del anonimato de la red, por lo que analizaremos el tratamiento que el nuevo texto legal da a estas actividades.

Interceptación de correo electrónico

En el apartado correspondiente a los delitos contra la intimidad se introduce la interceptación de correo electrónico, que queda asimilada a la violación de correspondencia.

El artículo 197 del Código Penal Español, extiende el ámbito de aplicación de este delito a las siguientes conductas:

- Apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales;

- Interceptación de las telecomunicaciones, en las mismas condiciones;

- Utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, en las mismas condiciones de invasión de la intimidad y vulneración de secretos;

- Estas actividades deben producirse sin consentimiento del afectado y con la intención de descubrir sus secretos o vulnerar su intimidad;

- La pena que se establece es de prisión, de uno a cuatro años y multa de doce a veinticuatro meses (Con el nuevo concepto de días - multa, un día equivale a un mínimo de 200 pesetas y un máximo de 50.000 pesetas);

- El Código Penal anterior no había previsto las modalidades comisivas consistentes en el uso de las tecnologías de la información para invadir la intimidad de la persona o para violar acceder y descubrir sus secretos;

Usurpación y cesión de datos reservados de carácter personal

- También quedan tipificados los actos consistentes en apoderarse, utilizar, modificar, revelar, difundir o ceder datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos.

- El artículo 197 castiga con prisión de 1 a 4 años para el caso de acceso, utilización, etc., y de 2 a 5 años si los datos se difunden, revelan o ceden a terceros. Cuando dichos actos afectan 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.

- Esta inclusión de los datos personales en el Código Penal Español supone una importante innovación puesto que este aspecto de la intimidad personal no estaba tutelado en el anterior texto.

Estafas electrónicas

- El nuevo Código Penal Español introduce el concepto de la estafa electrónica, consistente en la manipulación informática o artificio similar que concurriendo con ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

- El Código Penal anterior exigía la concurrencia de engaño en una persona, lo cual excluía cualquier forma de comisión basada en el engaño a una máquina.

- El artículo 248 y siguientes establecen una pena de prisión de 6 meses a 4 años para los reos del delito de estafa, pudiendo llegar a 6 años si el perjuicio causado reviste especial gravedad.

Daños informáticos

En el delito de daños se contemplan los supuestos de destrucción, alteración, inutilización, o cualquier otra modalidad por la que se dañen los datos, programas o documentos electrónicos contenidos en redes, soportes, o sistemas informáticos.

El artículo 264.2 del Código Penal español establece una pena de prisión, de 1 a 3 años en el caso de daños informáticos.

El Código Penal Español anterior sólo preveía la destrucción de bienes materiales, por lo que los daños causados en bienes inmateriales no quedaban incluida en dicho delito.

El valor que pueden alcanzar en la actualidad los datos o la información de una empresa o administración pública en formato digital, ha obligado a incluir la figura del delito de daños informáticos en el Código Penal.

Delitos contra la propiedad intelectual

Respecto a los delitos contra la propiedad intelectual, no se introducen cambios significativos. Con la proliferación de las obras multimedia y el uso de la red, este tipo se aplicará no sólo a los programas de ordenador, sino también a los archivos con imágenes, gráficos, sonido, video, texto, animación, etc. que incorporan las webs y las bases de datos accesibles a través de Internet.

El artículo 270 del nuevo Código Penal español establece la pena de prisión de 6 meses a 2 años, e incluye en la categoría de los delitos contra la propiedad intelectual 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.

Difusión y exhibición de material pornográfico a menores

El artículo 186 del Código penal español tipifica como delito la conducta consistente en la difusión, venta o exhibición entre menores de edad o incapaces, de material pornográfico.

Dicha exhibición o difusión puede efectuarse mediante cualquier medio directo, por lo que entendemos incluida en este supuesto la difusión a través de Internet mediante correo electrónico dirigido a menores de edad, o la exhibición a través de un "web" o una "base de datos sin tomar las precauciones oportunas para impedir el acceso de menores.

Pornografía infantil

El artículo 189 Código penal español establece que el que utilizare a un menor de edad o a un incapaz con fines exhibicionistas o pornográficos será castigados con la pena de prisión de uno a tres años.

Difusión de mensajes injuriosos o calumniosos

El artículo 211 del Código penal español establece que los delitos de calumnia e injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante.
Puede incluirse perfectamente en este supuesto la difusión de mensajes injuriosos o calumniosos a través de Internet, en especial, en el entorno W.W.W. que es el más similar a la prensa tradicional.

Las penas establecidas pueden llegar a los 2 años de prisión en el caso de la calumnia, y multa de hasta 14 meses en el caso de la injuria.

El artículo 212 del Código mencionado, menciona la responsabilidad solidaria del propietario del medio informativo a través del que se haya propagado la calumnia o injuria.

En el caso de Internet, la responsabilidad civil solidaria alcanzaría al propietario del servidor en el que se publicó la información constitutiva de delito, aunque debería tenerse en cuenta, en este caso, si existió la posibilidad de conocer dicha situación, ya que el volumen de información contenida en un servidor no es comparable al de una revista, un periódico o un programa de Televisión o radio.

En este sentido cabe recordar la tesis que asimila al propietario de un servidor al librero, en contraposición con los que lo asimilan a un editor. La primera teoría es partidaria de liberar de responsabilidad civil al propietario de un servidor, debido a

la imposibilidad de controlar toda la información que es depositada en el mismo por los usuarios.

Publicidad engañosa en Internet

El uso del W.W.W. con fines publicitarios hace que se trasladen a Internet los eslógans y mensajes publicitarios que se difunden en la vida real, ello hace posible la aplicación de la ley a las infracciones que se produzcan en el ciberespacio y que puedan causar un perjuicio grave a los consumidores.

En este sentido el artículo 282 del Código Penal Español castiga con la pena de prisión de seis meses a un año a los fabricantes o comerciantes que, en sus ofertas o publicidad de productos o servicios, hagan alegaciones falsas o manifiesten características inciertas sobre los mismos de modo que puedan causar un perjuicio grave y manifiesto a los consumidores, sin perjuicio de la pena que corresponda aplicar por la comisión de otros delitos.

Robo

El artículo 239 del mismo ordenamiento, considera llaves falsas, las tarjetas magnéticas o perforadas así como los mandos o instrumentos de apertura a distancia, considerando por lo tanto delito de robo la utilización de estos

elementos, el descubrimiento de claves y la inutilización de sistemas específicos de alarma o guarda con el fin de apoderarse de cosas muebles ajenas.

Revelación de secretos

El artículo 278 del Código Penal Español señala una pena de 2 a 4 años para el que, con el fin de descubrir un secreto, se apoderase por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo.

Si los secretos descubiertos se revelasen, difundieren o cedieren a terceros, la pena llegará a los 5 años de prisión.

Falsedades documentales

Los artículos 390 y siguientes castigan con la pena de prisión de hasta seis años las alteraciones, simulaciones y demás falsedades cometidas en documentos públicos.

Los artículos 395 y 396 del Código Penal Español se refieren a las falsedades cometidas en documentos privados, pudiendo alcanzar la pena de prisión hasta dos años. También se castiga la utilización de un documento falso para perjudicar a un tercero.

El artículo 26 del mismo ordenamiento define como documento cualquier soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

Entendemos que quedaría incluido en el concepto documento los mensajes estáticos, compuestos por información almacenada en un sistema informático después de haber sido remitida o recibida a través de la red, pero surgen dudas sobre la naturaleza documental del mensaje que está circulando.

Finalmente, el artículo 400 del citado código introduce el delito consistente en la fabricación o tenencia de útiles, materiales, instrumentos, programas de ordenador o aparatos destinados específicamente a la comisión de estos delitos informáticos. Entrarían dentro de este tipo los programas copiadores, las utilidades empleadas por los hackers y cualquier otro dispositivo similar.

CANADA.

El uso no autorizado o abuso de una computadora encabeza, la lista de comportamientos penados por el derecho canadiense el cual puede emplearse para denunciar un uso penado de Internet. Este delito se comete claramente cuando un usuario de la red obtiene en forma ilegal servicios o funciones desde una computadora, o la utiliza para cometer un delito informático.

Debido a que el delito implica el uso no autorizado en lugar de acceso no autorizado, es posible reprimir a un usuario que sobrepase los límites establecidos por un servicio. El delito abarca el uso de funciones, también permite indirectamente la supresión de dato apropiados y legalmente en Internet. Los intrusos que intenten apropiarse de datos ilegalmente, tendrán necesariamente que alcanzarlos primero a través del sistema de cómputo y al hacerlo utilizarán servicios telemáticos o de computo no autorizado.

El delito de uso mal intencionado de computadoras no sólo abarca la destrucción o modificación de datos, sino también, todos los actos que reduzcan el rendimiento de esos actos o que interrumpan temporal o permanentemente el acceso a ellos.

La interceptación de mensajes privados, incluyendo mensajes de telecomunicaciones, también se considera un delito en Canadá.

Ahora bien tomando en cuenta la presencia de estos delitos en los países mencionados debemos dar un panorama de estos ilícitos y su trascendencia geográfica, jurídica e histórica.

GRAN BRETAÑA

En 1988, varios "hackers" consiguieron entrar en los ordenadores de siete universidades de Gran Bretaña, la de Londres incluida. Para resolver este

"crimen", la policía necesito la ayuda técnica de un asesor informático, Robert Jones. Una vez arrestado un sospechoso, las pruebas se analizaron durante un año y medio antes de presentarlas ante el tribunal, que lo condenó a un año de prisión. Después de varias colaboraciones más, Scotland Yard propuso la creación de un centro universitario dedicado a la investigación de estos casos. El Centro de Investigación de Delitos Informáticos, adscrito al Queen Mary & Westfield College, se creó a principios de 1996 y el abogado Ian Walden, experto en la legislación de tecnología de la información, es su director.

El Centro obtiene fondos del Gobierno y se dedica a la investigación y la asesoría en el campo de los delitos informáticos, así como a impartir cursos de formación en la materia para policías, fiscales, abogados y cualquier interesado.

En el caso "Price" se investigó la acción de un joven hacker que accedía gratuitamente al sistema telefónico chileno y desde allí consiguió entrar en los ordenadores del Ministerio de Defensa de Estados Unidos. Copió archivos que no eran materia reservada, pero si investigaciones de temas delicados y provocó tanto daño y caos que toda la red norteamericana se cerró durante un corto período de tiempo. Y todo desde Londres. No trabajaba solo, porque siempre hay equipos de diferentes países que intercambian información.

ESTADOS UNIDOS

En 1997 se publica el libro "Takedown" de Tsutomu Shimomura y John Markoff de la editorial El País - Aguilar de 464 páginas. En el se relatan la búsqueda y captura de un escurridizo hacker que domina el arte del "IP-spoofing", que consiste en producir falsos números IP para ser reconocido por otras máquinas conectadas y pasearse por su interior. Es un reportaje novelado, contado en primera persona por el experto en seguridad Tsutomu Shimomura, que fue saqueado por el hacker en plena Navidad del 94 y dedicó medio año a detenerle. Lo escribió junto a John Markoff, un periodista del New York Times que había seguido el caso.

Microsoft anunció firmes avances en su lucha contra el delito informático durante el año fiscal de 1997, que incluye el embargo de cerca de 100.000 copias ilegales o programas falsos, CD-ROM y dispositivos hardware, procedentes de canales de distribución europeos y con un valor de más de 23 millones de dólares.

El 80% de los incidentes de seguridad suelen ocurrir "desde dentro", es decir, producidas por cuando se despide a un empleado de mala manera o se trata a algún alumno de forma poco coherente. Estos suelen crear puertas traseras creando cuentas con passwords que luego distribuyen o que son anónimas. Estas cuentas suelen disponer de bastantes privilegios sobre el sistema.

Según Julia A. Conley , agente especial del F. B. I., -"Hay una cuestión ética a resolver, que ha surgido hace poco y que está relacionada con las compañías que contratan a antiguos piratas informáticos como expertos de seguridad. Es un

problema porque estas personas reclamadas intentan crear una reputación de pirata informático para conseguir un buen trabajo. Esto quiere decir que tenemos individuos encargados de sistemas de seguridad que han tenido que violar la ley con el fin de obtener un empleo"-.

Unos de los phreakers más famosos fue el "Capitán Crunch", que eligió su apodo debido a la marca de cereales Cap'n Crunch. Esta marca regalaba en los años ochenta unos silbatos de plástico en sus cajas. Este phreaker descubrió que con una ligera modificación, estos silbatos daban una frecuencia de 2.600 ciclos, con la que engañaba a la central haciéndole creer que había colgado el auricular, pero en realidad estaba hablando y gratis.

Los Hackers se cuelan en la WEB de la N.A.S.A. se llaman H4G13 y han sido los primeros en lograr romper los códigos de seguridad que protegen el web principal de la N.A.S.A. (National Aeronautics and Space Administration), con el objetivo de demostrar hasta donde pueden llegar y amenazar con más ataques si no se liberaba a un conocido grupo de hackers que están es prisión. Los hackers colocaron un manifiesto, que estuvo presente durante media hora en el sitio gubernamental americano, en el que amenazan con asaltar próximamente a la sociedad anónima denominada "América", fundada para promover el uso comercial de Internet. Aunque éste ha sido el primer ataque con éxito al sitio de la N.A.S.A., este organismo ya ha sufrido algunos percances por culpa de hackers que la consideran como uno de sus objetivos más estimulantes. En 1987 el Chaos Computer Club entró en la red SPAN de la N.A.S.A. y, en el 90, otros vándalos

informáticos de Denver se colaron en los ordenadores que la agencia tiene en Huntsville y Greenbelt.

La noche de las elecciones norteamericanas de 1996 hubo un incremento notable del uso de la red que provoco una disminución de la velocidad de acceso a algunos sitios, en el Web del New York Times era absolutamente imposible entrar, ya que había sufrido un ataque de hackers. Alguien había programado un ordenador para que inundara el servidor del rotativo mediante el constante envío de falsos mensajes de autentificación, ocasionando 10 veces más hits de lo normal. Una técnica tan fácil que ni siquiera las revistas on line de hackers como 2600 o Phrack la consideraba digna de uso, pero tan efectiva que ha sido descrita como - táctica terrorista- por Stephen Hansen, jefe de ordenadores de la Universidad de Stanford.

El Subcomité Permanente de Investigaciones del Senado norteamericano estimó el costo producido por ataques a sistemas informáticos de empresas, durante el año 1995, en 800 millones de dólares, sin contar las pérdidas que muchos bancos no declaran por evitar la mala propaganda que ello supone.

ALEMANIA

En 1990 dos jóvenes alemanes apodados Bach y Handel descubrieron un agujero

en el sistema VAX de una de las empresas de software más importantes de Alemania, Scion. En muchos sistemas VAX actuales, el error está aún por subsanarse, debido a la experiencia o la decidía de los administradores de sistemas.

En 1996 el Grupo Antipiratería de la empresa de software Novell, informaba de la captura de un individuo que respondía al alias de "El Pirata". Con la colaboración de la Policía de Zurich, Novell consiguió atrapar a este cracker que ofrecía productos de la compañía a usuarios de Internet de forma ilegal por valor de 60.000 dólares, junto con software comercial de otros miembros de la B.S.A. (Business Software Aliance). Se localizaron también instrucciones para realizar operaciones fraudulentas con tarjetas de crédito. Sus acciones le pueden llevar a ser condenado un máximo de tres años y/o una multa de 10 millones de Marcos por ello. Martín Smith, el Director de Programas de Licencias de Novell para Europa, Oriente Medio y África, lo valora así: "Éste es un caso clave para el futuro de la industria del software. Desde hoy los individuos y organizaciones que distribuyen software ilegal en Internet saben que pueden ser capturados y procesados."

DINAMARCA

Las computadoras que numerosas bibliotecas de todo el mundo ponen a libre disposición del público están siendo usadas en grado cada vez mayor para la realización de actividades delictivas.

La policía de Dinamarca ha detectado el uso sistemático de computadoras instaladas en bibliotecas públicas en la comisión de delitos. En ese país, cualquier persona puede usar las computadoras con conexión a Internet en las bibliotecas sin necesidad de identificarse.

Al usar una computadora pública, el delincuente elimina la posibilidad de ser ubicado luego de haber realizado una actividad informática ilícita. En la mayoría de los casos, la policía estará en condiciones de seguir un rastro digital hasta dar con el paradero de la computadora, con la salvedad de que esta vez la pista se perderá al llegar a una computadora pública situada en una biblioteca.

Según la policía danesa, el principal problema está representado por los piratas informáticos, que han relevado en importancia a los depravados que se valen de la red para establecer contactos e intercambiar imágenes de pornografía infantil.
Otros delitos que buscan el ciberespacio como instancia de acción y encubrimiento son el espionaje industrial, venta de especies robadas, falsificaciones y usurpación de identidad.

2.4 DELITOS INFORMÁTICOS COMETIDOS A TRAVES DE INTERNET

El ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes. El efecto de aldea global generado por el entramado de redes y la proliferación de nodos en todo el planeta ayuda a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red. A las reconocidas ventajas que ello supone se unen las distorsiones y los malos usos que pueden tener lugar en el sistema y que confirman una vez más que el mal no está en el medio utilizado sino en la persona que lo utiliza.

Actualmente se está produciendo un intenso debate respecto a la necesidad de prevenir y sancionar estos malos usos en la red de redes Internet y el objetivo de este punto es localizar las distorsiones más habituales que se producen y resumir los argumentos que se han dado en contra y a favor de una regulación.

1. ARGUMENTOS EN CONTRA DE LA REGULACIÓN

Frente a la corriente reguladora se levantan los partidarios de que ciertas áreas queden libres del intervencionismo o proteccionismo estatal. Entre los argumentos más utilizados figuran el derecho a la intimidad y la libertad de expresión.

2. ARGUMENTOS A FAVOR DE LA REGULACIÓN:

Los partidarios de la regulación se apoyan en la tesis de que las redes de telecomunicaciones como Internet han generado un submundo en el que los delitos son difíciles de perseguir debido a la propia naturaleza del entorno y a la falta de tipificación de las modalidades de comisión y de los medios empleados. Entre los delitos, infracciones administrativas y malos usos que se pueden llevar a cabo en la llamada infraestructura de la información, destacan, sin ánimo de clasificarlos, los siguientes:

Acceso no autorizado: La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático no disponen en algunos países de preceptos que permitan su persecución.

Infracción de los derechos de autor: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio en el ámbito jurisprudencial. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line o de un sysop respecto a las copias ilegales introducidas en el sistema.

Mientras un tribunal condenó a un sysop porque en su BBS había imágenes scaneadas de la revista Playboy, en el caso La Macchia, el administrador del sistema fue hallado no responsable de las copias de programas que albergaba su BBS. El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a un "upload" de un programa o fichero que infrinja los derechos de autor de terceros.

Infracción del Copyright de bases de datos: No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohibe el replicado de la base de datos o la copia masiva de información.

Interceptación de e-mail: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

Fraudes Electrónicos: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de fraude, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra.

No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

Transferencias de fondos: Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema Informático. A pesar de que en algunas legislaciones y en sentencias aisladas se ha asimilado el uso de passwords y tarjetas electrónicas falsificadas al empleo de llaves falsas, calificando dicha conducta como robo, existe todavía una falta de uniformidad en la materia.

Espionaje: Se ha dado casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera. Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

Espionaje industrial: También se han dado casos de accesos no autorizados a

sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y know how estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

Terrorismo: La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación en el ámbito internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

Narcotráfico: Tanto el Buró Federal de investigación (F.B.I.) como el Fiscal General de los Estados Unidos de Norteamérica han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con sus respectivos "cárteles". También se ha detectado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas de drogas. El notable avance de las técnicas de encriptación permite el envío de mensajes que, a pesar de ser interceptados, pueden resultar indescifrables para los investigadores policiales. Debe tenerse en cuenta que sólo en 1994 los jueces americanos concedieron 1.154 órdenes de vigilancia electrónica, de las cuales un importante número tuvo resultado negativo

a causa de la utilización de técnicas de encriptación avanzadas. Por ello, tanto el F.B.I. como los fiscales americanos reclaman que todos los programas de encriptación generen puertas traseras que permitan a los investigadores acceder al contenido del mensaje.

Mal uso: cybertorts Usos comerciales no éticos: Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mailings electrónicos" al colectivo de usuarios de un gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red. Actos parasitarios: Algunos usuarios incapaces de integrarse en grupos de discusión o foros de debate on-line, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc. Aunque la mayoría de estas conductas están previstas por los suministradores de servicios on-line, disolviendo el contrato con los reincidentes, existen algunos partidarios de que se establezcan normas para sancionar estos actos.

Obscenidades: Así mismo establece la polémica generada por el proyecto de ley del senador Exon en Estados Unidos de América respecto a una Communications Decency Act. 1.4 Efectos transfronterizos

Otro de los aspectos sobre los que se reclama una regulación es el de la competencia jurisdiccional en el caso de actos realizados en un país determinado pero que, debido a la extensión de la red, tienen sus efectos en otro país. Aunque el derecho internacional da solución a este tipo de conflictos, existen diversos criterios respecto a la determinación del lugar en el que se ha producido la infracción.

Así como en una radiodifusión vía satélite existe una conducta activa de emisión, sujeta a unas normas especiales, la introducción de una obra infractora en un host conectado a Internet. ¿Debe entenderse también como un acto de difusión o comunicación pública? La conducta activa o pasiva del presunto infractor es determinante para apreciar la existencia de la infracción y la competencia jurisdiccional. Si hacemos una comparación de las autopistas de la información con las autopistas de asfalto, deberíamos reconocer que no es lo mismo enviar camiones de reparto a todos los países y ciudades con vías de acceso, que tener una tienda abierta al lado de la autopista.

Un ejemplo de conducta pasiva sería el caso de Phil Zimmermann, investigado por exportar tecnología de doble uso a otros países. Zimmerman se limitó a introducir su programa de encriptación de clave pública P.G.P. (Pretty Good Privacy) en hosts que se hallaban dentro del territorio de los E.U.A., pero al estar estos hosts conectados a Internet, todos los países conectados a la red pudieron obtener una

copia del programa. Zimmermann recibió numerosos mensajes de felicitación y agradecimiento desde países con embargo comercial y tecnológico. Este caso ha acabado siendo un exponente de la lucha entre el poder intervencionista del Estado y el derecho a intimidad de la persona, como más adelante veremos.

Un ejemplo de conducta activa sería remitir una recopilación de imágenes pornográficas scaneadas a los mailbox de un país en que dicho tráfico estuviese prohibido.

CAPÍTULO III.

ANALISIS COMPARADO EN MATERIA DE DELITOS INFORMÁTICOS.

3.1 LEGISLACIÓN EN MÉXICO: CÓDIGO PENAL DEL ESTADO DE SINALOA, MÉXICO.

Para el desarrollo de este capítulo se analizará la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos En este entendido, consideramos pertinente recurrir al Código Penal del Estado de Sinaloa y a la Ley Federal de Derechos de Autor y Código Penal para el Distrito Federal en Materia del Fuero común y para toda la República en materia del Fuero Federal.

CÓDIGO PENAL DEL ESTADO DE SINALOA

Ante la importancia que tiene el Delito Informático, en el Estado de Sinaloa, el Congreso Local ha considerado pertinente legislar sobre la materia, estimando conveniente transcribir íntegramente el texto que aparece en el Título décimo capítulo V del 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 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 del delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

Estimo que el Congreso Estatal de Sinaloa al legislar, sobre el delito informático, los ubico como un delito patrimonial dada la naturaleza de los derechos que sé transgreden con la comisión de estos ilícitos, pero a su vez, cabe señalar 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 libertad de expresión.

Derecho a la intimidad

Uno de los derechos más defendidos en los países en los que ha habido una gran implantación de los sistemas informáticos en la gestión de los datos de los ciudadanos por parte de la Administración, ha sido el derecho de la persona a que su intimidad no sea vulnerada por un abuso de estos medios. La protección de este derecho ha generado preceptos de rango constitucional en muchos países. En España, el artículo 18 del Código Penal garantiza el secreto de las comunicaciones y abre la posibilidad de que la Ley limite el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Del desarrollo de este precepto ha surgido hasta ahora la LORTAD como instrumento destinado a evitar que mediante el tratamiento automatizado de los datos se llegue a obtener el perfil de una persona, sus aficiones y sus hábitos. Con ello se reconoce que el uso de las tecnologías de

la información permite una rapidez en la manipulación de datos que era impensable con el empleo de medios manuales o analógicos. En la discusión de la LORTAD se llegó a establecer la comparación de que los sistemas manuales equivalían a pescar con caña y los informáticos a pescar con red.

La misma frase se ha repetido al hablar sobre el poder del Estado al investigar las transmisiones efectuadas en la infraestructura de la información, y concretamente al interceptar y leer el e-mail. En la declaración de Phill Zimmermann ante el Subcomité de Política Económica, Comercio y Medio Ambiente de la Cámara de Representantes de los Estados Unidos de América, puede leerse: "En el pasado, si el Gobierno quería violar la intimidad de los ciudadanos corrientes, tenía que gastar sus recursos en interceptar, abrir al vapor y leer el correo y escuchar, grabar y transcribir las conversaciones telefónicas. Eso era como pescar con caña, de uno en uno. Por el contrario, los mensajes de e-mail son más fáciles de interceptar y se pueden scanear a gran escala, buscando palabras interesantes. Esto es como pescar con red, existiendo una diferencia orwelliana cuantitativa y cualitativa para la salud de la democracia".

Con argumentos similares se está defendiendo la idea de que si los avances tecnológicos han creado un ciberespacio en el que cualquiera puede expresarse y comunicarse sin temor a ser oído por otros, el poder del Estado no debería ampliarse hasta poder controlar este nuevo mundo.

Por de pronto, el servicio secreto norteamericano ya ha sido condenado por introducirse sin mandamiento judicial en la BBS Esteve Jackson Games y leer el e-mail en ella depositado. El servicio secreto ha tenido que pagar una indemnización de 50.000 dólares al propietario de la BBS y 1.000 dólares a cada usuario de la misma, por haber vulnerado su intimidad.

Libertad de expresión

Pocas propuestas de ley han generado tanta discusión en Internet como la Communications Decency Act. Los detractores de este proyecto sostienen que no sólo prohibiría conversaciones públicas de contenido "obsceno, lascivo, sucio o indecente" sino incluso las de ámbito privado entre dos personas, con la posibilidad de sancionar al proveedor del servicio on-line. Los usuarios de Internet americanos se niegan a tener que hablar constantemente como si estuviesen en un entierro. La aplicación de esta ley, además de ser un importante obstáculo para la libertad de expresión, exigiría una enorme inversión en la monitorización y vigilancia del sistema y generaría constantes intromisiones en la intimidad de los ciudadanos. Durante el mes de abril y mayo de 1995, ha habido un importante movimiento para conseguir firmas de oposición a este proyecto. La dirección donde debían enviarse los mensajes era s314-petition@netcom.com

Una corriente de usuarios de la red considera que el derecho a la información está por encima de otros derechos como la propiedad intelectual, la propiedad de los datos el secreto que se da al know how. Los partidarios de esta idea consideran

que cualquier tipo de obra introducida en la red debería pertenecer al dominio público, y solicitan la inaplicabilidad de los derechos de autor y la supresión de fronteras en el ciberespacio para permitir el libre flujo de la información en todo el planeta.

LEY FEDERAL DEL DERECHO DE AUTOR

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

Sobre el particular, y por considerar de interés el contenido de la exposición de motivos cuando esta ley se presentó ante la Cámara de Diputados, a continuación se presentan algunos comentarios pertinentes respecto a los elementos que deben contemplarse en la atención a la problemática sobre los derechos de autor.

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.

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 ley Federal de Derechos de Autor, los cuales establecen lo siguiente:

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

Por su parte, el artículo 231, fracciones II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por esta Ley" y *"usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular"*.

La redacción de estas fracciones 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.

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

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

Esto, a la larga podría traer implicaciones muy desventajosas para México, entre las que podemos citar: la pérdida de prestigio en el ámbito 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 las implicaciones que traería aparejadas, justifica su regulación penal.

En otro orden, el Artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información.

Así, el 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.

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

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

Por otra parte, 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.
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 de la siguiente forma:

" Artículo 231 ...

.III Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros protegidos por los derechos de autor o

por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta Ley".

3.2 LEGISLACIÓN EXTRANJERA.

LEGISLACIÓN EN OTROS PAÍSES

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, a continuación se presenta los siguientes casos particulares:

ALEMANIA

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

- Espionaje de datos (202 a)
- Estafa informática (263 a)
- Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271, 273)
- Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Sabotaje informático (303 b). Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b)
- Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial, en el engaño de la computadora, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una

elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

- Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los Países Escandinavos y en Austria.
- En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.
- En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.
- Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo

constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos.

- Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.
- En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

AUSTRIA

- Ley de reforma del Código Penal de 22 de diciembre de 1987
- Esta ley contempla los siguientes delitos:
- Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
- Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la

introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

CHILE

El Código Penal Chileno en la parte relativa a Delitos Informáticos, establece los siguientes:

- Ley Relativa a Delitos Informáticos
- Artículo 1º. - El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
- Si como consecuencia de estas conductas se afectare los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.
- Artículo 2º. - El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

- Artículo 3º. - El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.
- Artículo 4º. - El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".

FRANCIA

La Ley Francesa número 88-19 de 5 de enero de 1988 sobre el delito de fraude informático, establece como tales los siguientes:

- Acceso fraudulento a un sistema de elaboración de datos(462-2). - En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje informático (462-3). - En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos (462-4). - En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o

modifique los datos que este contiene o los modos de tratamiento o de transmisión.

- Falsificación de documentos informatizados (462-5). - En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

ESTADOS UNIDOS

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986.

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

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

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

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

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

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

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

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o

gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

ESPAÑA

CÓDIGO PENAL ESPAÑOL

DELITOS RELACIONADOS CON LAS TECNOLOGIAS DE LA INFORMACIÓN

TÍTULO X.

Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

CAPÍTULO I

Del descubrimiento y revelación de secretos

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 248.

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

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 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.

CAPÍTULO XI

DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL E INDUSTRIAL, AL MERCADO Y A LOS CONSUMIDORES.

Sección 1ª. - DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL.

Artículo 270.

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

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.

CAPÍTULO III

Disposición general

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 paso 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.

3.3. **TRATADOS INTERNACIONALES.**

ORGANISMOS INTERNACIONALES

El objetivo de este capítulo es presentar todos aquellos elementos que han sido considerados tanto por organismos gubernamentales internacionales así como por diferentes Estados, para enfrentar la problemática de los *delitos informáticos* a fin de que contribuyan al desarrollo de este trabajo.

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

En un primer término, debe considerarse que en 1983, la **O.C.D.E.** Inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

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

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

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

La mayoría de los miembros de la Comisión Política de Información, Computadoras y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos *(Lista optativa o facultativa)*, espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.
Con objeto de que se finalizara la preparación del informe de la O.C.D.E, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía

conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la **O.C.D.E.** se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité, Especial de Expertos sobre Delitos relacionados con el empleo de las computadoras, del Comité Europeo para los problemas de la delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del *delito informático.*

Una vez desarrollado todo este proceso de elaboración de las normas en el ámbito continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras... " y en particular las directrices para los legisladores nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso

indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

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

En este contexto, consideramos que si bien este tipo de organismos gubernamentales ha pretendido desarrollar normas que regulen la materia de *delitos informáticos*, ello es resultado de las características propias de los países que los integran, quienes, comparados con México u otras partes del mundo, tienen un mayor grado de informatización y han enfrentado de forma concreta las consecuencias de ese tipo de delitos.

Por otra parte, en el ámbito de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la O. C. D. E. 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 de que los *delitos informáticos* eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad en el uso de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

Partiendo del estudio comparativo de las medidas que se han adoptado en el ámbito internacional para atender esta problemática, deben señalarse los

problemas que enfrenta la cooperación internacional en la esfera del *delito informático* y el derecho penal, a saber:

a) La falta de consenso sobre lo que son los *delitos informáticos;*
b) La falta de definición jurídica de la conducta delictiva;
c) La falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal;
d) La falta de armonización para investigaciones nacionales de *delitos informáticos.*
e) Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición.

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

En otro orden de ideas, debe mencionarse que la *Asociación Internacional de Derecho Penal* durante un coloquio celebrado en Wurzburgo en 1992, adoptó

diversas recomendaciones respecto a los *delitos informáticos*. Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta que punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

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

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

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

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

Con objeto de que se finalizara la preparación del informe de la O. C. D. E., el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía

conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la O. C. D. E. se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité, Especial de Expertos sobre Delitos relacionados con el empleo de las computadoras, del Comité Europeo para los problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estados pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Por otra parte, en el ámbito de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU) y 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.

Por todo ello, en vista de que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

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

delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados. Internacionales de extradición.

TRATADO DE LIBRE COMERCIO DE AMERICA DEL NORTE

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.

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse el contenido del párrafo 1 del artículo 1717 titulado procedimientos y sanciones penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

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 Tratado de libre comercio.

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.

CAPÍTULO IV

LA TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL PARA EL DISTRITO FEDERAL

4.1 LA NECESIDAD DE LEGISLAR EN MATERIA DE DELITOS INFORMÁTICOS EN MÉXICO.

En este fin de siglo la expansión y considerable demanda entre la población mundial, de las computadoras personales, dan como resultado un constante incremento en el número de usuarios y como consecuencia de ello el potencial delictivo aumenta en toda la esfera relacionada con la informática, es decir, la proliferación de centrales de computo, el uso del Internet y demás medios computarizados accesados por vía telefónica, son los objetos que se ven principalmente amenazados por delincuentes con habilidad en materia informática.

Uno de los más preocupantes campos amenazados por el delito informático es la transferencia de fondos, la problemática bancaria, el derecho a la intimidad, el patrimonio, entre otros, los cuales son causados por la interferencia indebida de los medios electrónicos, por los llamados delincuentes informáticos.

El abaratamiento de los equipos de cómputo, la proliferación de servidores de Internet en México y la necesaria dependencia de la iniciativa privada y del aparato del gobierno a estar "en línea", son los ingredientes potenciales para un

personalidad, las cuales se distinguen por un alto coeficiente intelectual, una introversión excesiva y una impunidad determinada por las propias leyes.

Hay otro elemento jurídico a determinar en la posible comisión de un delito informático y ese es el tiempo, ya que en segundos puede cambiar la información, no tan sólo de dueño sino también de jurisdicción. Además para cometerse, el sujeto activo, ni siquiera tiene que estar presente ante el equipo computacional del que sé este aprovechando, puede ejecutarse a distancia y aún más llega a ser tan sofisticado, que accesando al sistema puede eliminar todos los movimientos del " Delito Informático"

La tipificación del "Delito Informático" puede resumirse en las siguientes categorías:

a) Fraudes Informáticos;
b) Falsificaciones Informáticas;
c) Daños a datos computarizados;
d) Sabotaje Informático;
e) Acceso no autorizado a servicios y sistemas informáticos;
f) Robo Informático;
g) Pornografía Infantil;

Como lo he venido señalando ,apareció en las últimas cuatro décadas un nuevo acto delincuencial y al cometerlo, un nuevo delincuente que no usa herramientas típicas, antes conocidas como cortadores de alambres, desarmadores e inclusive armas de fuego; en su lugar maneja y trasgiversa la información.

El nuevo delincuente no necesita forzar puertas o ventanas para entrar en la propiedad de otros, lo único que requiere es el teclado de una computadora y un "Módem" telefónico para cometer el delito informático.

La comisión del delito, todavía se hace más fácil cuando se trata de un programador, quien pudiera decirse que tiene " la combinación de la caja fuerte" (es decir de la información en computadora o sistema).

Algunas de las conductas ilegales posibles con las computadoras, los sistemas y otros equipos aleatorios son:

a) Infringimiento de los derechos de autor con la usurpación de programas originales.

b) Interceptación del correo electrónico como en el caso de la información bancaria o petrolera, etc.

c) Robo de propiedad informática contenida en los discos, en los programas, los equipos, las cintas, etc.

Los delincuentes informáticos proliferan y aunque parezca un contrasentido, tendremos que agradecerles a ellos, el que presionen y pongan en dinámica a grupos interesados en contrarrestar la delincuencia. Ellos hacen resaltar los vicios comerciales, que solamente funcionan bajo la presión competitiva, imponiéndoles un grado de flexibilidad y sin contemplar y aún rebatir y evitar la introducción de restricciones o medidas de seguridad en las conductas.

Como ejemplo de lo dicho señalaremos las conductas de los altos ejecutivos, quienes están generalmente ajenos al "misterio" de la informática y dejan operar libremente a su técnico en turno, con el objeto de no confesar su propia ineptitud en el conocimiento necesario sobre los modernos métodos de computación e informática, especialmente cuando se enlazan con los grandes sistemas de comunicación.

Este sólo hecho pondría de inmediato a los altos ejecutivos en la lista de "capacitación requerida " y también en la otra enumeración más importante: La lista de "negligencia contributaria" para que los delitos puedan cometerse.

Otra omisión que cometen los altos ejecutivos y sus empresas, las que pueden ser públicas o privadas; es la de no reportar el ilícito cuando ocurre el delito informático, denuncia que es obligatoria y que al no hacerla, contribuyen a que siga proliferando la delincuencia, ya que no se logra catalogar a los personajes dedicados al robo, distorsión y fraude en las comunicaciones informáticas.

Las razones tras las cuales se escudan los altos directivos para no reportar el delito informático son variadas, pero se fundamentan en que ellos consideran y con razón, que resultaría deshonroso para su gestión directiva.

Primeramente demostraría si se reportara el ilícito, el que no se establecieron precauciones adecuadas descubriendo inmediatamente su negligencia contributaria y como resultado provocando la desconfianza de sus cuenta habientes.

Todas estas reticencias de los altos ejecutivos, desde luego resultan contrarias a un bien público de jerarquía mayor, como resultaría ser la protección legal.

Hubo en otras épocas, la posibilidad de proteger bienes materiales de una corporación o de una persona, con bardas altas que sirvieran de obstáculo impenetrable; pero en la época de las computadoras y el uso informático en general, ya no resulta viable, por ello, mencionaremos aquí algunos pasos preventivos que los estudiosos del Derecho señalan para iniciar una Ley que enmarque a la informática.

Primeramente esa Ley sería preventiva, para después desenvolver sus demás campos de acción en "El Derecho Informático".

Una medida preventiva podrá constituirse con la creación de los Códigos Éticos para los involucrados en informática.

Por ejemplo: Los más altos ejecutivos tienen la obligación de prever posibles atentados delictivos con el equipo de uso de su jurisdicción, pero generalmente delegan esa obligación al programador, porque ellos mismos, los directivos, no saben nada o muy poco del alcance real de un sistema. De esto se deriva que "el programador" podría decirse que: conoce la debilidad del sistema con los programas mismos que él diseñó y esta accesibilidad los hace más posibles delincuentes.

Con un Código de Ética, para ambos personajes: el alto ejecutivo y el programador, este último tendría la obligación de actuar en el desempeño de su trabajo, también como ingeniero, como auditor y como jurista, vigilándose a sí mismo.

Por la otra parte, el alto ejecutivo, se obligaría a capacitarse para el manejo del sistema y probar que su prevención fuese efectiva para evitar la comisión del Delito Informático o de otra forma quedar como negligente en sus funciones.

Otra medida pertinente de carácter preventivo, será el proponerse implantar un salvoconducto de entrada al sistema ("password o clave de acceso") en una longitud mínima de cuatro letras preferentemente una deberá cambiarse cuando

se considere que hubiera un peligro de ser descifrado, o hacer cambios periódicamente para desconcertar a los buscadores delincuentes.

El manejo de la información dentro de las organizaciones es esencial para sus operaciones, esta información es resultado de la labor de la institución para recabarla, clasificarla, almacenarla y procesar mas información, esta situación convierte a la información en un recurso invaluable ya que la pérdida de la misma, la fuga y su caída en manos de la competencia o de enemigos pueden ocasionar daños, pérdida de mercado o recursos capitalizables, prestigio y aún llevar una empresa a la quiebra o pérdida de la credibilidad de las políticas de la administración pública.

Es por eso que se convierte en imprescindible el normar y legislar en las empresas y los organismos públicos sobre la tipificación de los delitos informáticos.

Los fraudes electrónicos, el robo de información, es cada vez mayor la participación de los individuos sin profesionalismo y ética que no manejan de manera prudente y segura la información y que generan además código nocivo que afecta por igual a ambientes de cómputo y redes de comunicaciones con daño a los datos, también debe ser tipificado como delito.

El material aquí presentado fundamentalmente se centra en los actos que se definen por sí mismo como actividades perjudiciales y riesgosas.

La presente propuesta no es una posición personal del autor, es una recopilación de políticas que cubren los tópicos del tema y se presentan como una aportación que puede o no reflejar la opinión de otras personas que laboran dentro del área de seguridad informática.

4.2 LA CREACIÓN DE UN TÍTULO ESPECIAL SOBRE LOS DELITOS INFORMÁTICOS.

Ante la proliferación de los Delitos Informáticos, los cuales propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, y por lo tanto surge la necesidad en nuestra legislación penal de tipificar los Delitos Informáticos, puesto que es vital para la protección de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el Estado que legalmente utilizan las computadoras.

Como lo hemos mencionado a lo largo del presente estudio, en algunos casos relacionados con los excesos de la computación deben ser combatidos con medidas jurídico-penales.

No obstante, para entender ciertos comportamientos merecedores de sanción con los medios del Derecho penal tradicional, existen, al menos en parte, grandes dificultades. Estas provienen en buena parte, de la prohibición jurídico penal de

analogía y en ocasiones, son insuperables por la vía jurisprudencial. De esto surge la necesidad de adoptar medidas legislativas en materia penal en el mundo de la informática.

Pocos son los países que disponen de una legislación penal adecuada en materia informática para enfrentar el problema en particular.

Para tales efectos, se realiza más adelante una propuesta sobre el sostenido de los nuevos tipos penales, los cuales constituyen conductas antisociales preponderantemente contra los bienes patrimoniales.

Los bienes jurídicos a proteger por los nuevos tipos penales objeto de esta reforma, deberán garantizar por una parte la confiabilidad, seguridad e invulnerabilidad de los sistemas de informática y computacionales y; por otra los derechos de las personas en sus vertientes moral y patrimonial.

Los nuevos tipos penales deberán garantizar los importantes bienes jurídicos mencionados en la presente investigación, los cuales incluyen la protección de la intimidad de las personas, la protección de la información ante instrucciones no autorizadas, la salvaguarda contra la destrucción, el daño o la alteración de la

información; y la mayor protección frente a un número abierto de conductas similares a las mencionadas. Muy pocas de ellas ya se prevén en leyes especiales, la mayoría de ellas serán previstas por primera vez en este trabajo de tesis.

La informática es un fenómeno multifacético de realidad contemporánea. Su difusión se ha extendido rápidamente sobre la economía, la política, la organización del trabajo y el derecho. La problemática que plantea la gestación y diseminación de la que puede llamarse "la herramienta" de nuestro siglo, es tan amplia, compleja y novedosa que su examen teórico, así como su comprensión y encuadramiento a los fines de la formulación de políticas, presenta un desafío infrecuente para investigadores de todas las disciplinas, gobiernos, y actores económicos y sociales. Tal desafío es, ante todo, de orden político, en cuanto requiere que cada país tome una posición frente a este revolucionario fenómeno y opte por alguna de las diversas alternativas que objetivamente abren las condiciones tecnológicas y económicas en que aquel se desenvuelve.

Paralelamente, y como consecuencia inmediata de estos avances, a través del tiempo el delito fue mutando, alternando su estructura, modificando y adquiriendo distintos perfiles. Es cierto, y sabemos, que el crimen existe desde que existe el hombre. Sin embargo, el progreso tecnológico hace más dificultoso su control y penalización. Esa dificultad radica, en primera medida, en las sofisticadas formas que adquiere el delito con ayuda de la tecnología. En este sentido, los sistemas

informáticos logran potencializar las posibilidades de las distintas modalidades delictivas denominadas tradicionales. Las inimaginables posibilidades que estos sistemas aportan al desenvolvimiento del hombre en todas sus esferas de actuación, exteriorizan su faceta indeseable en el nacimiento de nuevas modalidades delictivas que radica su particularidad en su vinculación con los sistemas informáticos y en la potencialidad dañosa que esta herramienta posee en su uso ilícito. Podemos decir entonces que con el desarrollo de la informática, hace aparición un nuevo tipo de delincuencia, sofisticada, de calidad superior podríamos decir, suficientemente capaz en si misma, de aparejar nuevos problemas al derecho penal y a la administración de justicia. Esta nueva categoría, son los llamados " delitos informáticos".

¿Que hacer entonces frente a esta problemática? Es evidente que como punto inicial se presenta el comprender que es necesario generar marcos legales que reglamenten y delimiten el manejo usual de los sistemas informáticos, lo que tiene una directa relación con la naturaleza humana y las normas de convivencia civilizada. Los aspectos de delitos con intervención relevante de medios informáticos, se encuentran aun difusos y exigen al menos una primera aproximación que supere el mero traslado de las situaciones "comunes", al campo de la computación; existe una amplia cantidad de características y mecánicas propias, inequívocas y totalmente representativas de las nuevas tecnologías y su influencia en la sociedad.

Observando nuestra actualidad legislativa, se denota una gran diferencia entre las previsiones de la ley y la realidad tecnológica actual, observándose un vacío normativo que penalmente significaría, en muchas ocasiones, la impunidad. La informática plantea al jurista el desafío de adecuar el cuerpo normativo y doctrinal a la evolución de la tecnología y de nuevas formas de producción y comercialización de bienes y servicios. Resulta imperioso que desde el plano de las ciencias jurídicas nos preocupemos por encontrar soluciones adecuadas a los problemas que plantean las nuevas tecnologías. Ello debe hacerse con el consenso de toda la comunidad y la participación de los posibles afectados en esas decisiones, intentando conjugar la experiencia extranjera con la situación local. No hay que perder de vista que en un mundo globalizado no es posible tomar decisiones aisladas o unilaterales, pero tampoco es posible copiar o transportar, sin mas, modelos foráneos.

A la fecha no han sido tan fructíferos los estudios que se han realizado ante esta nueva amenaza económica. Tampoco son muy conocidos los programas de prevención que se han planteado para evitar este tipo de delincuencia, o por lo menos controlarla razonablemente. Y, esto se hace difícil no solo por el silencio legislativo imperante, sino porque además, y como agravante, este tipo de delitos es muy difícil de rastrear, ya sea porque no dejan huellas en la escena del crimen, ya sea por la impotencia o inconveniencia por parte de la víctima de denunciarlos. Además, este tipo de tecnología crece día a día en forma vertiginosa, dejando atrás las no tan rápidas iniciativas legislativas. Pero lo más preocupante de toda

esta cuestión no es solo la parte económica, y los millones que como consecuencia se pierden, si tenemos en cuenta que por lo menos en cada hogar existe una computadora personal, las cuales se encuentran al alcance de cualquier niño, quienes nos sorprenden constantemente con el manejo que tienen de las mismas, y paralelamente el fácil acceso a Internet, y la invasión que en ella han hecho las paginas de pornografía, con el consiguiente riesgo que ello implica, hace cada vez mas urgente una regulación de la informática con una adecuada legislación.

De lo expuesto precedentemente se desprende que si bien algunas de las formas ilícitas que adoptan los delitos informáticos pueden encuadrar en los delitos tradicionales, la mayoría de las veces estamos ante conductas típicas propias, por lo que se hace necesario distinguir, aquellas conductas o modalidades que solamente pueden concebirse en la relación de la conducta del autor con un sistema informático (delitos informáticos propios), de aquellas que implican el empleo de un ordenador para la comisión de delitos tradicionales, pero con la peligrosidad que los adelantos tecnológicos implican (delitos informáticos impropios).

Ante estas nuevas alternativas que en el tradicional concepto de delito producen los ilícitos informáticos, ellos obligan al Estado, frente al problema concreto que significa la delincuencia, a modificar o reformular todas sus estrategias y objetivos en materia de política criminal, sea desde una perspectiva de carácter preventivo,

como también desde un sentido puramente represivo. La realidad nos demuestra que las mencionadas 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. Ahora bien, estos cambios deben ser logrados respetando el principio de constitucional de legalidad, que en todo estado de derecho debe primar.

Deben determinarse conductas prohibidas en forma clara, precisa y taxativa, estableciéndose las sanciones aplicables al caso concreto. La tipicidad previa y la prohibición de la analogía en materia penal, imponen la creación de una tipología especial delictiva, que enmarque a la delictuosidad informática como una realidad delictiva autónoma, de casi imposible solución de esas conductas en las figuras penales típicas tradicionales.

Es impostergable cubrir un vacío legal que por la diversidad de intereses comprometidos, afectara negativamente legítimos derechos que deben ser asegurados mediante políticas eficientes y progresistas. Estamos ante una nueva dimensión de la victimización que sufre nuestra sociedad en estado de impotencia para ofrecer una razonable solución al problema expuesto. La cuestión solamente podrá ser superada en la medida en que, mediante una ley especial que se introduzca en el Código Penal para el Distrito Federal, en el cual se reglamente la materia de los delitos informáticos, definiéndolos, fijando los bienes que ellos garantizan, especialmente en los delitos contra el honor, la libertad, la propiedad

intelectual y común, la seguridad de la nación y la fe publica. El tema trasciende los limites políticos del Estado, y su tratamiento exige nuevas políticas criminales, cuyo presupuesto estará dominado por estrategias de prevención, detección y/o represión de estos ilícitos. A tal fin se necesitara trabajar para neutralizar las amplias modalidades que existen en esta esfera del crimen organizado, cubriendo los vacíos legislativos existentes no solo en nuestra legislación sino además en la extranjera, buscando la coordinación y complementación en orden a la creación de un sistema que se distinga por su eficacia y cohesión.

Es el Derecho, mas allá de toda duda, el valioso instrumento creado por la cultura humana tendiente a regular la vida del individuo en sociedad y de tal modo posibilitar la convivencia fecunda, que nos permitirá adecuarnos a estas nuevas épocas. Pero esta necesidad de regulación, no debe hacernos caer en el grosero error conceptual que anida en la creencia de que cuanto más se regule la actividad humana, que cuanto más se discipline el que hacer de los ciudadanos para obligarlos a que hagan o dejen de hacer acciones contrarias a su propia voluntad, que cuanto más se restrinja y coarte su desenvolvimiento espontáneo, mejores resultados se obtendrán en orden a lograr una adecuada convivencia social. El legislador debe tomar los datos que le acerca la criminología, la que elaborando una critica sobre la base de la legislación vigente, y abundando en esa critica con los datos que le aporta la dogmática, propondrá los nuevos programas

y criterios de legislación, dentro de los parámetros de la técnica legislativa correspondiente. Desde ese punto de vista, la política criminal es el conocimiento que debe apoyar la reforma de la legislación vigente.

4.3. PROPUESTA SOBRE EL CONTENIDO DEL TÍTULO VIGÉSIMO SEPTIMO DENOMINADO "DELITOS INFORMÁTICOS"

TÍTULO VIGÉSIMO SEPTIMO

DELITOS INFORMÁTICOS

Artículo 430. Se impondrá de uno a cuatro años de prisión y de cincuenta a trescientos días multa:

I. Al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de terceros, datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos.

II. Al que sin estar autorizado, acceda por cualquier medio a los mismos datos reservados descritos en la fracción anterior, y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

III. Al que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de información transmitida por correo electrónico.

IV. Si las conductas descritas en las fracciones anteriores se realizan por personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, se impondrá una pena de prisión de tres a cinco años de prisión, y si se difunden, ceden o revelan los datos reservados, se impondrá las tres cuartas partes más de la pena.

V. Igualmente, cuando los hechos descritos en las fracciones anteriores afecten 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 tres cuartas partes más de la pena que corresponda por el delito cometido.

VI. La autoridad o servidor público, que fuera de los casos previstos por la ley, sin mediar causa legal por delito, y valiéndose de su cargo, realizare cualesquiera de las conductas descritas en las fracciones anteriores, será castigada con las penas respectivamente previstas en este artículo, así como con la inhabilitación absoluta por un periodo de seis a doce años para desempeñar otro cargo o comisión.

Artículo 431. Se aplicará la pena de dos a cinco años de prisión y multa de cincuenta a quinientos días multa al quien difunda, revele o ceda a terceros los datos o hechos descubiertos o las imágenes captadas a que se refiere el artículo anterior.

Además será castigado con las penas de prisión de uno a tres años y de trescientos a tres mil quinientos días multa, a los que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realiza la conducta descrita en el párrafo anterior.

Artículo 432. Para proceder por los delitos previstos en este capítulo será necesaria la querella de la persona agraviada o de su representante legal. Cuando sea menor de edad, incapaz o una persona desvalida, también podrá formular la querella respectiva, tanto el agraviado como quien legalmente lo represente.

Artículo 433. Se castigará con cinco a diez años de prisión y multa de quinientos a diez mil veces el salario, al que mediante dolo causen perjuicio patrimonial a un tercero, influyendo en el resultado de una elaboración de datos automáticos a través de la confección de programas, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos.

Se castigará la manipulación informática o artificio similar que concurriendo con ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero.

Artículo 434. Comete el delito de Manipulación Informática:

I Al que mediante la manipulación de datos de entrada utilizando como medio las computadoras sustraiga datos del sistema en forma ilegal;

II Al que mediante la manipulación de datos de salida, coloque datos falsos en un sistema, provocando un menoscabo en el patrimonio de un tercero;

III La manipulación de programas, modificando programas existentes en el sistema de las computadoras o insertar programas o nuevas rutinas;

El delito de manipulación informático previsto en las fracciones anteriores se castigará con pena privativa de libertad de cinco a diez años de prisión y multa de quinientos a cinco mil veces el salario mínimo vigente en el Distrito Federal.

Artículo 435. Se castigará con una pena de prisión de cinco a diez años y una multa de mil a cinco mil veces el salario mínimo vigente en el Distrito Federal, al que altere datos de los documentos almacenados en forma computarizada.

Artículo 436. Se impondrá una pena de tres a ocho años de prisión y una multa de hasta tres mil veces el salario al que borre, suprima o modifique sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema informático.

Artículo 437. Se impondrá una pena privativa de libertad de tres a ocho años y una multa hasta de cinco mil veces el salario mínimo, al que cause daños en la red, destruya datos de especial significado mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático.

Así mismo se impondrá de dos a cinco años de prisión y multa hasta de cinco mil días de salario al que maliciosamente dañe, destruya, deteriore, inutilice o altere un sistema de datos contenidos en un sistema de tratamiento de información.

Artículo 438. Se castigará con pena privativa de libertad de cinco a diez años de prisión y multa de hasta de cinco mil veces el salario mínimo, al que mediante llaves falsas, entendiendo por estas tarjetas magnéticas o perforadas así como los mandos o instrumentos de apertura a distancia, realicen el descubrimiento de claves y la utilización de sistemas específicos de alarma o guarda con el fin de apoderarse de cosas muebles ajenas.

Se castigará con pena de prisión de tres a ocho años y multa de hasta diez mil veces el salario al que difunda o utilizare a un menor de edad o a un incapaz con fines exhibicionistas o pornográficos, mediante cualquier medio informático.

Artículo 439. Se castigará con pena de seis meses a dos años de prisión a los fabricantes o comerciantes que, en sus ofertas, publicidad y servicios, hagan alegaciones falsas o manifiesten características inciertas sobre los mismos de modo que puedan causar un perjuicio grave y manifiesto a los consumidores, sin perjuicio de la pena que corresponda aplicar por la comisión de otros delitos.

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

PRIMERA. Como consecuencia de la proliferación en el campo de la computación en México y en todo el mundo, el uso indebido de la informática ha hecho que surjan nuevas conductas merecedoras del reproche social, y como consecuencia nuevos delitos en materia Informática a los cuales denominaremos: Delitos Informáticos.

SEGUNDA. La presencia de nuevas conductas penales no tradicionales en el mundo de la computación ha dado origen a la impunidad de los delincuentes en materia de Delitos Informáticos.

TERCERA. Ante la proliferación de los Delitos Informáticos surge la necesidad de Legislar sobre este tipo de ilícitos, puesto que los delitos tradicionales tales como fraude, falsificación, han pasado de ser formas tradicionales a formas no tradicionales.

CUARTA. El delito Informático implica actividades que en un primer plano, los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, fraudes, falsificaciones, sabotaje, etcétera, sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades

del uso indebido de las computadoras, lo que ha propiciado la necesidad de regulación por parte del derecho.

QUINTA. Se puede conceptualizar el Delito Informático en forma típica y atípica, entendiendo por la primera a las conductas: típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y por las segundas, actitudes ilícitas en que se tienen a las computadoras como instrumento o fin.

SEXTA. El delito informático, no es fácil de conceptualizar, en razón de que su misma denominación alude a una situación muy especial, ya que para poder hablar de delitos en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, requiere que la expresión delitos Informáticos este consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos NO ha sido objeto de tipificación.

SEPTIMA. Podemos concluir que los delitos Informáticos en México y en el mundo han alcanzado un alto índice delictivo, toda vez que la falta de tipificación de los mismos permite a los delincuentes realizarlos con toda impunidad.

OCTAVA. El sujeto activo de los delitos Informáticos es de características especiales, puesto que este posee ciertas habilidades que no presentan el denominador común de los delincuentes, esto es, los sujetos activos controlan y manejan los sistemas Informáticos a la perfección.

NOVENA. Considero que los delitos informáticos dada su naturaleza de los derechos que transgreden con la comisión de estos ilícitos, van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de estos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad y libertad de expresión.

DÉCIMA. Para aprender ciertos comportamientos merecedores de pena con los medios del Derecho Penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida de la prohibición jurídica - penal de aplicación analógica y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas.

DÉCIMA PRIMERA. La falta de preparación de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de los sujetos pasivos de denunciar este tipo de ilícitos y las consecuentes pérdidas económicas, entre otros aspectos más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra negra".

DÉCIMA SEGUNDA. Para lograr la prevención efectiva de la comisión de los delitos informáticos se requiere, en primer lugar, un análisis de las necesidades de protección y de las fuentes de peligro. 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.

DÉCIMA TERCERA. El presente trabajo no es sólo una posición personal del autor, es parte de una recopilación de políticas que cubren tópicos del tema y se presentan como una aportación que puede o no reflejar la opinión de otras personas que estudian el área de la seguridad informática.

GLOSARIO

A

ARCHIVO (fichero)

Es la base de la estructura de organización de la información en una computadora, de esta manera se puede manipular por el sistema operativo de la misma. Un archivo se compone de tres partes fundamentales: el nombre del archivo, el punto (.) y la extensión, de esta manera tenemos "ejemplo.html" (en este caso se trata de un archivo HTML cuyo nombre es ejemplo).

ASCII

(American Standard Code for Information Interchange). Es de facto el estándar del World Wide Web para el código utilizado por computadoras para representar todas las letras (mayúsculas, minúsculas, letras latinas, números, signos de puntuación, etc.). El código estándar ASCII es de 128 letras representadas por un dígito binario de 7 posiciones (7 bits), de 0000000 a 1111111.

B

BBS

Bulletin Board System (Tabla de Anuncios Electrónicos)

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 BBS solían estar en manos de aficionados, existe un número cada vez mayor de BBS conectados directamente a Internet y muchos BBS son operados actualmente por las Administraciones Públicas, por centros docentes y de investigación y por empresas: Ver: "Correo Electrónico", "Internet", "WWW"

C

CABALLO DE TROYA (Trojan Horse)

Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa. Véase virus y "gusano".

CHIP (chip, microprocesador)

La parte más importante de una computadora la representa este circuito con soporte de silicio e integrado por transistores y otros componente electrónicos.

CIBERNÉTICA.

Proviene del vocablo griego "cibernetes", que se traduce como timonel o piloto, que se refiere a la ciencia o estudio de los mecanismos de control o regulación de los sistemas mecánicos y humanos, en esta definición también se incluye a las computadoras.

COMPUTADORA.

Poderosa herramienta de trabajo electrónico capaz de procesar información para cumplir determinada tarea. Anteriormente fueron mecánicas, para posteriormente evolucionar al medio electromecánico.

COPYRIGHT (derecho de copia)

Los derechos que tiene un autor ya sea de un sistema, programa, hardware, etc. sobre todas y cada una de las obras que cree, así mismo establece las condiciones y el uso que se hará con respecto a la utilización y comercialización de las mismas. Este derecho es irrenunciable y las restricciones acerca de su uso quedan estrictamente bajo las condiciones que el autor decida. Para mostrar de manera este derecho se utiliza el símbolo: (c).

CORREO ELECTRÓNICO (e-mail)

Permite el intercambio de mensajes entre personas conectadas a una red de manera similar al correo tradicional. II Sistema mediante el cual un ordenador puede intercambiar mensaje con otros usuarios de ordenadores (o grupos de usuarios) mediante redes de comunicación. III. Sin duda alguna una de las más populares aplicaciones de Internet que ha cambiado la forma de comunicación de miles de personas en todas partes del mundo, de esta forma un usuario puede intercambiar información con otros desde puntos remotos. Se le llama así también a los mensajes que se manda a través de este medio.

COOKIE. (cuqui, espía, delator, fisgón, galletita, pastelito)

Procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para su posterior recuperación. (Proceso realizado por el Internet Explorer cuando utiliza Microsoft Network (http://www.msn.com)). En la práctica la información es proporcionada desde el visualizador al servidor del Word Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio.

CRACKER (intruso, saboteador).

Persona que trata de introducirse a un sistema sin autorización y con la intención de realizar algún tipo de daño u obtener un beneficio. II. Se define como un individuo cuyas malas intenciones lo llevan a tratar de entrar a una red o sistema burlando su seguridad. Son personas muy capaces y que cuentan con una serie de herramientas para lograr su cometido.

CYBER- (ciber-)

Se ha popularizado el uso de este término dentro de la cultura de Internet para definir conceptos relacionados con la misma como son: cibernauta, ciberespacio, etc. Su origen viene del vocablo griego "cibernao", que significa "pilotear una nave".

CYBERCULTURA (Cibercultura)

Surge con el Internet y sé retroalimenta de este medio. Se define como el conjunto de conocimientos, experiencia, etc. que se genera en los usuarios que navegan en la red. En un principio no era tan popular como lo es ahora, en la actualidad cada día se hace más común dentro de la sociedad llegando ya a ser tomada como parte de la cultura misma, aunque aún se pueden encontrar ciertos rasgos que la distinguen.

CYBERESPACIO.

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.

CYBERNAUTA (cibernauta)

Usuario que navega por la red.

D

DIRECCIÓN ELECTRÓNICA (address).

Dirección de un usuario en Internet. Por medio de ella es posible enviar correo electrónico a un usuario. Esta es única para cada usuario y se compone por el nombre login de un usuario, arroba y el nombre del servidor de correo electrónico. Por ejemplo: usuario@computadora.com.

DIRECCIÓN IP.

La dirección del protocolo de Internet (IP) es la dirección numérica de una computadora en Internet. Cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de la siguiente forma:132.248.53.10

DOMINIO.

Conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios. II. Se trata de la dirección electrónica de una página de Internet, el cual se conforma de caracteres que lo identifican de manera única. Por ejemplo tenemos que la extensión de dominio que identifica a las páginas de Internet mexicanas es el ".mx", a las alemanas ".de", etc.

Los dominios se establecen de acuerdo al uso que se le da a la computadora y al lugar donde se encuentre. Ejemplo:

.com Comercial

.edu educación (USA),

.gob gobierno (USA)

.mx México

.es España, etc.,

Los dominios a su vez se van dividiendo en otros dominios:

.gob.mx Gobierno de México

.com.mx Comercio en México

DOWNLOAD (bajar, descargar)

Se denomina en Internet al proceso de bajar información desde un servidor que se encuentra en cualquier parte del mundo a nuestra computadora.

E

e-mail.

Abreviatura de correo electrónico. Vea Correo Electrónico

F

FCC (Comisión Federal de Comunicaciones)

Su principal función es la de mantener el control sobre el amplio sector de las telecomunicaciones en los Estados Unidos.

FICHERO. Ver: Archivo.

FIRMA DIGITAL.

Se trata de un protocolo en Internet a través del cual se verifica la autentificación de un usuario y nos confirma que es quien dice ser.

FREEWARE. (programas de libre distribución, programas gratuitos, programas de dominio público)

Aplicaciones que pueden obtenerse directamente de Internet y que no es necesario pagar por su utilización.

G

GLOBALIZACIÓN (globalización, mundialización)

Se trata de un fenómeno que ha cobrado mucha fuerza a últimos días, fomentado ampliamente por el efecto Internet, en donde se traspasan fronteras y las distancias se acortan entre un país y otro en segundos, se da en todos los ámbitos, tanto social, cultural, económico, etc. Existen ya problemas generados a causa de la globalización y algunos países toman ya medidas para evitar un desajuste como el de la denominada "Tasa Tobin", que gravaría los flujos financieros internacionales.

GUSANO (worm).

Programa informático que se duplica automáticamente y propaga automáticamente. 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" en marzo de 1982. El gusano más famoso fue el que en noviembre de 1988 se propagó por sí solo a más de 6.000 sistemas a lo largo de Internet. Véase también caballo de troya, y virus.

H

HACKER.

Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo. II. (pirata) 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". III. Persona de elevados conocimientos en el ramo informático que tiene la capacidad de violar los sistemas de seguridad de una computadora o una red, lo cual le provoca placer, este término no debe de llevarse al extremo de alguien malo con fines de destruir sistemas, esto encaja mejor en la definición de "cracker". Ver también: "cracker".

HACKING (pirateo) Ver: "hacker".

HARDWARE (fierros, hardware, maquinaria)

Se trata de todos los componentes físicos de una computadora, entre los cuales se pueden mencionar el disco duro, procesador, monitor, etc. que en conjunto con el software (programas) hacen que funcione nuestra máquina. Ver: "software".

HTML

Lenguaje de marcado de hipertexto, (Hiper-Text Markup Languaje) es el lenguaje con que se escriben los documentos en el World Wide Web. A la fecha existen tras versiones de HTML. HTML 1, donde se sientan las bases para la disposición del texto y las gráficas, HTML 2 donde se agregan formas y HTML 3 (llamado también extensiones Netscape) donde se añaden tablas, mapas, etc. II. Este lenguaje es donde se forman la mayoría de las páginas que se visualizan en Internet, admite elementos de hipertexto y multimedia entre otras muchas cosas. Vea HTTP.

HTTP.

Protocolo de Transferencia de Hipertextos (Hiper-Text Transfer Protocol). Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.

I

INTERNET.

Es una red de cómputo a nivel mundial que agrupa a distintos tipos de redes usando un mismo protocolo de comunicación. Los usuarios en Internet pueden compartir datos, recursos y servicios. Internet se apoya en el conjunto de protocolos TCP/IP De forma más específica, Internet es la WAN más grande que hay en el planeta, e incluye decenas de MAN's y miles de LAN's. Las computadoras que lo integran van desde modestos equipos personales, minicomputadoras, estaciones de trabajo, mainframes hasta supercomputadoras. Internet no tiene una autoridad central, es descentralizada. Cada red mantiene su independencia y se une cooperativamente al resto respetando una serie de normas de interconexión. El organismo que se encarga de regular, establecer estándares, administrar y hacer operacional a Internet es la ISOC (Internet Society). II. (Internet, La Red) Se denomina así a la red de telecomunicaciones que surgió en los Estados Unidos en 1969 y que en sus orígenes era de carácter meramente militar, para el día de hoy convertirse en uno de los principales medios de comunicación que de manera global afecta la sociedad en diversos aspectos como son el social, cultural, económico, etc.

Se puede clasificar en tres niveles: el primero lo conforman las redes troncales, el segundo las redes de nivel intermedio y el tercero lo constituyen las redes aisladas. El Internet es además una red multiprotocolo capaz de soportar cualquier tecnología.

INTRANET.

Una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno. Por ejemplo, muchas compañías tienen servidores World Wide Web disponibles solo para sus empleados

INFORMACIÓN.

Se trata de la suma de varios datos que tiene un significado completamente distinto al de cada uno de ellos visto de manera individual. Por ejemplo j, o, s, u y e son datos, josue es una información. Es un recurso invaluable dentro del desarrollo y expansión de las tecnologías.

L

LOGIN.

Clave de acceso que se le asigna a un usuario para que pueda utilizar los recursos de una computadora. El login define al usuario y lo identifica dentro de Internet junto con la dirección electrónica de la computadora que utiliza.

LLAVE ELECTRÓNICA.

Se trata de una serie de signos previamente convenidos que sirven como clave o fórmula para transmitir mensaje secretos o privados.

M

MULTIMEDIA.

Material digitalizado que combina textos, gráficos, imagen fija y en movimiento, así como sonido.

MICROSOFT.

Compañía creadora del sistema operativo Windows 95, Windows NT, de los controles Active X , desarrolladora del visualizador del World Wide Web Internet Explorer, entre otros recursos.

MÓDEM.

I. Se trata de un aparato que se encarga de convertir las señales digitales en analógicas y viceversa que a su vez permite que dos computadoras que se comuniquen a través de una línea telefónica normal o de cable. II. Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una red digital de servicios integrados (ISDN), mediante un proceso denominado de modulación (para transmitir información) y demodulación (para recibir información), de ahí su nombre. La velocidad máxima que puede alcanzar un módem para línea telefónica es de 33 kBps, sin embargo los más comerciales actualmente son los de 28 kBps. Un módem debe cumplir con los estándares de MNP5 y V42.bis para considerar su adquisición. Los módems se dividen en internos (los que se colocan en una ranura de la computadora) y en externos (que

se conectan a un puerto serial de la computadora). Instalación: Modems Internos. Estos deben ser configurados antes de ser instalados. Es necesario mover los puentes (jumpers) para indicar un puerto (COM) y una interrupción (IRQ). Modem Externos. La instalación requiere de un cable (DB25 o de 25 agujas macho a 25 agujas hembra o a 9 agujas hembra) que conecte directamente al puerto serial de la computadora. Es necesario asegurarse que no se esta utilizando un puerto compartido con otro elemento de hardware (por ejemplo: un mouse). Para ello debe instalarse en COM2 o COM4 sí el mouse esta instalado en COM1 o en COM1 o COM3 si el mouse esta instalado en COM2. La interrupción (IRQ) depende del puerto donde este instalado.

MOUSE (mouse, ratón)

El multiconocido mouse o ratón es el dispositivo electrónico que nos permite dar instrucciones a nuestra computadora a través de un cursor que aparece en la pantalla y haciendo click para que se lleve a cabo una acción determinada.

N

NAVEGAR (navegación por la red)

Se refiere a la acción de buscar en Internet información novedosa o tan solo como un motivo de entretenimiento. Cada día se hace más común esta actividad en nuestra vida diaria.

NETSCAPE COMMUNICATOR (Comunicador Netscape)

Se trata de uno de los navegadores de Internet más utilizados en el ámbito mundial, creado por la compañía Netscape y hace poco comprado por AOL en uno de los traspasos más escandalosos de la historia de Internet.

O

OFF LINE (fuera de línea, desconectado, off line)

Se refiere al estado en que nuestra computadora no se encuentra conectada a Internet o a una red en general en ese preciso momento. Ver: "on line".

ON LINE (en línea, conectado, on line)

Es el estado en que nuestra computadora se encuentra en línea, o sea, conectada a Internet. Ver: "off line"

P

PASSWORD (contraseña, palabra de paso)

Conjunto de números, letras y caracteres especiales que dan acceso a un usuario a un determinado recurso del sistema o de Internet.

PC (computador personal, computadora personal, ordenador personal, PC)

Se trata del avance tecnológico que en los últimos años cambió al mundo. Cada día se revoluciona la tecnología haciéndolas más poderosas y capaces de realizar múltiples tareas.

PHRACKER (fonopirata)

Es un individuo de alta capacidad en el manejo y manipulación de las redes telefónicas, las cuales utiliza para obtener cierta información de redes ajenas. En muchas ocasiones se pone en juego este tipo de prácticas para evadir el pago de los recibos telefónicos.

R

RED (Network)

Una red de ordenadores es un sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en diferentes lugares. II. Se compone de una red de computadoras que se encuentran dentro de un sistema de comunicación que conecta entre sí sistemas informáticos que se encuentran en lugares remotos. Se puede componer por diversos tipos de redes.

S

SERVIDOR

Se le llama así a todo aquel servidor que se encuentra en línea y que proporciona información a los usuarios. Ver: computadora.

SHAREWARE (programas compartidos)

Se llama así a las muestras de prueba que algunos fabricantes proporcionan de software para su evaluación por parte del posible cliente. Dichas pruebas por lo general expiran a los 30 días de instalación de dicho programa en nuestra computadora. Ver:"public domain", "freeware".

SOFTWARE (componentes lógicos, programas, software)

Se llama así a todos los programas o elementos lógicos que hacen que una computadora funcione, poniéndose en interacción con los componentes físicos de la computadora. Ver: "malware", "hardware". (Piratería de programas, piratería de software) Una de las industrias más fuertes dentro de los negocios sucios es la piratería de software, violando todas las leyes que protegen los derechos de autor, esto se fomenta en gran medida debido al elevado costo de la mayoría de los programas, pero de ninguna manera es motivo para realizar esta práctica.

SYSOP (Operador del Sistema)

Se le denomina de esta manera al técnico o ingeniero responsable del funcionamiento de una red.

U

UPLOAD (cargar, subir).

Se denomina así al proceso en donde nosotros subimos una información desde nuestra computadora a un servidor en Internet (como es el caso de las páginas personales PoderNet). Ver:"download".

V

VIRTUAL (virtual)

Es lo que no existe o no es real aparentemente.

VIRUS (virus)

Se le llama así a todo programa computacional que se duplica a sí mismo dentro de un sistema y que se añade a otros programas que se utilizan ocasionando fallas. En la actualidad son la principal preocupación de los usuarios que navegan en Internet, en donde por cierto tienen su mayor campo de acción.

W

WEB, web (malla, telaraña, web)

Se emplea este término para definir a un servidor WWW, así como para definir el universo de Internet en su totalidad.

World Wide Web -- WWW, W3 (Telaraña Mundial, Red Mundial, WWW).

Sistema global de la información basado en la tecnología del hipertexto, que se crea en los 90's por Tim Bemers Lee, investigador en el CERN, Suiza. Este sistema soporta todo tipo de información (audio, video, imagen, texto, etc.) y se accesa de manera fácil por los usuarios a través de los navegadores. II. Los usuarios pueden crear, editar, y visualizar documentos de hipertexto con características multimedia. Se puede acceder fácilmente a sus clientes y servidores.

W.W.W. Ver World Wide Web.

BIBLIOGRAFÍA.

I. DOCTRINA

ARTEGA S., Alberto. "El delito informático: algunas consideraciones jurídico penales" Revista de la Facultad de Ciencias Jurídicas y Políticas. No. 68 Año 33. Universidad Central de Venezuela. 1987. Caracas, Venezuela.

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.

CORREA, Carlos M. Derecho Informática, Editorial Depalma, Buenos Aires, Argentina 1987.

DAVARA RODRÍGUEZ, Miguel Angel. Derecho Informático, Editorial Arazandi, Caracas Venezuela 1993.

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

FERNÁNDEZ Calvo, Rafael. "El tratamiento del 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.)

GARVARINO, Alvaro, Curvelo, Carmelo, et all. "Nuevas normas jurídicas en materia informática" Revista de la Asociación de Escribanos del Uruguay. Vol. 76 No. 1 - 6. Enero-Junio 1990. Montevideo, Uruguay.

GUTIÉRREZ FRANCÉS, María Luz, Fraude Informático y Estafa. Ministerio de Justicia, Secretaría General Técnica, Madrid 1991.

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

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.

LOSANO, G., Mario. "Anteproyecto de ley colombiana de 1987. Una propuesta de ley sobre la privacy en la República de Colombia." Cuadernos y Debates. No. 21. Colombia.

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

NUÑEZ PONCE, Julio, Derecho Informático, Nueva disciplina jurídica para una sociedad moderna, Marsol Perú Editores, S.A., Lima Perú 1996

QUIÑOS GÓMEZ, Gregorio. Cibernética Penal, El delito Computarizado. Edición Epson Venezuela, S.A. Caracas Venezuela 1989.

TELLEZ Valdés, Julio. Derecho Informático. 2ª. Ed. México. Ed. Mc Graw Hill 1996.

TONIATTI, Roberto. "Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada". Revista Vasca de Administración Pública. No. 29, Enero-Abril, 1991, España.

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

II. LEGISLACIÓN

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

Código Penal para el Distrito Federal. Editorial SISTA, S.A. de C.V. México D.F. 2000.

Código penal para el Distrito Federal en materia del fuero común y para toda la república en materia del fuero federal, Editorial SISTA, S.A. de C.V. México D.F. 1999.

Código de Procedimientos Penales para el Distrito Federal, Editorial SISTA, S.A. de C.V. México D.F. 2000.

Ley de Vías Generales de Comunicación. Colección Porrúa. Editorial Porrúa. 23ª edición. México.1999.

Legislación sobre propiedad industrial e inversiones extranjeras. Colección Porrúa. Editorial Porrúa. 19ª edición. México 1999.

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

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

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

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

Código Penal del Reino de España, Editorial Promociones y Distribuciones Universitarias 1999.

III. OTRAS FUENTES

"Aprobó el Senado reformas a la Ley sobre Derechos de Autor y el Código Penal", El Universal, México, martes 29 de abril de 1997. Sección primera, segunda columna página 3.

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Europa en la vanguardia de la sociedad mundial de la información: plan de actuación móvil. Bruselas, 21.11.1996 COM (96) 607 final.

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Contenidos ilícitos y nocivos en Internet. Bruselas, 16.10.1996 COM (96) 487 final.

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

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

III. OTRAS FUENTES

"Aprobó el Senado reformas a la Ley sobre Derechos de Autor y el Código Penal", El Universal, México, martes 29 de abril de 1997. Sección primera, segunda columna página 3.

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Europa en la vanguardia de la sociedad mundial de la información: plan de actuación móvil. Bruselas, 21.11.1996 COM (96) 607 final.

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Contenidos ilícitos y nocivos en Internet. Bruselas, 16.10.1996 COM (96) 487 final.

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

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

NACIONES UNIDAS. Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. La Habana, 27 de agosto a 7 de septiembre de 1990. (A/CONF.144/28/Rev.1) Nueva York, Naciones Unidas.1991.

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

* Primer Congreso Internacional de Delitos Cibernéticos. España. 1982.

"Tratado de Libre Comercio", Novedades, México, jueves 20 de agosto de 1992.

"Tarjetas: superfraudes". El Sol de México Mediodía. México, lunes 21 de abril de 1997. Primera plana.