332

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"ACATLAN"

DERECHO PENAL INFORMATICO

FALLA DE ORIGEN

TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN DERECHO

P R E S E N T A :

MA. IMELDA RODRIGUEZ MORALES

NAUCALPAN, EDO. DE MEX. MARZO DE 1995.

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

AGRADECIMIENTO

A LOS DRES. MIREILLE ROCATTI V. Y JULIO TELLEZ VALDEZ, TODA MI ADMIRACION Y AGRADECIMIENTO POR SU APOYO BRINDADO.

MIL AGRADECIMIENTOS A:
NADINE TERREIN ROCATTI;
GEO GASTON HASS, Y
ERIKA TAPIA, POR LAS --
TRADUCCIONES REALIZADAS
QUE HICIERON POSIBLE, -
ESTE TRABAJO.

A TODOS AQUELLOS QUE ESPERARON, LA CONCLUSION DEL CITADO TRABAJO.

Y DESDE LUEGO, MI PROFUNDO AGRADECIMIENTO A AQUELLA PERSONA QUE HA CREIDO TANTO EN ESTAS INQUIETUDES Y SUPO ALENTARME, ASESORARME PROFESIONALMENTE, PARA - LA REALIZACION DE ESTE TRABAJO. ME REFIERO AL PROF. MIGUEL GONZALEZ MARTINEZ, QUE TAMBIEN LO ADMIRO Y - PIENSO QUE ALGUN DIA BRILLARA COMO LA MAS BRILLANTE ESTRELLA, ADEMAS DE TODO LO APRECIO.

DERECHO PENAL INFORMATICO

INDICE

Este trabajo de tesis que presento para obtener, el título de Lic. en Derecho denominado " DERECHO PENAL INFORMATICO," es una inquietud personal por vislumbrar nuestra legislación penal,- desprovista de una normatividad adecuada; tratándose de las acciones económica, política y socialmente peligrosas que se han engendrado en la periferia de la informática, y que desde luego demandan respuestas legales de leyes de información.

El primer capítulo, comprende principalmente los elementos del delito, tanto los aspectos positivos como negativos, atendiendo enfoques de diversas corrientes, así como el propio. Creemos pertinente partir de elementos moleculares, para poner en tela de juicio nuestro planteamiento concerniente a, crear un marco legal que tipifique dichas acciones.

En el segundo capítulo, la sustentante da su propio concepto de esta parte especial del derecho penal y del bien jurídico tutelado.

Por otra parte aludo también, a las materias que este recién nacido derecho, ha invadido por estar estrechamente vinculado a ellas; tales como el derecho civil, fiscal, laboral, Marcas y Patentes, Derechos de Autor, Protección al Consumidor, etc., y desde luego no podía hacer falta referirme a la proyección internacional que ha tenido dicha parte especial, los flujos transfronterizos de datos, las empresas transnacionales, así como el libre cambio de los mismos.

El capítulo tercero, es un bosquejo del impacto que ha - representado el papel de la informática, y luego hago una preci--

sión técnica de los términos que se emplean en ella, antes que nada esperando ser explícita para el jurado y los démas lectores. - En éste también se analiza el delito informático de acuerdo al -- criterio de algunos Doctores en la materia, así como las características de éstos, y su clasificación.

Por otro lado cabe mencionar que algunas estrategias para lograr una política criminal en la informática, son señaladas en el capítulo en alusión.

En el capítulo cuarto, la sustentante analiza en nuestra legislación penal, los tipos penales que se encuentran vinculados a los delitos informáticos, tales como el robo, el fraude, el abuso de confianza, espionaje, sabotaje, falsificación de documentos ultrajes a la moral, etc., nuestros razonamientos por los cuales son inaplicables; siendo importante en estos problemas el principio de la legalidad de las penas; la extensión, así como la interpretación analógica y por mayoría de razón.

En el último capítulo, contemplo la legislación comparada de los ilícitos informáticos de algunos países como Alemania, Dinamarca, Canadá, Francia, etc., con el proposito que se aprecie - como los países más informatizados, han solucionado éstos ilíci-- tos con textos legislativos y jurisprudencias.

CAPITULO I
EL DELITO

I.A. DEFINICION

Para varios autores, la verdadera noción formal del delito se encuentra prevista en el código penal, en el artículo 7º.- el cual establece " Delito es el acto u omisión que sancionan las leyes penales." (I)

El Dr. Fernando Castellanos Tena, citando a Edmundo Mezger, para quien " El delito es una acción punible; esto es, el conjunto de presupuestos de la pena." (2)

ELEMENTOS

Los diferentes autores del tema no han llegado a un acuerdo sobre los elementos del delito, pues para unos éste es indivisible (Corriente Unitaria) y para otros, se constituye por varios elementos (Corriente Atomizadora).

I.B. CLASIFICACION

Los delitos se ordenan de acuerdo a diversos factores como son los siguientes:

- Conducta;
- Resultado;
- Daño;
- Duración;

(I) Código Penal para el D.F., pág. 2, 52a. edición, Edit. Porrúa, S.A., México, D.F., 1994.

(2) Fernando Castellanos, Líneamientos Elementales de Derecho Penal, pág. 128, XXXIa. edición, Edit. Porrúa, S.A., México, D.F., 1992.

- Culpabilidad;
- Complejidad;
- Conformación o Actos Integrantes;
- Sujetos;
- Orden, y
- Legal.

Según la conducta del sujeto activo; pueden ser:

DE ACCION: Cuando el tipo requiere un acto.

DE OMISION: Existe una trasgresión a una norma preceptiva.

DE COMISION POR OMISION: Se transgreden dos normas una preceptiva y una prohibitiva.

Por el resultado que producen se dividen en:

FORMALES: Son aquellos en los que se agota el tipo penal con la actividad o inactividad del agente, no siendo necesario para su integración un resultado material.

MATERIALES: Estos requieren para su integración una variación externa.

Por el daño que causan a continuación se contemplan:

DE LESION: Son aquellos que ejecutados producen daño al interés jurídicamente tutelado.

DE PELIGRO: No causan daño directo, pero ponen en peligro inminente algunos intereses.

Por su duración se enuncian los siguientes; de acuerdo al criterio del Código Penal:

INSTANTANEO: Así lo establece la fracción I del ordenamiento legal en cita y dice " Cuando la consumación se agota en el mismo momento en que se han realizado todos sus elementos constitu

tivos; "

PERMANENTE O CONTINUO: Así lo prevé la fracción II, " cuando la consumación se prolonga en el tiempo ", y (3)

CONTINUADO: fracción III del artículo en cita establece " cuando con unidad de propósito delictivo y pluralidad de conductas se viola el mismo precepto legal." (4)

Por su culpabilidad igualmente atendiendo el criterio del Código Penal, prevé los siguientes: (5)

DOLOSOS: Establece el primer párrafo del artículo 9º.- " Obra - dolosamente el que conociendo los elementos del tipo penal, o - previendo como posible el resultado típico, quiere y acepta la realización del hecho descrito por la ley, " y (6)

CULPOSOS: La segunda fracción del artículo en comento dice " Obra culposamente el que produce el resultado típico, que no -- previo siendo previsible o previó confiando en que no se produciría, en virtud de la violación a un deber de cuidado, que debía y podía observar según las circunstancias y condiciones personales." (7)

Por la complejidad pueden ser:

SIMPLES: Se lesionan a un sólo bien jurídicamente protegido.

COMPLEJOS: El Dr. Fernando Castellanos Tena, citando a Sebas--- tián Soler, para quien esta especie de delitos son " Aquellos - en los cuales la figura jurídica consta de la unificación de -- dos infractores, cuya fusión da nacimiento a una figura delic-- tiva nueva, superior en gravedad a las que la componen, tomadas

(3) Código Penal para el D.F., ob. cit., pág. 3.
(4) Idem.
(5) Idem.
(6) Idem.
(7) Idem.

aisladamente." (8)

Por la conformación o actos integrantes se dividen en:

UNISUBSISTENTES: Se integran en un sólo acto.

PLURISUBSISTENTES: Se constituyen por diversos actos.

Por los sujetos pueden ser:

UNISUBJETIVOS: Se consuman con la intervención de un sólo sujeto.

PLURISUBJETIVOS: Se consuman con la intervención de varios sujetos.

De acuerdo al orden se dividen en:

COMUNES: Localmente son establecidos y aplicados.

FEDERALES: Son aquellos que emanan de la Carta Magna y de otras leyes especiales, expedidos por el Cóngreso de la Unión, por en de tienen aplicación en todo el territorio nacional.

MILITARES: Están contemplados en su Ley Castrense en función de la disciplina del Ejército, Armada y Fuerza Aérea, por lo tanto sólo es aplicable a este sector.

POLITICOS: En la Constitución Política de los Estados Unidos Mexicanos se alude a delitos políticos, así mismo están previstos en el Título Primero, Libro Segundo de nuestra Legislación Penal algunos de ellos son los siguientes:

- Rebelión;
- Sedición;
- Motin; etc.

Estos delitos, se pueden analizar de acuerdo "con una - triplicidad, y son, cualquier comportamiento que atente, contra

(8) F. Castellanos, ob. cit., pág. I 42.

la democracia, la Federación o bien la seguridad interior de la Nación," así lo señala el Lic. Agustín Pérez Carrillo.

(9) La última clasificación, o sea la legal es la que da la Ley sustantiva, en el Libro Segundo.

I.C. LA CONDUCTA

Todo delito proviene de la conducta humana, algunos tratadistas lo llaman conducta, y otros lo llaman hecho.

Quienes sustentan la primera hipótesis, el objetivo del delito será la conducta; si el tipo legal describe una ac-- ción o una omisión, para los segundos, cuando para colmar el ti po legal se requiere además de la acción o de la omisión, un re sultado material, unido por un nexo causal.

Para el Dr. Fernando Castellanos Tena, el elemento - objetivo en cita puede presentar las formas de acción, omisión y comisión por omisión. Al respecto señala " La acción se integra mediante una actividad (ejecución) voluntaria (concepción y decisión), la omisión y la comisión por omisión se conforman -- por una inactividad, diferenciándose en que en la omisión hay - una violación de un deber jurídico de obrar, en tanto que en la comisión por omisión se violan dos deberes jurídicos, uno de -- obrar y uno de abstenerse." (IO)

Por lo que conceptúa el Dr. en comento la conducta - en los siguientes términos:

" Es el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito." (II)

(9) Agustín Pérez, Derechos Humanos, Desobediencia Civil y Delitos Políticos, pág. I99, Cuaderno del inacipe Núm, 39, Méx.I99I.

(IO) F. Castellanos, ob. cit., pág. I49.

(II) Idem.

Solamente el hombre, puede cometer infracciones penales, no así los entes colectivos, ni los animales por carecer de voluntariedad.

En todo caso solo serán responsables las personas físicas que integran a las personas morales, en la comisión de algún acto delictuoso; o bien serán responsables ante la ley penal los propietarios de los animales que causen algún daño.

Sujeto Activo; es el perpetrador de un acto delictuoso.

Sujeto Pasivo; será aquel sobre quien recae una --- transgresión penal.

El Ofendido; señala el Dr. Fernando Castellanos Tena " Es la persona que resiente el daño."(I2)

OBJETOS DEL DELITO

Algunos tratadistas distinguen entre objeto material y objeto jurídico del delito.

El objeto material es confundido con el sujeto pasivo toda vez que sostienen " Es la persona o cosa sobre quien recae el daño o peligro; la persona o cosa sobre la que se concreta la acción delictuosa ", ya que a juicio personal sería entonces el objeto en comento el resultado delictuoso.

El objeto jurídico o formal; es el bien jurídico -- vulnerado.

LA ACCION

El Dr. en comento citando a Cuello Calón, quien defi

(I2) F. Castellanos, ob. cit., pág. I52.

ne, la acción stricto sensu, en los siguientes términos " es - el movimiento corporal voluntario encaminado a la producción - de un resultado consistente en la modificación del mundo exterior o en el peligro de que se produzca."(I3)

ELEMENTOS DE LA ACCION

Desdoblando el anterior concepto de Cuello Calón, tendrémos los siguientes elementos;

- Un acto de voluntad;
- Una actividad corporal;
- Modificación del mundo exterior, o bien
- la producción de un peligro.

LA OMISION

El Dr. en comento citando a Eusebio Gómez, para quien los delitos de omisión " son aquellos en los que las condiciones - de donde se deriva su resultado reconocen, como base determinante, la falta de observancia por parte del sujeto de un precepto obligatorio."(I4)

Pueden distinguirse dos tipos de omisión;

Simple omisión como ya lo he señalado con antelación, son aquellos en los que hay una transgresión a una norma preceptiva.

Comisión por omisión; igualmente los he señalado anteriormente, son aquellos que transgreden dos normas, una preceptiva y una prohibitiva.

ELEMENTOS DE LA OMISION

En delitos de omisión existe una abstención de realizar -

(I3) Idem.

(I4) Ibíden, pág. I53.

un deber jurídico, o de obrar.

Sus elementos serían;

- La voluntad;
- abstención, y
- violación de un deber jurídico.

LA CAUSALIDAD EN LA ACCION

Al respecto dos corrientes comprenden diversas teorías -- procurán determinar cuales actividades humanas, pueden considerarse como causas del resultado.

Una es la individualizadora, la cual ha de ser tomada en, cuenta, de entre todas las condiciones, una de ellas en atención a factores de tiempo, calidad o cantidad, la segunda corriente es la generalizadora en virtud ella, todas las condiciones productoras del resultado son iguales.

LA CAUSALIDAD EN LA OMISION

En los delitos de omisión, como no se produce un resultado material, no se da una relación causal, en cambio en los delitos de comisión por omisión si existe un nexo causal, al provocar una variación en el mundo exterior.

LUGAR Y TIEMPO DE COMISION DEL DELITO

Estos problemas, señala el Dr. Fernando Castellanos Tena se pueden solucionar con tres teorías de Cuello Calón:

La teoría de la actividad, " según la cual el delito se - comete en el lugar y al tiempo de la acción o de la omisión ";

La teoría del resultado; " de acuerdo con ella el delito se realiza en el lugar y al tiempo de producción del resultado;" y

La teoría de la ubicuidad, " para la cual el delito se comete tanto en el lugar y al tiempo de realización de la conducta - como en donde y cuando se produce el resultado."(I5)

Nuestra Legislación Penal acoge la Teoría del Resultado.

ASPECTO NEGATIVO DE LA CONDUCTA

La aludida Legislación Penal prevé, en la fracción I del artículo I5º.- El delito se excluye cuando;

"El hecho se realice sin intervención de la voluntad del agente;"(I6)

Este supuesto es lo que los doctrinarios llaman vis absoluta, o fuerza física exterior irresistible, que en realidad es un factor eliminatorio de la conducta humana, igualmente consideran a la vis maior (fuerza mayor) y los movimientos reflejos por carecer las personas de voluntad.

Algunos tratadistas consideran como aspectos negativos de la conducta: el sueño, el hipnotismo y el sonambulismo, dado que el sujeto se halla en un estado en el cual su conciencia se encuentra suprimida y han desaparecido por las fuerzas inhibitorias.

I. D. LA TIPICIDAD

El Dr. Raúl Carranca y Trujillo conceptúa la tipicidad en la forma siguiente, " Es la adecuación de la conducta concreta al - tipo legal concreto. " (I7)

La mayoría de los tratadistas contemporaneos, coinciden en - las ideas, respecto a la tipicidad; al considerar en su concep -

(I5) Ibídem., pág. I6I.

(I6) Código Penal para el D.F., ob. cit., pág. 5.

(I7) Raúl Carranca, DERECHO PENAL MEXICANO, pág. 423, XVI edición Edit. Porrúa, S.A., México, D.F., I988.

to al tipo; aunque históricamente éste es el antecedente del - aspecto positivo que nos ocupa. En Alemania por ejemplo el tipo era considerado como el conjunto de caracteres integrantes del delito, tanto los objetivos como los subjetivos; es decir incluyendo el dolo y la culpa.

Posteriormente fueron separados los elementos en cuestión con la evolución de las teorías de diversos tratadistas, partiendo de la ratio cognoscendi; hasta la ratio essendi, considerando la primera de éstas al tipo,como indiciario de la antijuridicidad; y la segunda lo estimó como fundamento real de la - misma.

LA FUNCION DE LA TIPICIDAD

Se basa en el principio de que ; " No hay delito, sin tipo legal " , es decir ninguna acción humana podrá ser considerada como delictuosa, sino está prevista así en la legislación.

CLASIFICACION DE LOS TIPOS

Atendiendo a criterios de diversos tratadistas en torno, a los tipos se ordenan en la forma a continuación descrita:

POR SU ESTRUCTURA METODOLOGICA: Pueden ser los básicos, especiales y complementados.

POR SU COMPOSICION:Se dividen en normales y anormales.

POR SU AUTONOMIA: Serían los independientes y los subordinados.

POR SU FORMULACION: Son los casuísticos, que a su vez se subdividen en alternativos y acumulativos; y los siguientes son los amplios.

Nuestra Legislación Penal, en el aludido precepto - I5º prevé la exclusión del delito,"cuando falte alguno de los elementos del tipo penal del delito que se trate;"así lo establece la fracción II. Consecuentemente por adolecer (I8) de un elemento esencial no se integrará, por ende no habrá delito.

Al respecto el Dr. Ferando Castellanos Tena, señala " Cuando no se integran todos los elementos descritos en el tipo legal, se presenta el aspecto negativo del delito llamado - atipicidad." (I9)

Algunos doctrinarios equiparan la atipicidad con la falta de tipo.

El Dr. en cita reduce las causas de atipicidad en - la forma siguiente:

" a) Ausencia de la calidad o del número exigido por la - Ley en cuanto a los sujetos activo y pasivo;

b) Si faltan el objeto material o el objeto jurídico;

c) Cuando no se dan referencias temporales o espaciales requeridas en el tipo;

d) Al no realizarse el hecho por los medios comisivos específicamente señalados en la Ley;

e) Si faltan los elementos subjetivos del injusto legalmente exigidos, y

f) Por no darse, en su caso, la antijuridicidad especial.

En el primer caso el legislador incurre en ambigüedades al describir las hipótesis, requiriendo una calidad a am--

(I8) Idem.

(I9) F. Castellanos, ob. cit., pág. I74.

bos sujetos, o a uno sólo." (20)

En el segundo caso cuando falte la persona, cosa o el bien jurídico tutelado, no habrá tipicidad.

El tercer caso, se presenta cuando no se colman algunas circunstancias, de modo o de tiempo que exige el tipo.

El cuarto caso, se refiere a las modalidades que, tiene que presentar algún comportamiento; para poder integrar el ilícito correspondiente.

El quinto caso, se presenta cuando algún caso específico carece de un elemento subjetivo.

El último, es una situación especial, que por existir ciertas permisiones legales, manifiesta el Dr. en cita " no se colma el tipo y las causas que en otros delitos serían, por su naturaleza, causas de justificación, tornanse atipicidades en estos casos." (21)

I.3. LA ANTIJURIDICIDAD

Este elemento es abordado, bajo teorías monistas - y dualistas de diferentes tratadistas:

Los primeros conciben a la antijuridicidad como la contrariedad al derecho; los segundos consideran una doble antijuridicidad, formal y material; siendo la primera de éstas cuando se transgrede a una norma establecida por el Estado y la segunda cuando signifique contradicción a los intereses colectivos.

EL ASPECTO NEGATIVO DE LA ANTIJURIDICIDAD

El aspecto negativo de la antijuridicidad lo conti

(20) Ibídem, pág. 175.
(21) Ibídem, pág. 176.

tuyen las causas de justificación, que son aquellas que excluyen de incriminación, a un sujeto capaz.

Nuestra Legislación Penal denomina al aspecto negativo en cita, como Causas de Exclusión del Delito y se encuentran previstas principalmente en el aludido precepto 15 fracciones IV, V, y VI.- comprendiendo las siguientes:

a) Legítima Defensa;
b) Estado de Necesidad;
c) Cumplimiento de un deber, y
d) Ejercicio de un derecho.

Quienes excedan en los casos citados con antelación serán punibles como delitos culposos.

Legítima Defensa, el Dr. Castellanos Tena citando, a Jiménez de Asúa, para quien ésta excluyente es " La repulsa de una agresión antijurídica, actual o inminente, por el atacado o tercera persona contra el agresor, sin traspasar la necesidad de la defensa y dentro de la racional proporcionalidad de los medios." (22)

Este concepto es muy similar al contenido de la fracción IV del artículo en comento, que aborda ésta eximente en los términos siguientes:

" Se repela una agresión real, actual o inmediatamente, y sin derecho, en protección de bienes jurídicos propios o ajenos,- siempre que exista necesidad de la defensa y la racionalidad de los medios empleados y medie provocación dolosa suficiente e inmediata por parte del agredido o de la persona a quien se

(22) Ibídem, pág. 191.

defiende.

Se presumirá como defensa legítima, salvo prueba en contrario, el hecho de causar daño a quien por cualquier medio trate de penetrar, sin derecho, al hogar del agente, al de su familia, a sus dependencias, o a los de cualquier persona que tenga la obligación de defender, al sitio donde se encuentren bienes propios o ajenos respecto de los que exista la misma obligación; o bien, lo encuentre en algunos lugares en circunstancias tales que revelen la probabilidad de una agresión;" (23)

De su análisis se desprenden los siguientes elementos;

a) Repulsa de una agresión real, actual o inmediatamente;

b) Sin derecho;

c) En protección de bienes jurídicos;

d) Que exista necesidad de la defensa, y

e) Ausencia de provocación dolosa del agredido, o de la persona a quien se defiende.

Algunos doctrinarios consideran bajo la forma de legítima defensa las hipótesis siguientes:

a) Riña y legítima defensa;

b) Legítima defensa contra exceso en la legítima defensa;

c) Legítima defensa recíproca;

d) Legítima defensa del inimputable, y

e) Legítima defensa contra inimputables.

(23) Idem.

Estado de necesidad, el Dr. Castellanos Tena citando a Von Liszt, para quien ésta excluyente " es una situación de - peligro actual para los intereses protegidos por el derecho, en la cual no queda otro remedio que la violación de los intereses de otro, jurídicamente protegidos. " (24)

La fracción V del artículo 15 de la Legislación citada, que a la letra dice:

" Se obre por la necesidad de salvaguardar un bien jurídico propio o ajeno, de un peligro real, actual o inminente, no ocasionado dolosamente por el agente, lesionando otro bien de menor o igual valor que el salvaguardado, siempre que el peligro no sea evitable por otros medios y el agente no tuviere el deber jurídico de afrontarlo;" (25)

Analizando éste precepto, podemos desdoblar sus elementos del estado de necesidad:

a) Necesidad de salvaguardar un bien jurídico;

b) Que exista un peligro real, actual o inminente;

c) Que no sea provocado dolosamente por el agente;

d) Que el peligro no sea evitable por otros medios, y

e) Que el agente no tuviere el deber jurídico de afrontarlo.

Algunas especies del estado de necesidad son:

a) El aborto terapéutico, y

b) Robo de famélico.

Cumplimiento de un Deber y el Ejercicio de un Derecho; la fracción VI del precepto en comento, dice:

(24) F. Castellanos, ob. cit., pág. 203.

(25) Idem.

" La acción o la omisión se realicen en cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional del medio empleado para cumplir el deber o ejercer el derecho, y que este último no se realice con el solo propósito de perjudicar a otro;" (26)

En el primer caso consiste en el actuar por obligación; en el segundo cuando la persona que actúa conforme a un derecho, que la propia ley le confiere.

Las formas específicas de estas excluyentes son:

a) Homicidio y lesiones en los deportes;

b) Las lesiones inferidas en el ejercicio del derecho de corregir;

c) Lesiones consecutivas de tratamientos médico-quirurgicos, e

d) Impedimento legítimo.

I.F. LA IMPUTABILIDAD

Para que una persona le sea atribuible un delito, es necesario que tenga un mínimo físico representado por la edad, y otro psicológico, que se refiere a su salud y desarrollo mentales.

El Dr. Castellanos Tena, define la imputabilidad -- como, " El conjunto de condiciones mínimas de salud y desarrollo mentales en el autor, en el momento del acto típico penal que lo capacitan para responder del mismo." (27)

LA RESPONSABILIDAD

Sólo las personas capaces pueden dar cuenta de sus

(26) Ibídem, págs. 5-6.

(27) F. Castellanos, ob. cit., pág. 218.

hechos a la sociedad, porque entendieron y quisieron la comisión del delito que realizaron.

Al respecto la Escuela Clásica, estima que la responsabilidad se funda en el libre albedrío, ya que el individuo quiere y tiene conciencia de sus actos, porque tiene la facultad de elegir su forma de conducta, en consecuencia la responsabilidad penal, deriva de la responsabilidad.

La Escuela Positivista y la Determinista; manifiestan que la conducta del hombre está sujeta a diversas fuerzas del medio ambiente y social, por lo que el hombre es responsable por el hecho de vivir en la sociedad, es decir que la responsabilidad es social y no moral.

EL ASPECTO NEGATIVO DE LA IMPUTABILIDAD

El aspecto negativo de la imputabilidad, lo constituyen las causas de Inimputabilidad, o bien es la incapacidad para entender y querer en materia penal.

Nuestra legislación penal, contempla como causas de inimputabilidad las siguientes;

- Padecer trastorno mental, y
- Desarrollo intelectual retardado.

Nuestra Carta Magna, así como la Ley para el Tratamiento de Menores Infractores, fundamentan ; otra causa de inimputabilidad que es,

- La minoría de edad.

I.G. LA CULPABILIDAD

Se identifica por la reprochabilidad hacia el perso

trador del ilícito, por haber transgredido una norma penal. 18

Para el Dr. Castellanos Tena, la culpabilidad es " El nexo intelectual y emocional que liga al sujeto con su acto," - es decir, es el enlace entre la acción querida y ejecutada con el resultado. (28)

De acuerdo a las recientes reformas que, ha tenido -- nuestra Legislación Penal, las acciones u omisiones delictivas solamente pueden realizarse dolosa o culposamente, del análisis a las reformas en cuestión, se deduce que ya no se prevé la preterintencionalidad.

Estas dos formas que reviste la culpabilidad, al respecto señala el Dr. en cita, " Se puede delinquir mediante una determinada intención delictuosa (dolo), o por descuidar las -- precauciones indispensables exigidas por el Estado para la vida gregaria (culpa)." (29)

Algunas especies del dolo son:

- Directo;
- Indirecto;
- Indeterminado, y
- Eventual.

La primera se presenta, cuando el resultado corresponde al que había previsto el perpetrador.

La segunda, existe cuando el perpetrador se representa un fin, pero prevé y acepta la realización necesaria de o--- tros propositos delictivos.

(28) Ibídem, pág. 234.
(29) Ibídem, pág. 238.

La tercera, es la voluntad genérica del perpetrador de delinquir, sin fijarse un resultado delictivo concreto.

la última especie se presenta, cuando el perpetrador - se propone un resultado delictivo, pero se prevé la posibilidad de que surjan otros típicos no deseados, pero que se aceptan en el supuesto de que ocurran.

Clases de culpa:

- Consciente, con previsión o con representación, e
- Inconsciente, sin previsión o sin representación.

La primer forma se presenta, cuando el perpetrador -- prevé la posibilidad de un resultado ilícito penal, pero no desea tal resultado y espera que no haya tal evento típico.

La segunda se presenta, como señala el Dr. Castellanos Tena, " Cuando no se prevé un resultado de naturaleza previsible." (30)

Algunos autores clasifican la culpa inconsciente o sin previsión en lata cuando el resultado es previsible por cualquier persona, leve cuando es previsible por una persona cuidadosa y levísima por los extremadamente cuidadosos.

EL ASPECTO NEGATIVO DE LA CULPABILIDAD

Serían las Causas de Inculpabilidad y estas se presentan cuando existe un error de hecho o de derecho, que afecta el conocimiento del activo, por lo tanto, hay una coacción volitiva, situación que impide reprochar su conducta.

(30) Ibídem, pág. 247.

Algunos tratadistas consideran a las siguientes -- Causas de Inculpabilidad:

- El error accidental;
- La obediencia jerarquica;
- Las eximentes putativas;
- Legítima defensa putativa;
- Legítima defensa putativa recíproca;
- Legítima defensa real contra la putativa;
- Delito putativo y legítima defensa putativa;
- Estado necesario putativo;
- Deber y derecho legales putativos;
- La no exigibilidad de otra conducta;
- El temor fundado;
- Encubrimiento de parientes y allegados, y
- Estado de necesidad tratándose de bienes de la misma entidad.

I.H. LA PUNIBILIDAD

Para algunos autores la punibilidad es un elemento esencial del delito y cuando no existe el delito desaparece; en cambio para otros únicamente es un elemento externo, pues aun - en el caso de existir alguna excusa absolutoria el delito per-- siste, tan es así que en algunos delitos no se sanciona a los - autores pero si a los copartícipes.

El Dr. Castellanos Tena, define la punibilidad como " El merecimiento de una pena en función de la realización de cierta conducta. " (31)

(31) Ibídem, pág. 275.

Lo constituyen las Excusas Absolutorias, en virtud de - las cuales se excluye la posibilidad de punición.

Algunos tratadistas consideran algunas especies de las Excusas Absolutorias:

- Excusa en razón de mínima de temibilidad;
- Excusa en razón de la maternidad consciente;
- Otras excusas por inexigibilidad, y
- Excusa por graves consecuencias sufridas.

I.I. LA VIDA DEL DELITO

Para que un delito surja, éste primero se concibe en la mente del perpetrador como idea criminosa, naciendo como delito en el momento de su consumación. A este recorrido o proceso se - le conoce como Iter Criminis o camino del crimen y se integra -- por las siguientes fases:

a) FASE INTERNA: Esta fase a su vez se compone de tres momentos:

- IDEACION: Que es cuando cuando el perpetrador concibe - en su mente, realizar una vulneración penal.

- DELIBERACION: En este momento el perpetrador realiza un juicio valorativo, donde medita y reflexiona entre la realiza--- ción o abstención de un ilícito penal.

- RESOLUCION: En este momento el perpetrador decide lle-- var a cabo la comisión de una conducta delictiva.

b) FASE EXTERNA: Se integra a partir del instante en el -- que perpetrador exterioriza su idea criminosa, hasta su consumación.

- MANIFESTACION: Es el momento en el que el perpetrador exterioriza su pensamiento delictivo, al externar su idea o ideas criminosas.

- PREPARACION: Es un momento intermedio entre la manifestación y ejecución en el cual el perpetrador realiza actos con la finalidad de llegar a la ejecución del delito, pero en los cuales no se vislumbra el nexo de la idea criminal con la transgresión de la norma penal.

- EJECUCION: Es este momento en el cual el perpetrador, agota la conducta delictiva, previamente; ideada, deliberada, resuelta, manifestad y preparada.

Si se colman todos los elementos típicos del delito, se habrá consumado el delito, en caso contrario, se estará en presencia de la tentativa.

LA TENTATIVA

Por tentativa se entiende cuando el activo efectúa actos de ejecucion con el proposito de realizar un ilícito penal, cuya consumación no se lleva a cabo por causas ajenas al activo.

La Tentativa a su vez, se divide en dos formas:

- TENTATIVA ACABADA O DELITO FRUSTADO: El sujeto activo lleva a cabo todos los actos idóneos para cometer el delito, pero el resultado no se presenta por causas ajenas a la voluntad. Hay ejecución completa de actos, lo que no se efectúa es el resultado.

- TENTATIVA INACABADA O DELITO INTENTADO: Consiste esta forma en la omisión de uno o varios actos tendientes a la verificación del delito. En este caso por ser incompleta la ejecución, -

obviamente es el resultado, como consecuencia de la carencia de uno o varios actos, por ende no se produce el delito.

DELITO IMPOSIBLE: Es aquel en el que no se produce el resultado, como afirma el Dr. Castellanos Tena, " por inidoneidad de los medios empleados o inexistencia del objeto del delito." (32)

(32) Ibídem, pág. 291.

CAPITULO II
DERECHO PENAL INFORMATICO

II.A. CONCEPTO

Para nosotros el Derecho Penal Informático, es la parte especial, del derecho penal que incrimina todas las vulneraciones a los sistemas de cómputo, así como los atentados a los mismos, que se han engendrado en el ámbito de la informática.

Hasta mediados del siglo XX, la regulación sobre la protección de la información y entes intangibles, no era tan predominante. La situación ha cambiado rápidamente en las últimas décadas: del desarrollo industrial a la sociedad post-industrial, el creciente valor de la información para la economía, política y cultura, así como el crecimiento de la tecnología computacional, induce a las demandas legales y a nuevas respuestas legales de leyes de información.

El bien jurídico tutelado de la aludida parte especial del derecho penal, es la información, no de una simple información sino de aquella que es resultado de un tratamiento automatizado, concebiéndose ésta como un bien intangible, incorporeo, para el profesor Theodore Roszak; la información "se mueve con la velocidad de la luz, y no es más de lo que ha sido siempre: discretos paquetitos de datos, a veces útiles y a veces triviales." (I)

A pesar de que la informática tiene una interdependencia con otras ramas del derecho, presenta en éstas insuficiencias legislativas, o carencias de una normatividad congruente.

(I) Theodore Roszak, El Culto a la Información, pág. II2, Edit. Grijalbo, S.A., Consejo Nacional para la Cultura y las Artes, México, I990.

DERECHO PENAL

El derecho penal se vincula a la informática, por lo -- que respecta a las figuras tales como el robo, fraude, abuso de confianza, etc., toda vez que en estas vulneraciones; el soporte es una computadora.

Los problemas que se derivan, por ejemplo en el robo -- que se requiere del apoderamiento de una cosa mueble, por lo que hace a la información es algo incorporeo, intangible, no integra convincentemente el supuesto. En el paradigma, del fraude se requiere un engaño o aprovechamiento de un error que permita hacerse ilícitamente de alguna cosa o alcanzar un lucro indebido, el cual resulta abstracto frente al problema, que ofrece varias inconveniencias en la práctica. En el abuso de confianza se requiere de la disposición de una cosa mueble, el cual presenta dificultades a nivel de la carga de la prueba.

DERECHO PENAL POLITICO

Esta parte especial del derecho penal, tiene relación - no sólo con la informática, sino con la telemática; específicamente aquellas acciones que tienden a poner en peligro la democracia, la seguridad de la nación, así como de las instituciones públicas, etc., verbigracia el espionaje, terrorismo y sabotaje, en los cuales el instrumento para perpetrar éstos ilícitos es la computadora.

DERECHO PENAL ECONOMICO

Igualmente esta parte especial del derecho penal, está estrechamente implicada con la informática, tal es el caso que -

la comercialización de productos y servicios informáticos, pueden originar problemas de precios, tales como prácticas anti-concurrenciales individuales (rechazo de venta) o colectivas (entendimientos y abusos de posición dominante).

DERECHO FISCAL

Es directamente el interesado por la informática con la informatización de las contabilidades de las empresas. Sin embargo las reglas del derecho fiscal pueden ser desconocidas por el tratamiento informatizado de los datos contables, vemos que dado el uso de la computadora se pueden engendrar ciertos ilícitos vergracia, la defraudación fiscal.

DERECHO LABORAL

También en el derecho del trabajo, la informática puede conducir a realizar conductas que obstaculizen el funcionamiento de las instituciones representantes del personal, como infracciones a los reglamentos de la medicina del trabajo, y aun más violaciones a la legislación del trabajo, ejemplo; el trajajo temporal.

DERECHO CIVIL

Esta relacionado con la informática, tratándose del enrquecimiento ilegítimo y reparación del daño. En el primer caso el actor debe probar que la utilización de su idea o invención por un tercero ha permitido a éste enriquecerse y correlativamente ha provocado un empobrecimiento, en el segundo caso, consiste en la reparación del daño propiamente dicho, o en el pago de daños y perjuicios, las regulaciones de éstas acciones, no fa

cilitaría mucho su uso, ya que provocaria graves abusos, en virtud del riesgo latente de ver particulares o empresas invocar -- falsamente un enriquecimiento ilegítimo o la reparación de un daño o perjuicio, largamente ficticio o ampliamente sobrestimado.

DERECHO MERCANTIL

En lo que respecta con algunas de sus leyes complementarias, se encuentran entrelazadas con la informática, tal es el - caso de la Ley Federal de Protección al Consumidor, la cual a -- través de la Procuraduria Federal del Consumidor, vigila que las autoridades administrativas competentes regulen la venta de productos o prestación de servicios cuando por causas inherentes a dichos productos o servicios, o a su empleo inadecuado o anárquico se deriven efectos perniciosos para la sociedad en general o para la salud física o psíquica de los consumidores. Siendo las resoluciones que dicten las autoridades administrativas, de interés social y de orden público.

Constantemente esta Ley es violada, sobre todo por los proveedores de software y hardware, que insertan en los contratos de adhesión, ciertas cláusulas leoninas que van en detrimento de la población consumidora, o bien cuando la información subliminal o publicidad mentirosa, comunican mensajes referentes - a las condiciones óptimas de las computadoras, entre ellas que una vez vendidas no requieren de algunos soportes ya sea,

- lógicos, o
- físicos.

El concepto de propiedad intelectual está basado en el reconocimiento natural de derechos en propiedad intelectual, y en la razón pragmática estipulada en la creación del trabajo de la calidad de autor concediendo una remuneración a su creador. En el campo de la información tecnológica, este concepto es meramente importante para la protección de los programas de cómputo.

Estos derechos, son la figura aparentemente aplicable a la protección de los programas, atendiendo a criterios como - sostiene el Dr. Julio Téllez Valdez,

- de selección del género;
- de forma de expresión;
- del mérito;
- la destinación, y
- el principio de exclusión de las ideas.

Estos criterios, son de orden subjetivo referentes al " principio de originalidad," como señala el Dr. en comento, el cual también citando a Vivant,(2) para quien la originalidad es, - en efecto, " el pasaje obligado de toda obra que aspira (donde el autor aspire) a la protección bajo esta forma."(3)

Frente a este problema, es decir a la protección de -

(2) Julio Téllez, Derecho Informático, pág. 91, segunda edicion U.N.A.M. México, 1987.

(3) Julio Telléz, La Protección Jurídica de los Programas de -- Computación, pág. 59, segunda edición, U.N.A.M., México, 1989.

los programas, se presentan algunas prerrogativas tales como el término de duración de los derechos, ejercicio de los derechos de exposición, representación pública, divulgación, retiro de - obra, etc, las cuales no encuentran un acomodo de acuerdo a la naturaleza de los programas de cómputo.

VIA PATENTARIA

Esta figura, la consideran algunos autores tratándose de los programas de cómputo; inaplicable, mientras otros opinan lo contrario.

Toda invención, para ser suceptible de atribuirle una patente requiere como señala el Dr. en cita, " denotar una novedosidad, actividad inventiva, así como una aplicación industrial." (4) Los dos primeros elementos presentan mayor grado de dificultad en función de la complejidad del llamado estado de la técnica con base en la existencia o no de antecedentes, así como que dicha invención resulte o no evidente.

En la novedosidad de las patentes, señala el Dr. en comento se aprecia un " criterio objetivo." (5)

II.C. PROYECCION INTERNACIONAL DEL DERECHO PENAL INFORMATICO

Es increíble que un derecho, a penas recién nacido, tenga o haya invadido ya tantas ramas del derecho penal especial, la observación vale en el sentido que toca a casi todos sus capítulos. También es cierto que en algunas legislaciones se encuentra más desarrollado que en otras, como paradigma del primer caso, lo constituyen Francia, Alemania, algunos países ba-

(4) ob. cit. pág. 91.

(5) Idem.

jos, Suiza, Canadá, E.U.A., etc. Dentro de los cuales existen soluciones legislativas, así vemos que entre los delitos informáticos más importantes son; fraude informático, sabotaje informático acceso inautorizado, falsificación de los datos informatizados, - estafa informática, espionaje informático, robo de tiempo-máquina violación del secreto profesional, violación del secreto de fabricación, corrupción de funcionarios o empleados, distorciones de - ficheros automatizados para dirigir propaganda electoral, en fin se comienza a ampliar la gama de éstos. Por otra parte en los países en que el derecho penal informático no está tan desarrollado tenemos a los que se encuentran en vías de desarrollo entre los - cuales figuran principalmente los países latinoamericamos, países asiáticos, así como de europa oriental.

Por señalar un ejemplo de nuestro segundo supuesto citaremos a Japón, en el cual el número de computadoras, se ha incrementado considerablemente en ésta última década, sin embargo los crímenes perpetrados por este medio son muy escasos. El motivo -- por el que ocurren pocos incidentes, de ésta naturaleza, es por-- que la cultura japonesa no se presta para la manipulación. Los -- perpetradores de dichos actos son castigados y rehabilitados en - en la compañía de la víctima o simplemente despedidos, en muy raros casos. Esto sirve ya que el dueño de la compañía tiene en sus manos la actividad laboral y profesional de sus empleados.

Para los japoneses es realmente inconcebible perder el - honor al verse minimisados por una sociedad que señalará a toda - su familia.

En Japón se utiliza el dinero en efectivo, no hay cheques. Los pagos se hacen frecuentemente en sobres de color café discretos y sellados. Se presentan más de 70 millones de pagos - por sobre, sin embargo, sólo son reportados en promedio de 250 - casos. Si tomamos en cuenta el doble de casos reportados simplemente encontraremos una gran abstinencia de robos.

Al respecto sostiene la Dra. Ma. de Luz Lima, " Sólo -- programando integralmente un programa de prevención estaremos en posibilidad de disminuir la cifra negra de los delitos electrónicos, y no sólo simular una prevención."(6)

Por lo que respecta a nuestra legislación penal, no ha legislado en la materia en alusión, a pesar de que el ámbito político ha estado muy concatenado al uso de la computadora, verbi gracia los comisios de la presidencia de la república, las hostilidades en Chiapas donde la Revista Méxicana de Comunicación, ha publicado un artículo periodístico titulándolo, " LA GUERRA ELECTRONICA Y DE PAPEL ", que sostiene que en la " comunicación masiva en México, ha caído en actitudes como el vedetismo o redencionalismo, el triunfalismo o la piratería informativa. "(7)

Pero no sólo éstas acciones están de moda, sino también fraudes a las casas de bolsa e instituciones bancarias, alteraciones de calificaciones en instituciones educativas, etc.

Por otra parte cabe hablar de la Internacionalización -

(6) Ma. de la Luz Lima, Delitos Electrónicos, pág. 115, Revista Criminalia, Año L, Nos. 1-6, Edit. Porrúa, S.A., México, 1984.

(7) Revista Mexicana de Comunicación, LA GUERRA ELECTRONICA Y DE PAPEL, pág. 19, Año seis- Núm. 34, Abril- Mayo, Mexico, 1994.

de la Delincuencia Informática:

a) Del hecho de la Tecnología

Siendo la informática, el tratamiento automatizado de los datos, el uso de la computadora dio luz a una nueva delincuencia, y ésta es la delincuencia informática, dando alcance a los valores extrapatrimoniales; la libertad, el secreto de la vida privada o bienes intangibles, un monopolio de explotación, una clientela. Esto puede traducirse materialmente, cuando el fraude llega por ejemplo a un giro bancario, a la reproducción, la divulgación viendo la comercialización de una información confidencial de un archivo o de un programa. Pero casi siempre es así.

Tales dificultades no son verdaderamente exclusivas de la delincuencia en computación.

b) La interacción de la Informática-Telemática.

Al aparecer la conmutación, amplificación, etc., la telefonía amplía su cobertura, crecen las redes y nace el télex que, al igual que el teléfono, permite el enlace telegráfico entre usuarios de distintas latitudes.

Recientemente, en la década de 1940 a 1950, aparecen las computadoras, primero a válvulas, luego a memoria de ferrita, semiconductores, burbuja magnética, etc. Primeramente se aplican en la investigación y temas militares y después a aplicaciones comerciales. Para aprovechar mejor los equipos surge la necesidad de compartirlos aprovechando la capacidad y velocidad de éstos. La interconexión entre equipos informáticos no justifica en principio el nacimiento de una infraestructura propia paralela a la ya existente, por lo que utilizando la planta instalada se han ido

usando redes de interconexión de computadores con computadores,- con terminales, con sistemas de control, etc. Desde esa primaria necesidad de interconexión de computadores y terminales remotos, han ido surgiendo necesidades y aplicaciones que han llevado aparejadas las palabras Teleproceso, Teletratamiento, Transmisión - de datos, Teleinformática y Telemática.

Los conceptos hasta aquí estables y concretos de informática y Telecomunicación han evolucionado, o quizá sería más exacto decir que se han extendido en todos los ámbitos, de tal -- forma que la informática ha tendido por un lado a acercarse a -- las telecomunicaciones y éstas, a su vez, a apoyarse en la informática. Así han nacido nuevos campos y que es difícil precisar - el marco en que se encuadran, de manera que la " Teleinformática es tanto las telecomunicaciones para la Informática como la in-- formática para las telecomunicaciones." La palabra Telemática se origina en una contracción de Teleinformática, aunque engloba diversos campos: redes de datos, telemedicina, conmutación electrónica, videotex, teletex,... un sin fin de aplicaciones que ya -- hoy existen y tantos otros conceptos que irán apareciendo hoy la telemática es: el correo electrónico, telex, redes de telegrafía privada, facsímil, televenta, transferencia electrónica de fon-- dos, teleconferencia, telediagnósticos, telebanco, telealarma, - telemando, telemedida, guía telefónica electrónica, etc. Pero además Telemática es también el enlace de datos entre computadores y terminales, por líneas dedicadas, por redes específicas de

(8)

(8) Jóse Mompin, Telemática, pág. IO, Edit. Marcombo, S.A. de -- Boixareú Editores, Barcelona, 1986.

datos (Transpac, Iberpac, etc.), por líneas conmutadas, etc. También es Telemática la interconexión de todas las redes, las de telex-telefonía y datos, lo mismo que serán las Redes Digitales de Servicios Integrados (RDSI).

Existen ramales de transferencia electrónica de datos -- que ofrecen la posibilidad de trabajar o de cometer fraude a distancia, como si la computadora, que se encuentra a decenas o cientos de kilómetros de la terminal, estaba colocada en el cuarto de al lado. Decenas, cientos o miles de kilómetros, ya que éstos ramales se convirtieron en internacionales. Esto no afecta las características de la delincuencia en computación, ya que sólo basta marcar un número de teléfono, así como otras conecciones suplementarias para perpetrar un fraude.

El funcionamiento de éstos ramales multiplica los lugares siempre y cuando termine con la distancia. Hay una multiplicación de los lugares territoriales, extraterritoriales (altamar) o aun extraterrestre (sátelite) sin que se sepa demasiado si una -- misma operación se desarrolla o pasa por cada uno de esos lugares. En lugares de instalación del material de cómputo en sí (terminales- unidades de entrada A,B..., computadora en C, terminales - unidades de salida en D.E...), se debe en fin, agregar aquéllos de la implantación de los diferentes componentes de un ramal de - telecomunicaciones (cables, emisoras, receptores, adaptores, relevos...).

El paso de un lugar a otro se efectúa instantáneamente,- "en directo", en "tiempo real", hay una especie de abolición, una negación de distancias cuyo franqueo ya no se mide en tiempo, en

atraso, pero únicamente en el costo de la comunicación. No solamente se pasa frecuentemente de un territorio a otro, entonces según Michel Masse, " la conception la plus repandue de la compétence des Etats, d'un ordre juridique á un autre- mais cela se fait en un trait de temps."

" El concepto más extenso de la competencia de los Estados, de un orden jurídico a otro-pero se hace en un instante." (9)

Sin embargo el problema de ésta delincuencia, en relación a su soberania estriba en los efectos inmateriales, que dificulta su localización.

c) Del hecho de la Economía

Sociedades Transnacionales

Aparece hoy que el desarrollo de los flujos de materias de datos contribuye a acentuar el papel de las sociedades institucionales, que la O.N.U. califica de transnacionales.

La creación de redes internacionales de datos y las informaciones son, con las agencias de prensa, los principales utilizadores que han respondido a una de las necesidades vitales de las empresas transnacionales: comunicaciones privadas rápidas y fiables. Las telecomunicaciones transnacionales les permiten en realidad de disponer rápidamente a las operaciones necesarias de su gestión, de proseguir día con día en movimiento de sus filiales, de organizar en todo momento los movimientos financieros de las diferentes monedas... Es la telemática que debe de rendir sus redes de comunicación internas y su sistema de entrenamiento en

(9) Traducción de Gaston Haas Geo, del VIII Congreso de la Asociación Francesa de Derecho Penal, pág. 6, Grenoble, 1985.

operación. Ha hecho máquinas para tratar la situación económica - mundial que son actualmente sin igual operando en potencia en la mayor parte de los Estados.

Pero ésta acentuación de la concentración ya considera-- ble y económica entre las manos de un número restringido de empre sas cuya única consecuencia de ósmosis ahora realizado por las em presas y el modelo de organización-funcionamiento de las empresas transnacionales. Puede resultar igualmente una modificación de la situación geográfica de las actividades económicas en el mundo, - en especial de aquellas que son sencibles a la división interna-- cional, que conoce el ejemplo de la toma de datos operados de los cuales la mano de obra es barata cuando su tratamiento de las to- mas de decisión se localizan en los países ricos. Lo que importa es subrayar, es un cierto reacomodo, un despliegue de las opera-- ciones regulado por los Estados mayores que no obedecen más que - la única lógica netamente interna de sus empresas, tiene el ries- go de escapar totalmente a los Estados.

Algunos de ellos podrían no tener un territorio más que los fragmentos de actividades económicas internacionalmente plani ficadas fuera de todo control posible de su parte. Ya las transfe rencias electrónicas de fondos y las facilidades con la cual los datos contables pueden circular de un país a otro, haciendo resal tar los beneficios recíprocos.

La delincuencia de éstas empresas transnacionales, será muy seguido de la computación, porque la telemática les es prácti camente con substancial, internacional, ya que ellas operan a es- cala mundial, y difícil de combatir, ya que igualan en potencia a

la mayor parte de los Estados.

Las primeras investigaciones lanzadas ponen el acento sobre las prácticas de corrupción y de los jarros de vino, los fraudes con las subvenciones y los alcances a la concurrencia, pero también las manipulaciones que existen en el dominio de los servicios, de las transferencias de bienes incorporales y de los movimientos internacionales de capitales, tres dominios en los cuales la computación se multiplica considerablemente, las posibilidades así como la facilidad de fraudes. En lo que toca a la represión, la dificultad principal mora en la identificación de las personas (morales o físicas) a los cuales imputar (en el doble sentido material y moral) la infracción cometida por el interés del grupo completo.

Libre Cambio

La permeabilidad casi total de las fronteras a libre circulación de las informaciones es uno de los datos esenciales de los problemas de la telemática. Es un dato técnico (la telemática conduce de hecho a ésta situación jurídica)encarándolo inicialmente bajo el ángulo de la libertad de expresión y económica (se descubre progresivamente que la libre circulación de las mercancias no puede realizarse sin la libre circulación de las informaciones que le conciernen). Dicho de otra manera la libre circulación de los datos y principio del libre cambio están íntimamente ligados.

Para calificar la situación actual, algunos autores hablan de la misma anarquía. Los bienes de información, cuyo valor y estatuto jurídico no estan aún precisamente definidos, pasan en efecto de una computadora a otra, de una manera que no se puede ser más libre.

CAPITULO III
USO INDEBIDO DE LA INFORMATICA

III.A. GENERALIDADES

Los grandes descubrimientos tecnológicos entre ellos la informática, ha originado una Segunda Revolución Industrial. Estos impactos tecnológicos han transformado las relaciones humanas al grado de romper límites que antes las sujetaban, como eran los del tiempo y el espacio. La informática no hace excepción a ésta especie de ley sociológica del desarrollo de las sociedades industriales, y se puede decir que constituye una ilustración particularmente sugestiva y amplificada.

Los vaticinados impactos, llegan en forma vertiginosa y sorprenden al hombre, tanto que no sólo aproveche ésta máquina para su beneficio, sino para su perjuicio; cuando lo hace indebidamente.

La delincuencia informática engendrada, ha proliferado de manera exorbitante en la última década, y no ha cesado de multiplicarse y alcanza en los países principalmente capitalistas una amplitud considerable.

En los países en vías de desarrollo, no se descartan éstas acciones, sólo que en la mayor parte de ellos se encuentran impunes.

Como ya se señalo en el anterior capítulo, la informática tiene interacción con la telemática, por la interconexión entre equipos informáticos y terminales remotos; las aplicaciones son el Teleproceso, el Teletratamiento, la Transmisión de datos, la Teleinformática, etc

a) ESTRUCTURA

Definición

Computadora: Es un sistema que puede procesar información - de acuerdo con las instrucciones que le son dadas por seres humanos para así efectuar tareas útiles, mediante el manejo de símbolos electrónicos, capaz de almacenar automáticamente datos. La - computación es la técnica de conseguir que la computadora haga - lo que uno desea.

Elementos Básicos de un Sistema de Computación: Una computadora se compone de dos partes;

HARDWARE: Es la estructura física de las computadoras,(sus accesorios o periféricos.).

SOFTWARE: El término se refiere, en general, a todos los -- programas de computación que pueden correrse en el hardware de - la computadora. Pueden distinguirse los programas responsables - del funcionamiento de la computadora- su mantenimiento interno y los sistemas de operación, etc.- de los programas de aplicación. En última instancia, todo el software consiste en patrones de información binaria que dan a la computadora las órdenes de proceso.

PERIFERICOS: Las partes y piezas de un sistema de computa-- ción que se conectan de varias formas al procesador central y a la memoria, constituyen sus dispositivos de entrada y salida. Se incluyen las impresoras, los manejadores de discos, las palancas de mando, las tabletas de graficación, plumas luminosas, etc.

DISPOSITIVOS DE ENTRADA: Los sistemas de computación utilizan muchos dispositivos para la entrada de datos. Algunos permiten la comunicación directa entre los humanos y las máquinas y - otros sólo entre éstas últimas. Sin embargo, sin importar el tipo de dispositivo usado, todos son componentes para la interpretación y comunicación entre personas y sistemas de computación.- Entre ellos tenemos los siguientes:

a). TARJETAS PERFORADAS: Están divididas en columnas verticales numeradas en forma consecutiva de izquierda a derecha. A - su vez, cada columna tiene posiciones o renglones. Las columnas pueden representar un carácter de los datos; un agujero equivale a un dígito y una letra se registra con dos perforaciones.

b). CINTA DE PAPEL PERFORADO. Los datos se registran en una cinta perforando agujeros redondos. La cinta está ordenada en columnas y filas. Un carácter se codifica mediante una perforación o una combinación de perforaciones en una columna.

c). CINTA MAGNETICA: Es un medio para almacenar archivos -- grandes que se leen y procesan en forma secuencial. Las separaciones entre registros sirven para identificar los diferentes registros. No obstante, en muchos casos se combinan varios registros para formar un bloque y se transfieren al procesador como - una unidad, a fin de ahorrar espacio en la cinta y acelerar la - entrada de datos. Para tener acceso a los datos almacenados en - una cinta magnética se emplea una unidad de cinta. La cinta magnética es de plástico cubierta por un lado con una capa de óxido de hierro que se puede magnetizar.

d). DISCOS FLEXIBLES: Diskette o disco flexible, es un disco delgado magnético en que los programas y datos pueden almacenarse y recuperarse rápidamente es mucho más veloz que en la cinta de - cassette, pero más costoso. Hay algunos otros discos auxiliares - para el almacenamiento de la computadora, entre ellos el disco de Winchester que consiste en un disco rígido magnético dentro de un recipiente sellado, recorrido por una cabeza que prácticamente no lo toca, por lo cual no lo desgasta.

e). LECTORES DE CARACTERES DE TINTA MAGNETICA: Los documen-- tos son previamente codificados con números y símbolos impresos - con tinta especial que contiene partículas magnetizables de óxido de hierro. Estos documentos se colocan en el estante de entrada - de datos de una unidad de lectura y clasificación. Conforme en--- tran a la unidad lectora, los datos pasan a través de un campo -- que magnetiza las partículas contenidas en la tinta; después in-- terpretar los caracteres conforme los documentos pasan a través - de la unidad de lectura. Los datos que se están leyendo pueden introducirse directamente en la Unidad Central de Procesamiento o - pueden transferirse a la cinta magnética para su procesamiento -- posterior.

f). LECTORAS DE CARACTERES OPTICOS: Dispositivos en formas - de plumas, capaces de leer ópticamente etiquetas codificadas, que son un patrón de líneas impresas sobre un objeto que lo identifica y contiene información sobre él que puede leerse en la computadora recorriéndolo con una pluma luminosa. Ahora es común en los artículos envasados.

g). TERMINALES: Son dispositivos periféricos que suelen con-

sistir en un teclado y una pantalla que puede enlazarse con una - red de computadoras utilizando a veces la línea telefónica como - enlace (modem), entre las terminales más importantes se encuen--- tran las siguientes:

LAS TERMINALES TELEIMPRESORAS: Para captar o introducir da-- tos, cuentan con un teclado parecido al de una máquina de escri-- bir y una impresora interconstruída para registrar lo que se haya teclado.

LAS TERMINALES PORTATILES DE CAPTACION DE DATOS: Tienen te-- clados de tamaño reducido, reciben energía de baterías y se emple an para enviar datos a una computadora y recibir información pro- veniente de la Unidad Central de Procesamiento.

LAS TERMINALES PARA OPERACIONES FINANCIERAS: Conocidas como terminales de punto de venta y de transacciones financieras al -- respecto señala Donald Sanders H., " son dispositivos de aplica-- ción especial que se utilizan en las tiendas de venta al menudeo y en las instituciones financieras. Las terminales de punto pue-- den reducir el tiempo que debe esperar el cliente cuando va a pa- gar sus compras y pueden actualizar directamente los archivos en línea de las aplicaciones de cuentas por cobrar, control de inven tarios, y análisis de ventas."(I)

LAS TERMINALES DE DESPLIEGUE VISUAL: Se utiliza el teclado - de una terminal para introducir datos a la Unidad Central de Pro- cesamiento (UCP) y se usa un tubo de rayos catódicos para mostrar los datos de entrada y recibir información procesada y mensajes -

(I) Donald Sanders, Informática: Presente y Futuro, pág. 249, Edi t. McGraw- Hill, México, 1987.

provenientes de la computadora. El usuario puede emplear una pluma luminosa unida a la terminal en lugar del teclado para seleccionar una respuesta o para solicitar más información.

LAS TERMINALES INTELIGENTES: Aparte de teclados para entrada, que es el medio de comunicación con la UCP, y una impresora o pantalla para recibir salida, éstas cuentan con un microprocesador y algún almacenamiento interno. Pueden editar datos y consolidar los de entrada antes de enviarlos a la UCP. Los trabajos pequeños de procesamiento de datos pueden ser manejados por la terminal sin necesidad de interactuar con la UCP más grande.

SISTEMAS DE ENTRADA POR MEDIO DE LA VOZ: Estos como señala Donald Sanders H., " convierten el habla humana en señales eléctricas que la computadora puede reconocer ", pueden ser un micrófono, un teléfono, etc. (2)

Hay muchos problemas por resolver en el reconocimiento de la voz, ya que se le está utilizando en aquellas aplicaciones en que el teclado no es práctico para la introducción de datos. Los sistemas de visión electrónica emplean cámaras de television para alimentar imágenes a las computadoras, las cuales a su vez -- comparan los patrones detectados con las imágenes almacenadas -- que su programa les permite reconocer. Se están utilizando ya robots con estos sistemas de visión en la tareas de seleccionar -- piezas, verificar la calidad de objetos ensamblados y realizar labores de ensamble.

UNIDAD CENTRAL DE PROCESAMIENTO: Es el cerebro del control de la computadora, donde se enlazan entre sí todas las partes --

(2) Idem.

del sistema y donde tienen lugar los cálculos y el manejo de los datos. Aquí se alojan los circuitos que regulan la ejecución de - las instrucciones de los programas. Se integra de los componentes siguientes:

SECCION PRIMARIA DE ALMACENAMIENTO (MEMORIA): Es un dispositivo o una serie de dispositivos capaces de almacenar información temporal o permanentemente en forma de patrones de unos y ceros - binarios. La computadora lee la información en la memoria o, en - ciertos casos, también escribe información en ella cuando opera,- se divide en:

I.- MEMORIA INTERNA: Consiste usualmente en chips de silicio que se hallan dentro del cuerpo de la computadora. Algunos de e-- llos contendrán información que se mantiene permanentemente y que sólo puede ser leída y no se borra cuando se apaga la computadora (no volátil, memoria de sólo- lectura). Otros chips representan - la memoria de trabajo de la computadora, donde puede almacenarse información temporalmente cuando corre el programa y se pierde al apagar la computadora (volátil, memoria de acceso aleatorio). En consecuencia, hace falta tener una memoria de apoyo fuera de la - computadora.

2.- MEMORIA EXTERNA: Suele consistir en una cinta o disco -- magnéticos en los que se almacena la información binaria que la - computadora solicita cuando se requiere. La información no se --- pierde cuando la computadora se apaga.

SECCION ARITMETICO- LOGICA: Todas las computadoras almacenan números, letras y otros caracteres en una forma codificada. Todos los caracteres se representan mediante una cadena codificada de -

de dígitos binarios (bits) que se tratan como una unidad. Los números binarios (unos y ceros) permiten simplificar el diseño de las computadoras. Se puede utilizar un sistema de codificación - de cuatro bits del tipo decimal codificado en binario (BCD) para representar números decimales, pero se usan códigos de siete u - ocho bits para representar caracteres en versiones alfanuméricas de BCD. En las computadoras personales se usa el código ASCII de de siete caracteres y en muchas máquinas más grandes se emplean dos códigos de ocho bits muy populares (EBCDIC y ASCII- 8).

Donald Sanders H., señala que la sección aritmética- lógica " Es la que se encarga del procesamiento propiamente dicho bajo control del programa y la sección del control selecciona, interpreta y hace que se ejecuten las instrucciones de programa en la secuencia apropiada. La velocidad con que se ejecuta una instrucción está relacionada directamente con la velocidad de reloj intrínseca de la computadora."(3)

SECCION DE CONTROL: A pesar de que no se ejecuta ningún procesamiento real de datos, la unidad de control actúa como un sistema nervioso central para otros componentes de la computadora, pues si cada uno de los dispositivos sabe cuándo y cómo actuar,- es debido a la sección, interpretación y vigilancia de la ejecución de las instrucciones del programa que la Sección de Control de la UCP puede mantener en orden y a que puede también dirigir las operaciones del sistema entero.

El procesamiento convierte los datos originales en información. Sin embargo, la interpretación de una información generalmente requiere de un juicio humano y puede variar de una persona

(3) ob. cit., pág. 204.

a otra.

El hardware de una computadora se integra también por lo que se conoce como ROM, igualmente el firmaware; que es un programa - situado permanenmeente en una memoria de sólo- lectura en la computadora.

LAS SALIDAS: Es la información que envía la computadora a -- una pantalla o a una impresora o a un almacén auxiliar de memo—— ria. Para que se efectúen las salidas son necesarios dispositivos de interpretación y comunicación entre los humanos y el sistema - de computación, a continuación se señalan los siguientes:

IMPRESORA DE CARACTER: Este es uno de los dispositivos de salida que prepara documentos que serán usados por las personas. Emplean el método de las máquinas de escribir, es decir, golpean la cara de un tipo contra una cinta entintada que toca el papel, sólo que a una velocidad de 30 a 90 caracteres por segundo, a diferencia de las impresoras de línea de alta velocidad que imprimen entre 300 y 2000 lineas de información por minuto. Son ejemplo la

IMPRESORA DE MARGARITA: Impresora que utiliza un disco, alrededor de cuyo borde hay un conjunto de caracteres de impresión. - la rueda gira con rapidez hasta que el caracter requerido queda - frente a un martinete que lo golpea contra una cinta. El disco -- puede cambiarse fácilmente por otro con diferente tipo de letra,- y la ;

IMPRESORA MATRIZ DE PUNTOS: Es una impresora que usa una serie de agujas móviles golpeadas eléctricamente para crear caracteres compuestos con un patrón de puntos.

MICROFILM: Aquí se registra la información de salida de la -- computadora.

en forma de imágenes microscópicas filmadas. A una hoja de película de cuatro por seis pulgadas, se le conoce como microficha, la cual reproduce hasta 270 imágenes del tamaño de una página, sin embargo, existen sistemas de ultrafichas que pueden almacenar mil páginas normales en el mismo espacio.

PANTALLA: Al dispositivo de salida alfanumérica y gráficas, por lo tanto sólo recibe información de salida en forma de letras, números y caracteres especiales. Además de exhibir dibujos de ingeniería, las computadoras personales también pueden mostrar por medio de gráficas, diagramas, mapas y otras ayudas visuales; las relaciones, cambios y tendencias que muchas veces están sumergidas en montones de informes alfanuméricos. Una vez que las presentaciones gráficas se exhiben de manera satisfactoria en la pantalla, los usuarios pueden preparar copias permanentes empleando impresoras, graficadores y cámaras.

RESPUESTA CON VOZ: Todos los sonidos necesarios para procesar las posibles preguntas están previamente grabados en un medio de almacenamiento; a cada sonido se le asigna una clave. Cuando se reciben los cuestionamientos, el procesador sigue un conjunto de reglas para crear en forma codificada un mensaje de respuesta, mismo que es transmitido a un dispositivo de respuesta de audio, el cual ensambla los sonidos en la frecuencia adecuada y transmite el mensaje de audio de regreso a la estación que pidió información.

Sólo cabe abundar respecto de los programas, " el conjunto de instrucciones estructuralmente dispuestas, de modo que al ser leídas y ejecutadas por el computador produzcan, recibe indistin

tamente el nombre de programa o software ", así lo señala Pedro - Antonio Prado. (4)

Muchos entendidos, sin embargo, aplican el término software exclusivamente a aquellos programas desarrollados para ser comercializados en el mercado.

Como ya hemos analizado el funcionamiento de la computadora, por lo tanto ya se hizo referencia a intrucciones de distinta naturaleza tales como:

I) Las que se introducían desde el exterior;

2) Las contenidas por el sistema operativo, dirigidas a facilitar el funcionamiento del computador y los periféricos;

3) Las correspondientes a los lenguajes de alto nivel, que - permiten adecuar instrucciones transmitidas de modo comprensible para el usuario al lenguaje de señales de la máquina, efectuando la traducción de una a otra lengua.

El objetivo de las instrucciones citadas a excepción de las primeras, está dirigido a guiar o facilitar el funcionamiento de la computadora. Se trata de programas cuya finalidad es contri--- buir al funcionamiento de la computadora, y son conocidos con el nombre de software de base, y conforman junto con el hardware el medio indispensable para que un sistema de computación esté en -- condiciones de operar.

El resto del software, es decir todos aquellos programas destinados directamente a desarrollar tareas específicas vinculadas al manejo de información y a procesos de gestión, recibe el nom-- bre de software de aplicación.

(4) Pedro Antonio Prado, La Informática y el Abogado, pág. 38, -- Edit. Abeledo- Perrot, Buenos Aires, Argentina, 1988.

LOS LENGUAJES: Al respecto señala Pedro Antonio Prado, " se trata de lenguajes que utilizan representaciones mnemónicas o -- símbolos para las instrucciones fáciles de recordar. El programador debe escribir todas las instrucciones que tiene que realizar la computadora, pero se evita tener que describir todos los pasos imprescindibles para dar una orden, tal como sumar o restar, pues el lenguaje ensamblador se ocupa de hacerlo, bastando entonces con indicar el nombre del código."(5)

Entre los lenguajes de alto nivel tradicionales podemos mencionar el ALGOL, BASIC, COBOL, FORTRAN, PASCAL, LENGUAJE DE AUTOR, etc.

En los últimos tiempos son muchos los nuevos lenguajes que vienen desarrollándose, incluso con distintas finalidades, como el UNIX, PASCAL TURBO, C, etc.

ALGOL: Es uno de los lenguajes de alto nivel, usado muy a menudo por los matemáticos.

BASIC: Lenguaje de programación de alto nivel orientado al procesamiento conversacional de aplicaciones lógico-matemáticas.

COBOL: Lenguaje de programación de alto nivel concebido para aplicaciones empresarias.

FORTRAN: Lenjuaje de alto nivel usado principalmente para problemas científicos y matemáticos.

PASCAL: Lenguaje de alto nivel preferido por muchos al BASIC para trabajos de programación en general.

LENGUAJE DE AUTOR: Lenguaje de muy alto nivel que permite

(5) ob. cit., pág. 43.

a quienes no dominan la programación en BASIC, por ejemplo, escribir programas de aplicación, porque el lenguaje de autor requiere poco más de la escritura de instrucciones en inglés ordinario.

CLASES DE COMPUTADORAS: Se dividen en MINICOMPUTADORA, MACRO COMPUTADORA, y SUPERCOMPUTADORA.

MINICOMPUTADORA: Es una máquina pequeña de aplicación general. De 16 y 32 bits, se han utilizado en funciones especializadas de control y de aplicaciones generalizadas de procesamiento de datos. Las organizaciones también emplean actualmente miles de minis como procesadores satélite en redes de procesamiento distribuido de datos.

MACROCOMPUTADORA: Es generalmente más poderosa (y más costosas) que las minis, pero en éste caso también existe un traslape considerable entre las superminis grandes y las macrocomputadoras su tamaño va desde muy grandes casi siempre se agrupan bajo designaciones de familia. La mayor parte de las macrocomputadoras pequeñas son básicamente máquinas de 32 bits pero los sistemas más grandes pueden mantener 48,60 o 64 bits a la vez.

SUPERCOMPUTADORA: Es la computadora más grande, rápida y costosa que existe. Aunque su número es reducido, la supercomputadora es un recurso apreciable pues está diseñada para procesar complejas e importantes aplicaciones científicas.

IMPLICACIONES DE LAS COMPUTADORAS

Se puede decir que dada la interdependencia de intereses políticos, económicos y sociales, aunados desde luego al uso de la computadora, originan implicaciones tanto positivas como, negativas, en éstos respectivos ámbitos, señalados:

a). Mejor Servicio;
b). Aumento en la productividad;
c). Cambios en la competencia;
d). Problemas en el diseño de sistemas de información;
e). Problemas en la estructuración de la empresa;
f). Problemas por la concentración de poder;
g). Problema de desempleo;
h). Nuevas oportunidades de trabajo;
i). Mayor satisfacción en el trabajo;
j). Despersonalización;
K). Privacia;
i). Vigilancia;
m). Favorecimiento del progreso técnico;
n). Favorecimiento de la economía;
o). Amenaza a la democracia;
p). Mal funcionamiento técnico;
q). Amenaza a la identidad cultural, y
r). Dependencia tecnológica exagerada.

TIPOS DE INFORMACION

a). Científico- técnica;
b). Económica y social;
c). Educativa y cultural;
d). Comercial y financiera;
e). Administrativa;
f). Seguridad, y
g). Sobre las personas.

Para el Dr. Julio Téllez Valdes, los delitos informáticos, " son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin " (concepto atipico) o " las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin " (concepto típico); para el italiano Carlos Sarzana, citado por el aludido Dr.,(6) son " cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".(7)

Por su parte la Dra. Ma. de la Luz Lima, nos habla de delitos electrónicos, para quien en un sentido amplio los entiende, como " cualquier conducta criminógena o criminal que en su realización haga uso de la tecnología electrónica, ya sea como medio o fin ", y en un sentido estricto, se refiere exclusivamente al delito por computadora, en los siguientes términos, " es cualquier acto ilícito penal en el que las computadoras, su técnica y funciones desempeñan un papel ya sea como método, medio o como fin."(8)

Parker habla de abusos de computadoras, en lugar de crímenes de computadoras, el cual es referenciado por la Dra. en comento, para quien dichos abusos son, " cualquier acto criminógeno asociado con la tecnología de la computadora en el cual una víctima ha sufrido una pérdida, y el autor intencionalmente ha obtenido una ganancia."(9)

(6) Julio Telléz, Derecho Informático, pág. 105, segunda edición, U.N.A.M., México, 1987.
(7) Idem.
(8) Ma. de la Luz Lima, Delitos Electrónicos, págs. 99-100, Revista Criminalia, Año L, Nos. 1-6, Edit. Porrúa, S.A., México, 1984.
(9) Idem.

III.D. CARACTERISTICAS

a) DISCRESION. Se podría llamar a ésta delincuencia con un sólo nombre " discreta ", tratándose del comportamiento delictivo que del perjuicio engendrado.

Fuera de los casos, dentro de los cuales hay reproducción, destrucción o desaparición de un objeto (cinta magnética, diskettes, listing...) las consecuencias son en ellos mismos -- grandemente banales.

b) DE CONSECUENCIAS DIRECTAS. Tales como modificar (por alteración, adición, borrar, reemplazo...) los informes que electrónicamente se registran en la memoria de una computadora, que se trate de una base de datos o de un programa de convenio.

c) SON CONDUCTAS CRIMINOGENAS DE CUELLO BLANCO. Luis Marco Del Pont, citando a Sutherland, quien definío a éstas conductas " como aquellas cometidas por una persona respetable, de elevada condición social, en ejercicio de su profesión ", vemos al desdoblar los elementos de la definición, que en el tercer o sea; en el ejercicio de su profesión, es donde los perpetradores de los delitos por computadora los cometen. Toda vez que los nuevos sistemas de información son manejados por profesionales especialmente capacitados para ello, gentes por lo general muy bien preparadas. El personal de los centros informáticos tiene a su vez la - capacidad técnica y la posibilidad de hacer uso alusivo del sistema; hay una correlación entre capacitación y propención a éstas acciones.

(IO)

(IO) Luis Marco Del Pont, Manual de Criminología, pág. I64, Editorial Porrúa, S.A., México, I986.

Para Simonetti y Virgolini, no son sólo los delitos de cuello blanco, " un resultado de capas de inmunidad o vacios de control que existen natural e indebidamente en una sociedad compleja, o si, por el contrario, son ciertas actividades las que, a despecho de su nocividad para extendidos sectores sociales, -- crean reglas de juego asumidas por todos y las que se hacen in-- vulnerables o difícilmente alcanzables."(II)

Por su parte el Dr. Roberto Tocaven, refiriéndose a la criminalidad de cuello blanco, la divide en dos vertientes:

" I.- La del delincuente de cuello duro que sabe encontrar actividades marginales entre dos artículos del Código Penal; y

2.- La del que incluso, cometiendo delitos penados en el Código, no es capturado por los medios de que dispone para ocultarse. "(I2)

d) SON ACCIONES DE OPORTUNIDAD. Ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

e) SON ACCIONES DESHONESTAS. Son acciones que se encuentran en la periferia de la informática, dejan de ser pertinentes cuando la deshonestidad se situa en el corazón mismo de la informática.

f) SON ACTOS CRIMINOGENOS ASOCIADOS CON LA TECNOLOGIA DE - LA COMPUTADORA. En el cual el pasivo ha sufrido un menoscabo, y

(II) José M. Simonetti y Julio E.S. Virgolini, Del Delito de Cuello Blanco a la Economía Criminal, pág. 8, Cuaderno del inacipe Núm. 35, México, I99I.

(I2) Roberto Tocaven, Psicología Criminal, pág. I8, Cuaderno del inacipe No. I, México, I990.

el perpetrador ha alcanzado una ganancia.

g) INTERCONTINENTALES. A veces, no hay ninguna especie de contacto físico con los organos de la computadora; todo se efectúa a distancia, algunas veces a miles de kilómetros.

h) DE EFECTOS INMATERIALES. Se dejan difícilmente encerrar dentro de los límites territoriales exactos, son difíciles de localizar.

i) SON POCO VISIBLES. Firmar un cheque, escribir una carta olvidar enviar una convocatoria, etc.

k) NO DEJAN HUELLA. Lo que es raro y verdaderamente exacto pero son operaciones extremadamente difíciles de desenmarañar.

l) INCUANTIFICABLES. Difíciles de medir, pero particularmente durables. Su costo de fabricación es bastante caro, pero el de su producción es al contrario muy bajo.

III.E. DELITOS INFORMATICOS MAS COMUNES

Carlos Correa, citando a Uhlrich Sieber el cual ordena los delitos informáticos en las siguientes categorías:

" a) Fraude por manipulaciones de un computador contra un sistema de procesamiento de datos;

b) Espionaje informático y robo de software;

c) Sabotaje informático;

d) Robo de servicios;

e) Acceso no autorizado a sistemas de procesamiento de datos, y

f) Ofensas tradicionales en los negocios asistidos por un computador." (I3)

(I3) Carlos M. Correa, Derecho Informático, pág. 296, Editorial Depalma, Buenos Aires, 1987.

III.a. FRAUDE INFORMATICO

La primer categoría de los delitos informáticos, abordada en el apartado anterior de Uhlrich Sieber, citada por Carlos Correa," puede perpetrarse por manipulaciones; incluye el -- cambio de datos o informaciones para obtener un beneficio económico." Estos pueden afectar datos que representen activos (depósitos monetarios, créditos, etc.), o bien objetos materiales -- (manejo de inventario). Esta acción puede basarse en la intro-- ducción de datos falsos en la computadora (diversos casos de éste tipo se han dado en entidades bancarias), o bien en la modificación de los resultados. También resultan del cambio en los programas de computación, tal como las formulas de:

(I4)

CABALLO DE TROYA

Un Caballo de Troya es un programa que actúa como una utilería útil o un juego entretenido, pero que añade un ¡ Te atrapé ¡, asi como los griegos se ocultaron para poder entrar al fuerte de Troya mediante el regalo de un enorme caballo de madera, el programa Caballo de Troya parece un regalo, hasta que -- surge la trampa; introduciendo instrucciones para que el programa realice funciones no autorizadas, por ejemplo, acreditar la cuenta bancaria o un salario en la cuenta designada por el delincuente.

El perpetrador requiere acceso al programa o a la computadora, un conocimiento basto, servicios de pruebas para asegurar que el Caballo de Troya funciones correctamente, y finalmente llevar a la práctica su plan.

(I4) Idem.

Algunos fraudes que se pueden realizar por computación son los citados ulteriormente:

- Fraudes Disfrazados;
- Fraudes por Computadora que van a la basura;
- Procedimientos de Auditoría Inadecuados;
- Debilidad del Control Interno;
- Tácticas de Retraso;
- Proveyendo Demasiada Información;
- Fraudes por Desembolsos;
- Alteraciones de Precio y otros Descuentos, etc.

En el primer caso, la apariencia de errores de computadora, es el ocultamiento ideal para los fraudes por computadora, porque todo el mundo sabe y acepta la noción de que éstas máquinas cometen errores, algunas veces graves. Usando este tipo de decepción, es lo que se llama fraude disfrazado, un perpetrador puede, tener dos opciones como proceder. Puede por un lado crear el error en condición o trabajar con el ya existente. Por cierto han habido casos donde la verdadera existencia de errores reales eran de tal naturaleza de demostrar a su autor como el sistema puede ser aplastado.

El otro error, es el tipo de pista de Iceberg, se da cuando algunos records, son falseados como resultado de una modificación en el sistema, a manera de entrar, o de cambiar otros records.

El paradigma de éste primer caso de fraude, lo constituyen, algunos errores de derechohabientes (jubilados) de Insti-

tuciones de Seguridad Social, en los cuales aparecen después de éstos como personas fallecidas, por lo tanto se les retienen -- sus pagos.

En el segundo caso, una endidura del sistema puede, permitir hacer entradas por hacer; y una vez realizado el acceso - se pueden realizar manipulaciones de los programas y los datos.

Son ejemplo de éste tipo de fraude, la sobreproducción de boletos ganadores por una computadora, en determinadas predicciones de eventos deportivos, juegos y apuestas.

El tercer caso consiste en, generar impresiones vía telefónica por medio de una computadora, inflando los inventarios y las ventas.

-Estas discrepancias en la contabilidad, ocurren en varias compañías.

El cuarto caso se presenta, con algunos astronómicos -- fraudes, cuando algunos Estados se debilitan la auditoría interna; ocasionando el extravio o perdida de un rastro de auditoría obteniendo lucros excesivos.

El quinto caso consiste; en los retrasos como una excusa para no pagar. Los autores de estos delitos se ven favorecidos por el tiempo extra que da varias opciones, tomar más, darse a la fuga, o para gastarlo todo.

Este caso se ilustra, de la siguiente manera en las Instituciones Financieras (bancos, casas de bolsa), así como Seguros, en los cuales directivos retrasan los intereses o primas - correspondientes, en algunos hasta llegan a la quiebra, e impiden se propalen las noticias veraces, y comunican a las demás - Instituciones análogas, que los pagos se han retrasado, por causa del cambio del sistema de computación.

El sexto caso, puede ocurrir cuando alguien averiguando, datos concernientes a los antecedentes personales y financieros, telefónicamente, incluyendo el nombre de la Compañía de Seguros o de alguna Institución Financiera, el perpetrador puede realizar manipulaciones crediticias, que se encuentren registradas en los archivos de la computadora.

El septimo caso; concierne a los sobrepagos deliberadamente o pagos adicionales, muy seguido por servicios o inventario no recibidos. Estos sobrepagos son cubiertos de varias maneras, tales como faltas de inventario que caen dentro de las tolerancias aceptadas. A manera de obtener dinero en efectivo fuera del sistema, vendedores audaces o a otras personas que se deben de pagar se establecen dentro de la computadora. Esta y la entrada son arregladas para poder operar el sobrepago.

Otra característica común es el uso de apartados postales u otras direcciones especiales. El perpetrador o el complice, establecen una cuenta bancaria en el nombre del vendedor supuesto o la persona que se le debe pagar y usa esa cuenta para cobrar cheques fraudulentos de desembolso.

Las prácticas en comento, son realizadas por operadores de terminales de computadoras, los cuales algunas veces se las ingenian para recibir cheques de pensionados bajo diferentes nombres, éste acto es sencillo. Cuando llega la noticia de la muerte de un pensionado, se debe introducir en la computadora, de manera de terminar los pagos. Luego en lugar de meter la noticia de la muerte, introducen el cambio de domicilio y mandan el cheque correspondiente al apartado postal. Cuando los --

auditores verifican si los pensionados aún estan vivos, enviando cartas para checar tal situación. Las cartas llegan a la dirección fraudulenta. Es simple la cuestión para el operador de terminales, contestar afirmativamente.

El octavo caso, consiste en viejas prácticas de alteración de precios que se ha unido con la revolución de la computadora. El nuevo movimiento es que la computadora mantiene los datos, y descuentos no autorizados, se pueden perder en multiples entradas automatizadas.

Por ejemplo; cuando empleados usando la computadora, para facturar, cantidades inferiores de mercancias o productos; de las que realmente se venden. Los casos son descubiertos, después de que otros empleados, detectan haber visto a alguna persona no autorizada usando el teclado de la computadora.

Algunas otras especies de fraudes por computación son:

- Convirtiendo Prematuramente Gris a su Auditor;
- Convirtiendo a su Programador en Vacacionista;
- Los Fraudes de la Computación del Pega y Corre;
- Instalaciones;
- Ataques Desafuera, y
- Otros Debitos Fraudulentos.

III.c. TERRORISMO INFORMATICO

Esta acción es violenta y se da cuando se destruyen o deterioran los centros neurálgicos computarizados, o bien cuando hay un apoderamiento de los mismos.

El sabotaje de la informática puede tomarse, sea por - una forma violenta, o bien sea una forma no violenta.

En el primer supuesto, se consideran el incendio o a-- tentado con explosivo para destruir los centros de tratamiento de la informática.

En el segundo supuesto, es mucho muy sutil; y puede -- comprender el deterioro de los soportes lógicos o de las informaciones tomadas por la computadora hasta la simple anomalía o error introducido maliciosamente en un programa o en -- las informaciones almacenadas por la máquina.

Algunos tratadistas, así como algunas legislaciones -- clasifican los virus computacionales en el delito que nos ocupa.

Peter Norton y Paul Nielsen, definen al virus computacional en los siguientes términos;

" Cualquier programa que se reproduce a sí mismo mediante la infección de otros programas."(I5)

Es similar el virus computacional a un virus biológico. El virus biológico ataca una célula húesped y crece dentro de ella hasta que está listo para explotar y buscar otras celu-- las donde atacar.

De acuerdo con la definición; esto limita a los virus infectores de:

Programas ejecutables (archivos .EXE y .COM)

Overlays y manejadores (.OVL, .SYS y .DRV)

DOS (COMMAND. COM y otros)

(I5) Peter Norton y Paul Nielsen, Norton Antivirus, Pág. I2,- Edit. Prentice Hall Hispanoamericana, S.A., México, I992.

El programa de iniciación en el sector de arranque o la tabla de partición de un disco.

Los virus caen en dos grandes categorías de acuerdo al archivo que infectan:

- Los que infectan los programas; y
- Los que infectan el sector de arranque.

COMMAND. COM, se enlista aparte, puesto que varios de los que infectan programas sólo infectarán otros programas, excepto a COMMAND. COM, para evitar una fácil detección.

Norton Anti Virus identifica 1008 clases de 348 virus.

Algunos de ellos son:

- Camaleón
- Gusano
- Sembradores
- Darth Vader
- Devil's Dance
- 4096
- SeviL etybwodahs - Shadowbyte Lives
- El terrorista
- El investigador
- Carmen Sandiego
- Miguel Angel, etc.

Hoy en día, muchas funciones médicas están relacionadas con las computadoras. Las farmacias utilizan computadoras para advertir interacciones peligrosas de medicinas o alergias a éstas. Los exploradores médicos (MRI y CAT Scan) utilizan computadoras para el análisis gráfico de los resultados de exploración. Los equipos para rescates de emergencia utilizan enla-

ces computacionales para enviar signos vitales a los doctores de las salas de emergencia. La estación de enfermeras en las unidades de cuidado intensivo utiliza monitores centralizados de los signos vitales.

De nuevo, estos son ejemplos de computadoras que realizan funciones críticas respecto a la vida. Es probable que un médico conserve su historia clínica en una red de área local de computadoras personales.

El ataque de un sofware perverso puede costar una vida.

En la reunión de la Asamblea General en San Francisco, California, después de concluir el XI Congreso Mundial de Informática, la Federación Internacional para el Procesamiento de la Información (IFIP) ha lanzado una seria advertencia sobre la amenaza mundial que representan los virus informáticos.

Existiendo ya cientos de virus informáticos,"todos los países deben ser conscientes de las desastrosas consecuencias que estos virus pueden tener para los sistemas informáticos."(16)

Pudiendo ocasionar cuantiosas pérdidas económicas y de personal y, en el caso de sistemas de control industrial. Aparte de grandes, las pérdidas ocasionadas por los virus informáticos, así como sus otros efectos, están teniendo un notable impacto internacional, debido al uso creciente de redes de computadores como soporte básico de manipulación de información de un número cada vez mayor de compañías e instituciones.

El acuerdo tomado unánimamente por la Asamblea General de

(16) Instituto Nacional de Estadística, Geografía e Informática, Boletín de Política Informática, pág. 9, Año XIII, Núm. 4, México, Abril de 1990.

IFIP, que representa a 64 países, fue hacer una seria llamada de atención a los gobiernos, instituciones académicas, fabricantes y profesionales informáticos de todo el mundo, en los siguientes términos:

" En vista de las potencialmente graves e incluso, fatales consecuencias resultantes de la introducción de virus en los sistemas informáticos, IFIP pide urgentemente que:

1.-Todos los profesionales de la informática sean conscientes del gran peligro que suponen los virus informáticos.

2.-Todos los profesores de informática alerten en forma clara a sus alumnos sobre los peligros de estos mismos virus.

3.-Todos los editores se abstengan de publicar detalles de programación de virus informáticos.

4.-Los profesionales informáticos de todo el mundo no distribuyan código de virus informáticos a menos que sea como parte de un proceso de investigación, y de forma controlada y, los constructores de sistemas de detección y neutralización de virus informáticos dejen de distribuir virus como parte del juego de pruebas de dichos sistemas.

5.-Los gobiernos, universidades y fabricantes de sistemas informáticos dediquen mayores recursos a la investigación y desarrollo de nuevas tecnologías que permitan proteger a los sistemas informáticos de los desastrosos efectos de los virus.

6.-Los gobiernos adopten las medidas que conduzcan a que la distribución de virus informáticos sea delito."

(I7) ob. cit, págs. I0-I. (I7)

Como segunda categoría, de éste delito, tenemos a la - Bomba de Tiempo, que se implanta en un programa molesto, se - espera cierto acontecimiento, y entonces destruyen programas y datos.

También se sabe que las bombas de tiempo pueden ser implantadas en un programa por programadores contratados.

La tercer categoría la constituye, la Rutina - Cáncer, que distorciona el funcionamiento de aquél mediante instrucciones que se autoreproducen, o bien al equipamiento en sí.

III.e. ESPIONAJE INFORMATICO

Se refiere principalmente a la obtención, generalmente por parte de competidores, de resultados de investigaciones, - direcciones de clientes, etc. Pueden ser cometidos introduciendo programas copiadores, o por otros métodos (la radiación -- electrónica que emite una terminal de computación puede ser -- captada y registrada sin mayor complicación).

Ahora bien ésta forma de piratería puede tornarse en - espionaje en el sentido más preciso del término cuando es usado por Estados Extranjeros para el mantenimiento de inteligencia con fines de orden militar, político o económico. No sólo por el uso de redes de computadores, sino por el impacto internacional de la telemática interactiva que ofrece la facilidad para la perpetración de éste delito, efectuándose a distancias exorbitantes, y en su mayoría pueden ser ilocalizables éstas - acciones. Pueden ser realizadas en las siguientes formas:

a).- Alterando;

b).- Desviando;

c).- Captando;

d).- Usando, o bien

e).- Destruyendo, soportes físicos o lógicos inautorizadamente.

III.f. ULTRAJES Y DIFAMACION INFORMATICOS

El primero concierne a la posibilidad de realizar sugerencias o proposiciones obcenas a los buenos modales por la vía de la informática.

En el segundo concierne a la distorsión de ciertos medios publicitarios o redes informativas, en los cuales se puede variar un soporte de lo escrito, de la palabra o de la imagen, pero que decidir si hubo difamación pública por medio de la informática.

La respuesta es fácil la llave del problema se encuentra en las condiciones de acceso a la red telemática; si ésta está libre, la difamación será pública; si supone lo contrario a la adquisición de un código confidencial, dejará de ser pública.

Son posibles éstas acciones por la vinculación de la informática con la telemática, que cada día es más estrecha y se extiende no sólo al sector comunicaciones sino a otros campos tales como la medicina, instituciones crediticias, instituciones de investigación, la política, etc.

En la presente década, como ya hemos señalado anteriormente la delincuencia informática se está propalando considerablemente, y es en éste preciso campo donde puede modificarse la información, siendo tal fácilmente advertible de modo que nuestros sentidos pueden apreciarla.

Esta conducta se presenta cuando una persona ilegalmente, modifica datos electrónicos magnéticos u otros datos memorizados no visibles o no legibles directamente, en un proceso informático, sin tener autorización para ello.

También se configura éste ilícito cuando se procede a tal falsificación de datos memorizados licita o ilícitamente, o utilice estos datos alterados.

Estas acciones entrañan la persepción visual, pero en la aplicación de la incriminalidad de falsear la escritura por razón de la exigencia de un escrito. Sin duda la dificultad será fácilmente levantada cuando, lo que es muchas veces el caso, la maquina habrá editado un papel a la salida: una factura falsa, una falsa contabilidad, en el momento que se estime el valor probatorio.

Pero que decidir cuando el resultado de una manipulación informática se queda encerrado de alguna manera en la máquina, se puede considerar que la memorización de una información por una computadora es una forma de escritura.

Más aún respecto a la conexión y autenticidad de información, respecto a las nuevas formas de dinero, especialmente " Dinero de Plástico " y " Tarjetas ya pagadas ", (como tarjetas de teléfono).

Vemos, pues que los avances cibernéticos e informáticos, aportan novedosidades, que dadas sus características y usos, son empleadas por el hombre, tanto para su provecho, como para su perjuicio.

III.h. ABUSO DE CONFIANZA

Hasta ahora, en diversas legislaciones penales, el fraude informático ha caído en equiparaciones con el abuso de confianza, sin embargo son dudosas éstas equiparaciones, toda vez que el abuso de confianza, requiere de la disposición de una cosa mueble; mismo que no es posible porque la información es un bien intangible, por lo cual descarta la posibilidad de ser una cosa mueble y por lo tanto de colmar dicho tipo.

III.i. ACCESO NO AUTORIZADO

Se refiere éste delito informático, a la entrada ilegal o inautorizada de una persona a informaciones o programas informáticos (sistemas de procesamiento de datos). No sólo se trata del mero acceso a una computadora, sino también la entrada a una casa o a un lugar prohibido.

III.k. ALGUNOS OTROS DELITOS

Entre ellos la violación del secreto profesional, violación del secreto de fabricación y corrupción de funcionarios o de empleados, previstos en la Ley del 6 de enero de 1978 de Francia, y aun cuando se trate de informaciones nominativas, la cual regula la revelación o malversación de secretos; constituyendo éstas divulgaciones llevar alcances a la reputación, a la consideración de la persona o la intimidad de su vida privada.

Así mismo contempla la Ley en cita, la distorsión de informaciones nominativas.

La informática siendo en efecto la ciencia del tratamiento automático de la información. Para llegar a éste resultado, utiliza máquinas, las computadoras, y sus accesorios o periféricos (hardware, el material). Estas máquinas no funcionan enteramente solas, pero según los programas, o conjuntos de instrucción hacer funcionar toda una serie de operaciones elementales sobre la computadora escrita según un lenguaje particular. El conjunto de programas que permiten hacer funcionar se llama logicial (software), en fin estos elementos son base de la informática.

Entonces precisamente estos diversos elementos que componen la informática pueden ser el objeto de actos delictuosos sea en vista de apropiarselos, destruirlos o deteriorarlos.

Ejemplos de ésta categoría:

a) El Sabotaje de la Informática

La Piratería de la Informática a su vez se subdivide en: - Apropiación ilícita del hardware y el robo del tiempo - máquina.

- Apropiación fraudulenta del logicial y de informaciónes.

El Dr. Julio Tellez Valdez, cita como ejemplos de ésta categoría 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 computariza-- dos.

f) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etc." (I8)

Como medio de los delitos

La aparición y el desarrollo de la informática han dado a los malhechores medios sin precedente para cometer infracciones penales. Sin duda, la mayoria de éstos hechos delictuosos podian ser anteriormente cometidos por otros medios; así como atentados a la vida privada y las libertades podian ser perpetrados por los archivos manuales antes de ser por tratamientos automatizados de informaciones nominativas. Es porque la unión entre la informática y el delito es menos estrecha que -- cuando la informática es objeto del delito.

La informática, como medio del delito, puede ser así para cometer los delitos más diversos, de lo que se trate de infracciones contra los bienes o infracciones contra las personas.

La Dra. Ma. de la Luz Lima, da como ejemplos de ésta categoría los siguientes:

" a) Interceptar teléfonos con transistores, beepers, radios bugs; se usa mucho para realizar el espionaje industrial,- el sabotaje político, etc.

(Iò) Julio Telléz, ob. cit., pág. I07.

b) Lectura de información confidencial para bloquear la - capacidad operativa de la víctima y cometer sabotaje industrial.

c) Lectura de ficheros judiciales para extorcionar.

d) Lectura de datos confidenciales para chantajear.

e) Simulación de un servicio que no existe."(I9)

III.G. CONTROL PREVENTIVO Y CORRECTIVO

Las estrategias para la prevención y control de los delitos por computadora constituyen el control preventivo, y segundo, es decir, el control correctivo lo conforman todos los mecanismos legales que tiendan a evitar la comisión de estos ilícitos.

En el XIII Congreso Internacional, de Leyes Comparadas, - celebrado en Montreal, Canadá en I990, dirigido por el Dr. Uhlrich Sieber, se abordaron las siguientes medidas de seguridad:

" I) Voluntary Security Measures for Computer Users
2) Enforcement of Security Measures
3) Education and Deterrence of Potencial Perpetrators "

" I) MEDIDAS DE SEGURIDAD VOLUNTARIAS PARA LOS USUARIOS
2) MEDIDAS DE FORTALECIMIENTO DE SEGURIDAD
3) LA EDUCACION Y DISUACION DE PERPETRADORES POTENCIALES "(20)

Las primeras incluyen tanto la seguridad educacional como personal, la seguridad física, la seguridad organizacional y técnica, auditoría interna, seguro de delitos por computadora, al -

(I9) Ma. de la Luz Lima, ob. cit., pág. I0I.

(20) Uhlrich Sieber, XIII Congreso Internacional, de Leyes Comparadas, Montreal, Canadá, pág. 8, I990.Traducción de Erika Tapia.

igual que la formulación de un contrato.

Para mayor abundamiento respecto de la seguridad a continuación se señalan cinco objetivos que persigue:

a) Seguridad Lógica: Cada computadora tiene que tener suficientes defensas electrónicas, detención y capacidad de recuperamiento, y resistencia a la detección de anomalías. Esto último - junto con la implementación, seguido por un seguro inicial al periódico de continuidad integral.

El problema de ataques en el marcado por teléfono en -- computadora, requiere una mejor solución de tratar de desarro-- llar mecanismos de protección para uno en computadora. Hoy día,- un simple y pequeño cambio en el programa computacional, puede - resultar significable y vulnerable.

La redundancia lógica se puede construir directamente, dentro de una computadora para la protección contra la caida del sistema.

b) Seguridad Física: Esta seguridad es la única que está - imperfecta porque las personas han requerido la operación, mantenimiento, los reparos frecuentes. En otras palabras las computadoras se deben de proteger de los factores siguientes:
Calor, frío, liquidos, gases, proyectores, virus, corriente eléctrica inadecuada, aire especialmente frío y congelamiento.

c) Seguridad Manual: Esta seguridad es la más difícil de - asegurar, es el resguardo de datos y su uso que requiere una -- coordinación de control de la aplicación de programas y el con-- trol de la fuente de datos. Esta es la más importante, ya que la

mayoría de los errores y fraudes ocurren alrededor de la periferia de las computadoras y en donde se encuentran las personas. Esta ley es también difícil pues es necesario que se estén checando consecutivamente las acciones de las personas -- personas ahí laboran.

d) **Seguridad Prudencial:** Esta seguridad se deriva de - la prudencia en la práctica y en la política. Si las técnicas computacionales hacen su trabajo en una manera segura, la motivación debe ser realizada por los dirigentes, los cuales deben insistir en su trabajo lleno de seguridad. Los dirigentes tienen que ganar la confianza de sus empleados, y viceversa. ésta convergencia da como resultado un auxilio a los emple--- ados aparte de que el dirigente conoce las habilidades del empleado para que laborará más competitivamente, y se tuvieran antecedentes del mismo.

Para que ésta seguridad sea óptima, se tiene que tener el apoyo del dirigente. Los empleados tienden a ser guia-- dos en sus trabajos por las actitudes y habilidades del diri-- gente o jefe. Obviamente éstos tienen que mantener una conducta ética y sobre todo dedicarse a seguir las políticas y prácticas de la empresa.

e) **Seguridad Social:** Esta se basa en los valores sociales. La sociedad insiste en ser servida con eficiencia y seguridad, sobre todo se tiene esa espectativa de las personas que trabajan en computadoras. Esto se da por medio de la religión, educación y por medios gubernamentales para establecer los rangos liderales y profesionales.

Las segundas medidas, esto es las medidas de fortalecimiento de seguridad son aquellas que operan informando a las víctimas potenciales en el procesamiento de datos y por medio de la consultoria de seguridad. La información relevante es específicamente donada por la seguridad independiente, fabricantes de software y hardware, seguros para compañías, Universidades, Institutos de Investigación, servicios de inteligencia y otras agencias gubernamentales.

Las terceras, consisten en los métodos más comunes para disuadir a los perpetradores potenciales, que son bajo remedios civiles y administrativos, son normalmente para la prevención de quebrantamientos contra la privacidad, y están previstos en algunas legislaciones.

IV.A. TIPOS PENALES VINCULADOS A LOS DELITOS INFORMATICOS

IV.a. ESPIONAJE

Nuestra Legislación Penal, preceptúa en el artículo - I27.-

" Se aplicará la pena de prisión de cinco a veinte años y multa hasta de cincuenta mil pesos al extranjero que en tiempo de paz, con objeto de guiar a una posible invasión del territorio nacional o de alterar la paz interior, tenga relación o inteligencia con persona, grupo o gobiernos extranjeros o le dé instrucciones, información o consejos.

La misma pena se impondrá al extranjero que en tiempo de paz proporcione, sin autorización a persona, grupo o gobierno extranjero, documentos, instrucciones o cualquier dato de - establecimientos o de posibles actividades militares.

Se aplicará la pena de prisión de cinco a cuarenta -- años y multa hasta de cincuenta mil pesos al extranjero que, - declarada la guerra o rotas las hostilidades contra México, -- tenga relación o inteligencia con el enemigo o le proporcione información, instrucciones o documentos o cualquier ayuda que en alguna forma perjudique a la Nación mexicana. " (I)

Por lo que respecta al espionaje informático, se re-- fiere a cierta piratería, que puede ser cometida introduciendo programas copiadores, o por otros métodos como es la radiación electrónica.

Ahora bien ésta forma de piratería, puede mutarse en

(I) Código Penal para el D.F., pág. 33, 52a. edición, Porrúa,- S.A., México, D.F. I994.

espionaje en el sentido más preciso del término cuando es usado por los Estados Extranjeros para el mantenimiento de inteligencia con fines de orden militar, político o económico. Dada la interacción de la telemática, éstas acciones pueden realizarse a distancias considerables, bien sea alterando, desviando, captando, usando, o bien, destruyendo soportes físicos o lógicos en forma inautorizada.

Por lo que toca al espionaje, previsto en nuestra legislación penal escapa a las acciones anteriormente descritas ya que el artículo 127 en cita, sólo contempla el mantenimiento de inteligencia con persona, grupo o gobiernos extranjeros por medio de:

- documentos;
- instrucciones;
- cualquier dato, o bien
- información.

Sobre establecimientos o de posibles actividades militares, o cualquier ayuda que perjudique a la Nación mexicana.

Al desdoblar los elementos de esta figura analizamos- que a la información a que hace referencia es obscura, no podría determinarse con claridad si se trata de aquella que es resultado de un proceso de datos, así mismo tratándose del -- delito de espionaje informático, no es posible admitir pueda mantener, en forma fisíca, ya que muchas de las veces no existe contacto físico, con los órganos de la computadora del enemigo.

Claro éste espionaje, no sólo comprende las situaciones descritas anteriormente, sino inclusive se hace extensivo al sector político interior, ya que bien es sabido por diversas fuentes informativas del espionaje existente entre los partidos políticos sobre todo en la reciente sucesión presidencial del ejecutivo federal, también localmente, así como en las diputaciones y senado, en fin a otros hechos similares; los cuales se encuentran encadenados al uso de la computadora y que han tenido una trascendencia de gran magnitud en el sentido poder cambiar hasta el destino del país, escapando de una regulación precisa ya que las reformas que ha tenido la legislación penal en los delitos electorales, no prevé ésta circunstancia.

Como vemos es menester la creación de un nuevo tipo que regule dicha situación.

IV.b. SABOTAJE

El artículo 140 del Código citado establece:

" Se impondrá pena de dos a veinte años de prisión y multa de mil a cincuenta mil pesos, al que dañe, destruya o ilícitamente entorpezca vías de comunicación, servicios públicos, funciones de las de las dependencias del Estado, organismos públicos descentralizados, empresas de participación estatal o sus instalaciones; plantas siderúrgicas; eléctricas o de las industrias básicas; centros de producción o distribución de artículos de consumo necesario, - de armas, municiones o implementos bélicos, con el fin de trastornar la vida económica del país o afectar su capacidad de defensa".

(2) ob. cit., pág. 37. (2)

Este artículo, tutela bienes y servicios públicos, de modo que si se trata de bienes no correspondientes a éste sector, no se tipificaría el delito de sabotaje.

Por lo que hace a la informática, puede realizarse de varias formas el sabotaje informático:

El violento; puede ser incendio o atentado con explosivo para destruir los centros de tratamiento de la informática.

En las incipientes Reformas que tuvo el Código Penal para el D.F., en materia de Delitos Electorales, ya que no previó todas las prácticas fraudulentas, ni los trastornos que resultan.

En los pasados comisios del 21 de agosto del año en curso, existieron muchas irregularidades en la lista nominal, aparte de las viejas formulas " como carruseles ", " Urnas embarazadas ", " rasurados ", se ampliaron porque aparecieron, " fantasmas ", " homónimos ", " dobles credenciales ", " Presiones " y " chantajes " a empleados del gobierno para votar por el partido del poder.

En lo que se refiere al tema en comento, es decir al sabotaje informático, en Chiapas, se cayó el sistema de cómputo ya que la C.E.E. electoral suspendió el suministro de información, aunque varias horas después lo restableció frente a las protestas de oposición, que sostiene que se están dando cifras maquilladas.

Creemos necesario, que nuestra Legislación Penal contemple éste delito por las razones apuntadas.

El sabotaje no violento, en materia informática puede resultar mucho muy sutil de las destrucciones o deterioro de los soportes físicos o lógicos de las informaciones tomadas por la computadora hasta la simple anomalía o error introducido maliciosamente en un programa o las informaciones almacenadas por la máquina.

Una especie de ésta forma de sabotaje informático la constituyen los virus computacionales, los cuales como se ha afirmado en el capítulo anterior, dada la interdependencia del uso de la computadora con algunas funciones médicas, constituyen un peligro a las vidas humanas, en caso de que un software perverso dañe un sistema de cómputo de un hospital o de una computadora personal de alguna clínica.

También estos virus pueden ocasionar menoscabos económicos, con consecuencias desastrosas, por ejemplo en los sistemas de control industrial, en instituciones educativas, en las instituciones bancarias, etc.

Por lo anterior y acorde a las graves consecuencias que estos originan, El Congreso XI Mundial de Informática, la Federación Internacional para el Procesamiento de la Información, recomienda en el punto número 6.- " Que los gobiernos adopten las medidas que conduzcan a que la distribución de virus informáticos sea delito."(3)

(3) Loc. cit.

IV.c. ULTRAJES A LA MORAL PUBLICA

Nuestra Legislación Penal establece en el artículo - 200.- " Se aplicará prisión de seis meses a cinco años o san-- ción de trescientos a quinientos días multa o ambas a juicio - del juez:

I.-Al que fabrique, reproduzca o publique libros, escri tos, imágenes u objetos obscenos y al que exponga, distribuya o haga circular;

II.-Al que publique por cualquier medio, ejecute o haga ejecutar por otro, exhibiciones obscenas;

III.-Al que de modo escandaloso invite a otro al comercio carnal.

En caso de reincidencia, además de las sanciones pre vistas en éste artículo, se ordenará la disolución de la socie dad o empresa.

No se sancionarán las conductas que tengan un fin de investigación o divulgación científico, artístico o técnico."

(4)

Con la telemática, se pueden hacer aún ultrajes a -- los buenos modales por la vía de la informática. La posibili-- dad ha surgido por el uso inadecuado de la red minitel, en el cual se han suscitado distorciones, algunas de ellas con fines de correspondencia amorosa. De amorosa, la comunicación puede ciertamente mutarse en obsenidad.

Analizando éste precepto vemos que se refiere a re-- producciones, actos o propuestas obscenas, no así a los ultra-

(4) Código Penal para el D.F., ob. cit., pág. 51.

jes que se puedan realizar por la información de alguna red, - por lo que creemos sea necesario la creación de un nuevo tipo penal que se adecue a la acción descrita anteriormente; ya que la telemática se convierte en un medio para manifestar vulgaridades.

IV.d. INJURIAS Y DIFAMACION

Señala el artículo 352 del ordenamiento legal que -- nos ocupa:

" No se aplicará sanción alguna como reo de difamación ni de - injuria:

I.-Al que manifieste técnicamente su parecer sobre alguna producción literaria, artística, científica o industrial;

II.- Al que manifieste su juicio sobre la capacidad, -- instrucción, aptitud o conducta de otro, si probare que obró - en cumplimiento de un deber o por interés público, o que, con la debida reserva, lo hizo por humanidad, por prestar su ser-- vicio a una persona con quien tenga parentesco o amistad, o -- dando informes que se le hubieren pedido, si no lo hiciere a - sabiendas calumniosamente, y

III.-Al autor de un escrito presentado o de un discurso pronunciado en los tribunales, pues si hiciere uso de alguna - expresión difamatoria o injuriosa, los jueces, según la gravedad del caso, le aplicarán alguna de las correcciones disciplinarias de las que permita la ley. "(5)

Este artículo prevé algunas causas por las que no se configuran los delitos; injurias y difamación por mediar el -- consentimiento de una persona sobre una producción artística,-

(5) Ibídem, pág. 97.

científica, literaria o bien cuando lo marca la ley. 82

Por lo que se refiere a cierta publicidad, donde es - posible admitirse el parecer, pero en caso contrario es decir - cuando no media el consentimiento sobre alguna producción; que ocurrirá éste artículo en comento es obscuro, en todo caso es - viable que una persona cuando la idoneidad de las condiciones - de acceso a una red así lo permitan, una vez que ha adquirido - un código confidencial, pueda transformar la realidad de un escrito, de una palabra o de una imagen.

En el sector en que más han proliferado éstas acciones es el de comunicación, es decir, la radio, la prensa y la - televisión, desde luego con el soporte de una computadora, con la cual se puede transformar la realidad de la información ya sea en los espectáculos, en los discursos, en los artículos periodísticos, etc.

Generalmente esta alteración de la realidad es advertible, por ser inconexa, reticente, inexplicable, provocando -- la decodificación de símbolos, imágenes, o letras, por ende es posible admitirse ésta mutación, por la manipulación de estos - medios electrónicos.

A juicio nuestro sería necesario crear un tipo penal acorde a la infamia que pueda originarse por el uso indebido de la computadora, respecto de la realidad de un hecho, un escrito o de una imagen, precisando la forma inautorizadamente no dando lugar a obscurantismos o aplicaciones incorrectas. Ya que en -- estos tiempos electrónicos, van surgiendo vulneraciones a síste mas que se encuentran impunes.

Establece el artículo 239 del Código en cita, " Al que cometa el delito de falsificación de títulos al portador y documentos de crédito público, se le impondrá de cuatro a diez años de prisión y multa de doscientos cincuenta a tres mil pesos.

Comete el delito de que habla el párrafo anterior el que falsificare:

I.- Obligaciones u otros documentos de crédito público del tesoro, los cupones de interés o dividendos de esos títulos

II.-Las obligaciones de la deuda pública de otra nación, cupones de intereses o de dividendos de otros títulos;

III.-Las obligaciones y otros títulos legalmente emitidos por sociedades o empresas o por administraciones públicas de la Federación, de los Estados o de cualquier Municipio, y los cupones de intereses o de dividendos de los documentos mencionados."(6)

Este artículo en comento tiene relación con el 244 que establece, " El delito de falsificación de documentos se comete por alguno de los medios siguientes:

I.-Poniendo una firma o rúbrica falsa, aunque sea imaginaria, o alterando la verdadera;

II.-Aprovechando indebidamente una firma o rúbrica en blanco ajenas, extendiendo una obligación, liberación o cualquier otro documento que pueda comprometer los bienes, la honra la persona o la reputación de otro, o causar un perjuicio a la

(6) Ibídem, pág. 71.

sociedad, al Estado o a un tercero;

III.-Alterando el contexto de un documento verdadero después de concluido y firmado, si esto cambiare su sentido sobre alguna circunstancia o punto sustancial, ya sea añadiendo, enmendando o borrando, en todo o en parte, una o más palabras o cláusulas, o ya variando la puntuación;

IV.-Variando la fecha o cualquiera otra circunstancia relativa al tiempo de la ejecución del acto que se exprese en el documento;

V.-Atribuyéndose el que extiende el documento o atribuyendo a la persona en cuyo nombre lo hace, un nombre o una investidura, calidad o circunstancia que no tenga y que sea necesaria para la validez del acto;

VI.-Redactando un documento en términos que cambien la convención celebrada, en otra diversa en que varíen la declaración o disposición del otorgante, las obligaciones que se propuso contraer o los derechos que debió adquirir;

VII.-Añadiendo o alterando cláusulas o declaraciones, o asentando como ciertos hechos falsos, o como confesados los que no lo están, si el documento en que se asientan se extendiere para hacerlos constar y como prueba de ellos;

VIII.-Expidiendo un testimonio supuesto de documentos que no existen; dándolo de otro existente que carece de los requisitos legales, suponiendo falsamente que los tiene; o de otro que no carece de ellos, pero agregando o suprimiendo en la copia algo que importe una variación sustancial;

IX.-Alterando un perito traductor o paleógrafo el conteni

do de un documento, al traducirlo o descifrarlo; y

X.- Elaborando placas, gafetes, distintivos, documentos o cualquier otra identificación oficial, sin contar con la autorización de la autoridad correspondiente."

(7)

La autenticidad de los documentos es muy discutida, dado que la exigencia de un escrito ha hecho que tenga que emplearse la computadora en diversas ramas, para su elaboración.

En la actualidad se emiten por computadora multiples títulos de credito, así como instrumentos jurídicos tales como contratos u otras obligaciones, que incluso traen impresa la firma; mismos que tienen un valor probatorio como documentos originales.

Una de las prácticas viciosas es la producción indebida de originales, y no de copias de los documentos en cita, ya que es fácil emitir el número de originales de un documento como sea pertinente, circunstancias que pueden dar oportunidad a que una persona produzca uno o varios documentos de más.

Y que decidir cuando el resultado de una manipulación informática se queda encerrado de alguna manera en la máquina, se puede considerar que la memorización de una información por computadora es una forma de escritura. Igualmente como se le ordena expedir los documentos, se le puede ordenar modificar datos, o bien borrarlos; en consecuencia analizamos que la falsificación de datos memorizados no encuadra en los preceptos en alusión.

Ahora bien las nuevas formas de dinero, especialmente " Dinero de Plástico " y " Tarjetas ya pagadas ", (como tarjetas -

(7) Ibídem, págs. 72-4.

de teléfono), han creado problemas relativos a su autenticidad,- y escapan de una regulación adecuada, ya que tanto ésta acción - como las descritas con antelación requieren una redacción y de-- claración visual de las exposiciones que contienen el documento y por éste motivo, no cubre el almacenamiento electrónico de datos; luego por ser cuestionable la originalidad de dichos docu-- mentos, ya que a pesar de tener la firma impresa, reune todas -- las características de un documento original, razón por la cual no se ajusta a los multicitados artículos. Por lo tanto creemos necesaria la creación de un tipo penal que cubra el almacenamien to electrónico de datos.

IV.f. ROBO

El precepto 367 de la legislación en comento, establece:

" Comete el delito de robo, el que se apodere de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que pueda disponer de ella con arreglo a la ley."(8)

Es cuestionable si el tipo de robo, que requiere el apoderamiento permanente de un bien mueble se adecua, a la acción que resulta de apoderarse de la información, todo porque el apoderamiento exigido por la ley debe ser material. Ya que cuando - las condiciones de idoneidad de acceso así lo permiten una perso na inautorizadamente, puede tener acceso desde un lugar lejano a la unidad central de procesamiento de una computadora ajena, y examinar, modificar y hasta copiar la información allí contenida ya sea por transferencia electrónica u ordenándole a la máquina que la imprima, sin que por esta acción pueda resultar dicho apo

(8) Ibídem, pág. 102.

deramiento de la misma. La sigue dejando donde se encuentra ésta, a pesar de que no existe un desposeimiento, sí se da una -- disminución en el valor de la información, lo cual causa un menoscabo a su propietario.

Ahora bien, el motivo por el que es improcedente a -- juicio nuestro la figura del robo, a dicha nueva acción, es por que si bien es cierto el robo se refiere a bienes muebles.

La información es un bien intangible, puede ser sus-- ceptible de apropiación, pero no es un mueble.

IV.g. ROBO DE FLUIDO

El artículo 368, de la Legislación en referencia, establece:

" Se equiparan al robo y se castigarán como tal:

II. El aprovechamiento de energía eléctrica o de cualquier otro fluido, ejecutando sin derecho y sin consentimiento de la persona que legalmente pueda disponer de él."(9)

Este número resulta inaplicable, por hacer alusión - al aprovechamiento de energía eléctrica o de cualquier otro -- fluido, sin embargo, la información no es energía elécrica, ni tampoco es un fluido.

La persona que se accesa indebidamente, a la unidad - central de procesamiento de una computadora, lo realiza desde su terminal, por lo que utiliza energía a la que probablemente tiene derecho.Por otra parte, se designa como fluido a los " - cuerpos cuyas moléculas tienen poca coherencia y toman siempre la forma del vaso que los contiene." (IO)

(9) Idem.

(IO) Diccionario Pequeño Larousse, pág. 4II, Ediciones Larousse España, I98I.

Del concepto citado se desprende que la información no es un fluido, dado que lo que fluye a través de estos sistemas es energía eléctrica, y a pesar de que la información allí contenida es representada mediante impulsos eléctricos, ésta no es un fluido.

Finalmente cabe señalar que el acceso no autorizado -- a sistemas de procesamiento de datos, es la acción más común - allegarse información, por medio de un teléfono, la cual no implica siempre una privación de ella, sino que algunas veces se desvaloriza dicha información, o a veces causa cierta difusión que va en detrimento de su propietario y otras más el desposeimiento de tal.

IV.h. ROBO DE USO

Establece el artículo 380 de nuestra Legislación Penal " Al que se le imputare el hecho de haber tomado una cosa ajena sin consentimiento del dueño o legítimo poseedor y acredite haberla tomado con carácter temporal y no para apropiársela o venderla, se le aplicarán de uno a seis meses de prisión o de 30 a 90 días multa, siempre que justifique no haberse negado a devolverla, si se le requirió a ello. Además, pagará al ofendido, como reparación del daño, el doble del alquiler, arrendamiento o intereses de la cosa usada. "(II)

Este tipo no es adecuado, a la conducta que resulta, - de accesarse a una computadora ajena, ya que lo que toma no es, un bien, sino un servicio que es realizado por una máquina.

El robo consiste en servicios de procesamiento de da--

(II) Código Penal para el D.F., ob. cit., pág. 104.

tos, ésto es en utilizar funciones propias de una computadora y ésto ocurre, generalmente cuando empleados utilizan sin autorización la máquina para realizar trabajos particulares (-- que es propiedad del empleador).

El acceso no autorizado a una computadora puede ocasionar las siguientes acciones, que sería necesario crear un nuevo tipo penal acorde a ellas.

- Enterarse de la información; y
- Realizar servicios de procesamiento.

IV.i. ABUSO DE CONFIANZA

Establece el ordenamiento legal en cita en el artículo 382.-

" Al que, con perjuicio de alguien, disponga para sí o para otro, de cualquier cosa ajena mueble, de la que se le haya -- trasmitido la tenencia y no el dominio, se le sancionará con prisión hasta de un año y multa de 100 veces el salario, cuando el monto del abuso no exceda de 200 veces el salario.

Si excede de esa cantidad pero no de dos mil, la -- prisión será de uno a seis años y multas de 100 hasta 180 veces el salario.

Si el monto es mayor de 2,000 veces el salario la - prisión será de seis a doce años y la multa de 120 veces el - salario."(12)

Al igual que el tipo del robo, el abuso de confianza recae sobre sobre un bien mueble, toda vez que en una ac--

(12) Ibídem, pág. 106.

ción de transferir información de un patrimonio, a otro, no es procedente aplicar el segundo tipo, es decir, el abuso de confianza; así mismo exige éste la disposición de la cosa mueble; misma que no es factible en la transmisión de la información,- en primero por que dicha información es intangible y no es una cosa mueble; en segundo porque su transmisión no entraña una - disposición, razón por la que sería necesario incluir en un -- capítulo especial de delitos informáticos en la Legislación Penal, contemplando un dispositivo acorde con ésta acción que se encuentra impune.

IV.j. FRAUDE

El multicitado ordenamiento legal, establece en el - artículo 336.-

" Comete el delito de fraude el que engañando a uno o aprove-- chandose del error en que éste se halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido. "(I3)

Este precepto no es aplicable a la acción que resulta, cuando una persona indebidamente se accesa a la unidad central de procesamiento de una computadora ajena, que lo hace -- sin consentimiento de su propietario, por lo tanto no lo engaña, ni lo induce al error como lo exige la figura del fraude - simplemente el sujeto activo se accesa, examina, transfiere, - extrae, destruye, etc. la información que ésta contiene y sale cuidadosamente.

El elemento engaño, es cuestionable, porque habría - que preguntarse en el derecho, ¿ Quienes poseen voluntariedad ante la ley penal y por lo tanto ser responsables ?, consecuentemente ser susceptible no sólo de engaño, sino de cometer al-

(I3) Ibídem, pág. I07.

gún error.

IV.B. PRINCIPIO DE LA LEGALIDAD DE LAS PENAS

En nuestra Carta Magna, se encuentra plasmado en el artículo I4, parráfo 3º, un principio que han recogido todos los pueblos liberales y que repudian los regímenes totalitarios. En efecto, en las dictaduras el principio de la legalidad de los delitos y las penas es el primero que se deja de respetar; en cambio se crean leyes sin juicio previo o se hace un mero simulacro de éste, que a la letra dice:

" En los juicios del orden criminal queda prohibido imponer, por simple analogía y aun por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata."(I4)

Lo cual se traduce que en estos juicios, sólo podrá imponerse una pena si el acto o el hecho que se juzga está claramente previsto por la ley, o sea, si es exactamente igual a la conducta que la ley describe, en cuyo caso la pena con que se castigue al infractor debe ser la que fija la propia ley. En consecuencia, está prohibido en estos juicios aplicar una ley que contenga un caso parecido, similar o más grave, pero que no sea idéntico al que se trata de juzgar. Es decir, está prohibido aplicar la ley penal por analogía o mayoría de razón.

Tratándose de las vulneraciones que han surgido en la periferia de la informática, algunas veces les han aplicado análogamente o por mayoria de razón algunos tipos penales, constituyendo esto una violación flagrante a la Constitución Política.

(I4) Constitución Política de los Estados Unidos Mexicanos, pág.- I3, I03a. edición, Edit. Porrúa, S.A., México, I994.

IV.C. EXTENSION DE LA GARANTIA

El postulado abordado en el anterior inciso implica dos principios; los delitos y las penas con una aplicación en materia adjetiva (penal), en el primer supuesto desdoblando lo establecido por el aludido párrafo se infiere jurídicamente, la existencia de un hecho humano que de acuerdo con el artículo 7 de la legislación penal " Delito es el acto u omisión que sancionan las leyes penales," en consecuencia para que hecho configure un delito, es necesario que exista un precepto legal que instituya una pena a su perpetrador, por ende la ausencia de áquel no constituye un delito. (I5)

Por lo tanto para que un hecho, sea reputado como delito y penalizado acorde con el principio de la legalidad de los delitos y las penas, es menester que una ley considere a quél como tal, es decir, que exista un precepto legal que le confiera una penalidad. De acuerdo con el segundo supuesto, esto es, las penas sostiene el Dr. Ignacio Burgoa Orihuela,"está prohibida la aplicación de una sanción penal si no existe alguna disposición legal que expresamente la imponga por la comisión de un hecho determinado. En otras palabras, para todo delito la ley debe exprofesamente señalar la penalidad correspondiente," por ende se transgredera el principio en comento. (I6)

IV.D. INTERPRETACION ANALOGICA Y POR MAYORIA DE RAZON

(I5) Código Penal para el D.F., ob. cit., pág. 2.

(I6) Ignacio Burgoa, Las Garantias Individuales, pág. 569, 22a. ed., Edit. Porrúa, S.A., México, 1986.

El aludido principio constitucional, prohíbe imponer penas por analogía y por mayoría de razón, en el primer caso señala el Dr. Ignacio Burgoa Orihuela, " es la circunstancia de que ésta se hace extensiva a aquellos casos concretos que no están en ella previstos, pero que presentan con las hipótesis expresamente reguladas cierta similitud." (I7) Distinguiendo una semejanza relativa en relación a ciertos aspectos o elementos comunes (causa, efectos, formalidades, capacidad de los sujetos, etc.). En otras palabras, la imposición por analogía de una pena señala el Dr. en comento, " implica la aplicación, también por analogía, de una ley que contenga una determinada sanción penal, a un hecho que no está expresamente castigado por ésta y que ofrece semejanza substancial, pero discrepancia en cuanto a los accidentes naturales, con el delito legalmente penado." (I8)

En cuanto a la mayoría de razón se basa en elementos extrínsecos, los cuales en mayores cantidades en un caso concreto, completan el supuesto normativo. El multicitado Dr.en"conclusión, al prohibir el artículo I4 constitucional en su tercer párrafo la imposición por mayoría de razón, impide que la ley que contenga - la sanción penal se haga extensiva a hechos que, aunque de mayor gravedad, peligrosidad o antisocialidad, etc, que el delito previsto, no estén comprendidos en ella y sean esencialmente diferentes de su antecedente abstracto, asegurándose mediante tal prohibición la efectividad del principio nulla poena sine lege." (I9)

(I7) ob. cit., pág. 570.

(I8) Ibídem, pág. 57I.

(I9) Ibídem, pág. 573.

LEGISLACION COMPARADA DE LOS ILICITOS INFORMATICOS

V.A. ALEMANIA

La legislación penal Alemana, contempla en su artículo 263 la estafa informática en los siguientes términos:

"(I)Quiconque dans l'intention de se procurer ou de procurer á un tiers un avantage pécuniaire illicite, aura porté préjudice au patrimoine d'autrui, en influencant le résultat d'un processus informatique par une fausse formation du programme ou une manipulation du déroulement du programme ou par utilisation de données fausses ou incomplétes ou un emploi illégal de données sera puni d'une peine d'emprisonnement de cinq ans ou d'une amende.

(2)L'article 263, alinéas 2 á 5 est applicable par analogie."

" Cualquiera que tenga la intención de obtener o procurarse para un tercero o para sí mismo una ventaja pecuniaria ilícita, haya perjudicado el patrimonio de otro, influyendo el resultado de un proceso informático por una formación del falso programa o por una utilización de datos falsos o incompletos, o por un empleo ilegal de datos, será castigado con una pena de prision de 5 años o una multa."(I)

El artículo 270 prevé, el fraude en una transacción jurídica, en el ámbito informático:

"Le manipulation dans le traitement des données concernant une transaction juririque est assimilés á une fraude dans une tran

(I) Traducción de Nadine Terrein R., de la Compilación de Legislación Comparada de actos ilícitos informáticos de Alemania E.U.A., Didamarca y Canadá, sin autor y sin fecha de publicación.

saction juridique."

" La manipulación en el proceso de datos relativos o referentes a una transacción jurídica es equiparable a un fraude en una -- transacción jurídica."(2)

El artículo 271, hace alusión a la falsificación indirecta de documentos:

"(I)Sera puni d'un emprisonnement d'un an au plus ou d'une amende, celui qui, volontairement, aura fait constater dans des actes, livres, fichiers ou registres publics que des déclarations, négociations, faits juridiquement importans ou des rapports juridiques

ont eu lieu, alors que ces déclarations, négociations ou faits n'ont pas eu lieu, qu'ils ont eu d'une facon autree ou qu'ils - ont eu lieu d'une facon autre ou qu'ils émanent d'une personne ayant agi dans une qualité qui ne lui revenait pas ou une autre personne.

(2)La tentativa est punissable."

(I) " Será castigado con prisión de un año o con una multa, el que, voluntariamente, haya utilizado actas, libros, ficheros o registros públicos para comprobar declaraciones, hechos jurídicamente importantes o reportes públicos que en realidad no existieron o tuvieron lugar de manera diferente a la expresada que éstos hechos fueron realizados por una persona que sin personalidad jurídica los hubiera realizado.

(2) Este delito puede ser punible en grado de tentativa." (3)

(2) y (3) Traducción de Nadine Terrein R., de la Compilación de Legislación Comparada de actos ilícitos informáticos de Alemania, E.U.A., Dinamarca y Canadá, sin autor y sin fecha de publicación.

La utilización de documentos falsos es abordada por el artículo 273 que establece lo siguiente:

"Celui qui, dans le but de tromper, fait usage de documents faux ou de données mémorisées falsifiées de la nature de ceux visés á l'article 271, est puni des peines prévues audit article et s'il agit dans l'intention de procurer á lui-meme ou á un autre un avantage pécuniare, ou de causer préjudice á un tiers des peines prévues á l' article 272."

" El que, con el objeto de engañar, utilice documentos falsos o datos memorizados falsificados de la naturaleza de los que trata el artículo 271, tendrá la misma penalidad que el artículo citado, y si los utiliza con la misma intención de procurarse así mismo una ventaja pecuniaria, o causar un perjuicio a tercero, tendrá la misma penalidad que el artículo 272." (4)

En el artículo 274 se encuentra prevista la supresión de documentos, en la modificación de un señalamiento de límites, en los términos señalados ulteriormente:

"(I)Celui qui

I. dans l'intention de porter préjudice á autrui, détruit, endommage ou supprime un document ou une notice technique qui ne lui appartient absolument pas ou pas exclusivement,

2. dans l'intention de porter préjudice á autri, efface cu supprime des données mémorisées au sens de l' article 269 don il ne doit absolument past ou pas exclusivement disposer,

(4) Traducción de Nadine Terrein R., de la Compilación de Legislación Comparada de actos ilícitos informáticos de Alemania, E.U.A., Dinamarca y Canadá, sin autor y sin fecha de publicación.

3. dans l'intention de porter préjudice á autrui, enléve, détruit, rend méconnaissable, déplace ou place dans un endroit oú -- elle ne doit pas étre une borne ou une autre marque desinée á -- signaler une limite ou un niveau d'eau, est puni d'une peine privatice de liberté de cinq ans au plus ou d'une amende.

(2) la tentative est punissable."

"(I) El que

I.- con la intención de causar un daño a otro, destruya, o deteriore un documento o una nota técnica que no le pertenece o no - le pertenece exclusivamente,

2.- con la intención de causar un daño a otro, borre o suprima - datos memorizados en el sentido del artículo 269, a los que no - tenga acceso, o no tenga exclusivamente.

(2) Este delito es punible en grado de tentativa.

3.- con la intención de causar un daño a otro, quite, destruya,- haga irreconocible, desplaze o ponga en otro un señalamiento u - otra marca destinada a señalar el límite o nivel del agua, se le impondrá de 3 días hasta 5 años de prisión más una multa." (5)

Las certificaciones falsas en el ejercicio de las funciones públicas, se encuentran contempladas en el artículo 348, el cual prevé lo siguiente:

"(I) Tout titulaire d'une fonction publique habilité á dresser - des actes publics qui, dans le cadre de sa compétence, certifie faussement ou inscrit faussement sur des registres, livres ou fichiers publics, un fait juridiquement important, est puni d'une

(5) Traducción de Nadine Terrein R., de la Compilación de Legislación Comparada de actos ilícitos informáticos de Alemania, E.- U.A., Dinamarca y Canadá, sin autor y sin fecha de publicación.

peine d'emprisonnement de cinq ans au plus ou d'une amende.
(2) La tentative est punissable."

" Al titular de una función pública facultado para realizar actos públicos y que, dentro del marco de su competencia realice, falsamente certificación o inscripción en los registros, libros y ficheros públicos, de un hecho jurídicamente importante, será punible con una pena privativa de libertad hasta de cinco años o una multa.
(2) Es punible es grado de tentativa."(6)

V.B. DINAMARCA

la legislación de Dinamarca, prevé los delitos informáticos señalados ulteriormente:

El sabotaje informático, establecido por el precepto - I93 del Código Penal, de la legislación en cita que a la letra dice:

" Celui qui contre la loi entrave le bon fonctionnement des moens de communication, du courrier public, des installations télégraphiques, radio ou télévisions ainsi que des ordinateurs ou installations communes pour la distribution de l'eau, gaz, électricité ou chauffage, sera pénalisé soit d'une peine de simple police, soit d'emprisonnement pouvant aller jusqu'á 4 ans ou avec circonstances atténuantes, á une amende."

" El que en contra de la ley obstaculice el buen funcionamiento de los medios de comunicación, de correo público, de las instalaciones telegráficas, radio, televisión o de instalaciones de

(6) Traducción de Nadine Terrein R., de la Compilación de Legislación Comparada de actos ilícitos informáticos de Alemania, E. U.A., Dinamarca y Canadá, sin autor y sin fecha de publicación.

uso comun para la distribución de agua, gas, electricidad y calefacción, será sancionado desde una pena de simple policía o una pena privativa de libertad hasta de 4 años si existen circunstancias atenuantes, en caso de no existir se le sancionará con una multa."(7)

El acceso inautorizado, es regulado por el artículo 264 en los términos siguientes:

"I) Celui qui illégalmente accés:

I- á une maison ou autre lieu interdit ou

2- qui refuse de quitter un lieu aprés injonction

est pénalisé d'une amende, peine de simple police ou d'emprisonnement allant jusqu'á 6 mois.

2) Si quelqu'un délibérément fait ce qui est mentionné á l'article 264. no. I.I. pour avoir accés aux informations d'une entreprise ou autres conditions spécialement aggravantes peut etre pénalité peut atteindre jusq'á 2 ans d'emprisonnement."

"I) El que ilegalmente tenga acceso:

I.- a una casa o a un lugar prohibido o

2.- que se niegue salir de un lugar después de orden terminante o formal

Será penalizado de una multa, pena de simple policía o de prisión hasta 6 meses.

2) Si alguien deliberadamente hace lo mencionado en el artículo 264 núm. I.I. para tener acceso a la información de una empresa u otras condiciones especialmente agravantes la penalidad puede alcanzar hasta 2 años de prisión."(8)

(7) y (8) Traducción de Nadine Terrein R., de la Compilación de Legislación Comparada de actos ilícitos informáticos de Alemania E.U.A., Dinamarca y Canadá, sin autor y sin fecha de publicación.

El fraude informático se encuentra previsto, en el artículo 279 a:

" Celui qui fait de l'escroquerie informatique pour se procurer du profit, qui change, ajoute ou efface des informations ou programmes informatiques ou cherche á manipuler le résultat d'un - tel traitement de l'information est passible de peine."

" El que haga un fraude informático para procurarse un beneficio que cambie, añade o borre informaciones o trate de manipular el resultado de un proceso de datos, es sujeto a una pena."(9)

El abuso de confianza está contemplado en el artículo - 280, el cual dispone lo siguiente:

" Dans le cas oú il ne s'agit pas d'escroquerie informatique, la personne sera penalisée conformément au paragraphe qui concerne l'abuso de confiance."

" En el caso de que se trate de fraude informático, la persona - será sancionada conforme al párrafo que se refiere al abuso de - confianza."(IO)

El encubrimiento de objetos robados, de programas informáticos, se encuentra consignado en el precepto 284:

" En ce qui concerne le "recel de programmes informatiques" la - pénalité est la meme que celle prévue au paragraphe du recel d' objets volés."

" Lo que se refiere al "encubrimiento de programas informáticos" la penalidad es la misma que la prevista por el párrafo de encubrimiento de objetos robados."(II)

(9),(IO) y (II) Traducción de Nadine Terrein R., de la Compilación de Legislación Comparada de actos ilícitos informáticos de Alemania, E.U.A., Dinamarca y Canadá, sin autor y sin fecha de - publicación.

V.C. CANADA

Este país ha adoptado en su Código Criminal, infracciones relativas a las computadoras; divididas en dos vertientes:
I.- La relacionada al uso no autorizado de un sistema informático, y
2.- La relacionada a la modificación o destrucción no autorizada de datos informatizados.

El artículo 30I.2 del texto en referencia hace alusión, al beneficio, que una persona se procure directa o indirectamente, ya sea obteniendo cualquier servicio computarizado, o bien - interceptando por algun dispositivo toda función de un sistema - de cómputo. El perpetrador de éste ilícito, es culpable de un acto criminal y sujeto a una pena de privación de libertad que no excederá de I0 años o es culpable de una infracción castigable - sobre declaración sumaria de culpabilidad.

El artículo 387, trata de proteger la esencia de los datos informatizados, haciendo acreedora a una pena no mayor de I0 años de prisión a la persona que:

(a) Destruya o altere los datos;

(b) Transforme los datos haciéndolos incomprensibles, inútiles o ineficaces;

(c) Obstruya, interrumpa o interfiera con el uso legítimo de los datos, u

(d) Obstruya, interrumpa o interfiera con cualquier persona - en el legítimo uso de los datos o niegue el acceso a éstos a toda persona que esté autorizada para ello.

V.D. FRANCIA

En Francia, vemos que existen soluciones legislativas, a problemas jurídicos originados por la informática tales como:

(a) La Ley del 6 de enero de I978 sobre la informática, los ficheros y las libertades;

(b) La Ley del 4 de enero de I980 relativa a la automatización del archivo judicial;

(c) La Ley del I2 de enero de I980 sobre la prueba de los actos jurídicos;

(d) Artículo 97 de la Ley de Finanzas para I982 y su decreto de aplicación del 29 de diciembre del mismo año, sobre la verificación fiscal de las contabilidades informatizadas de las empresas;

(e) El Plan Contable revisado en I979, aprobado por la Ley del 27 de abril de I982;

(f) La Ley del 30 de abril de I983 relativa a las obligaciones contables de los comerciantes y de las sociedades;

(g) Decretos del I7 de enero de I984, sobre la telemática interactiva, y

(h) Ley que reforma los derechos de autor, que incluye los logiciales en las obras que benefician la protección de la propiedad literaria y artística.

La enumeración de estos textos legislativos, prevén incriminaciones específicas.

Por otra parte el Código Penal Frances, sólo contempla en la mayor parte, incriminaciones tradicionales.

La Ley del 6 de enero de I978, es una ley especial que contiene ante todo disposiciones substanciales y, accesoriamen-

te, reglas sancionadoras al primer jefe de las cuales figuran incriminaciones penales. La reglamentación en sí, comprende tres - capítulos:

El primero referente, a la creación de tratamientos automatizados de informaciones nominativas; el segundo regula la - colecta, el registro y la conservación de dichas informaciones, y el tercero hace alusión a un derecho de rectificación.

La Ley del 4 de enero de I980, consigna algunos atentatados a las personas por medio de la informática, y es ésta ley relativa a la automatización del expediente judicial, presenta - una importancia muy particular. No agota sin embargo, tanto que sea, todas la hipótesis de atentados a las personas que puedan - ser cometidos por medio de la informática.

El artículo 97 de la Ley de Finanzas para I982 y su decreto, el Plan Contable para I979, aprobado por la Ley del 27 de abril de I982; así como la Ley del 30 de abril de I983, establecen los procedimientos modernos de tratamiento de los datos contables.

La violación de las reglas del derecho contable no da - lugar directamente a una sanción penal, pero se encontrará sancionada indirectamente bajo la calificación eventual de bancarrota la presentación del estado de cuentas inexacto o de fraude fiscal.

Los Decretos del I7 de enero de I984, prevén todo lo -- concerniente a la comunicación audiovisual.

La Ley que reforma, a la del I3 de julio de I978, relativa a los derechos de autor, el proyecto de reforma fue discuti

do enfrente del Parlamento tiene, sobre recomendación del Senado elevado el logicial a la dignidad de una obra del espíritu, de - manera que el problema esté resuelto.

Por lo que respecta a las incriminaciones tradicionales que prevé la legislación penal francesa, relativa a actos ilícitos informáticos son señalados ulteriormente:

Raymond Gassin cita el caso " Muntean (Crim. 23 mars -- I982, Bull. crim., nº 85, p. 230) d'oú il résulte que le piratage informatique peut constituer le crime d'entretien d'intelligence avec les agents d'une puissance étrangére (art. 80-3º c. - pén.)."

" Muntean (Crim. 23 de marzo de I982, Bull. crim., No. 85, p. -- 230) de donde resulta que la piratería de la informática puede - constituir el crimen de mantenimiento de inteligencia con agentes de una potencia extranjera (art. 80-3º c. pen.)." (I2)

En segundo lugar se agrupan aquellos contra los bienes, entre éllos el fraude informático, estafa a la informática y abuso de confianza; el primero de éstos consiste en apropiarse de - bienes o de fondos por medio de manipulaciones irregulares de la computadora. Las manipulaciones pueden situarse en tres fases de entrada, de tratamiento y de salida de la computadora. La estafa ésta regulada por el artículo 405 del Código en cita, y puede - perpetrarse usando un código y una palabra de paso, después de - haber pasado el secreto, puede ser considerado como la toma de -

(I2) Raymond Gassin, Derecho Penal de la Informática: Relación - presentada al Congreso de la Asociación Europea de los Magistrados, pág. 36, Grenoble, I985.

un falso nombre o de una falsa cualidad en todo caso de manio-- bras fraudulentas, si por otro lado el hecho de usar un servi-- cio de la computadora puede ser considerado como una remesa en sentido del artículo en alusión, por analogía con la estafa a - la taxifonía. Para no citar más de un ejemplo, se mencionará -- una técnica muy conocida de los banqueros desde 1973; la letra de cambio-relevada, por lo menos bajo la forma extrema del LCR- magnético. Es precisamente la destrucción de éstas informacio-- nes con valor probatorio puede caer bajo el artículo 439 del or denamiento legal en referencia; sin embargo algunos autores han sostenido la afirmativa en racionamiento por analogía con la so lución jurisprudencial retenida en materia de estafa al parquí- metro o al taxífono.

El abuso de confianza, hasta ahora se ha aplicado por analogía al hecho que resulte de apropiarse ilícitamente no de la computadora en sí, pero de su uso. Y se puede perpetrar con- siderablemente con la telemática.

También entra dentro de ésta categoría el robo, que es de dudosa aplicación, y aun cuando algunas veces la aprehensión del soporte material no tenga lugar más que el tiempo necesario para hacer una copia. La Cámara criminal en el célebre paro Lo- gabax del 8 de enero de 1979, tratado a propósito del empleado de una empresa con fines personales, que el delito de robo esta ba constituido en la especie, ya que el empleado había actuado fraudulosamente los documentos durante el tiempo necesario para su reproducción.

El sabotaje informático éste delito está reprendido --

por los textos 434 I párrafo y 439 I párrafo, que a la letra señalan respectivamente; el primero:

" quiconque aura, volontairement, detruit ou deteriore un objet - mobilier ou un immobilier appartenant á autrui, saul s'il s'agit de détériorations légéres..."

" Quienquiera que hubiera voluntariamente destruido o deteriorado un objeto mobiliario o un bien inmueble perteneciente a una tercera persona, salvo si se trata de destrozos ligeros...", castiga - (I3)
con penas correccionales (tres meses a dos años de prisión y 2500 a 5000 francos, de una multa o de una de las dos penas solamente, y el segundo:

" quiconque aura volontairement brule ou détrit, d'une maniére -- quecolque, des registres, minutes ou actes originaux de l'autorité publique, des titres, billets, lettres de change, effets de commerce ou de banque, contenant ou opérant obligation, disposition ou décharge."

" quienquiera que habrá voluntariamente quemado o destruido, de una manera cualquiera, los registros, minutas o actas originales - de la autoridad pública, títulos, billetes, letras de cambio, e-- fectos de comercio o de banco, que contengan u operando obligaciones, disposición o descargo."(I4)

Algunos "atentados tecnológicos", no levantan dificulta- (I5)

(I3) ob. cit., pág. 37.

(I4) Idem.

(I5) Nota aclaratoria: Es la obra en Francia de una organización que se bautizó CLODO (Comité liquidador de las computadoras).

des jurídicas particulares en el estado actual de la legislación ya que encuadran en los artículos 435 al 437, siendo el más co-- mún el primero de los citados, que al efecto castiga con penas - correccionales reforzadas (cinco a diez años de prisión y 5000 a 200,000 francos de multa) a:

" quiconque aura volontairement détruit ou détérioré un objet mo bilier ou un bien immobilier appartenant á autrui, par l'effet - d'une substance explosive ou incendiaire, ou d'un incendie ou de tout autre moyen de nature á crér un danger pour la sécurité des personnes."

" quienquiera que hubiera voluntariamente destruido o estropeado un objeto mobiliario o un bien inmueble que pertenezca a una ter cera persona, por el medio de una substancia explosiva o incen-- diaria, o de un incendio o de cualquier otro medio de naturaleza para crear un peligro para la seguridad de las personas."(I6)

Por otra parte el delito de falsificación se encuentra previsto en los artículos 425 y 426 de la legislación en comen-- to, que también se encuentra estrechamente unido a la informáti- ca.

(I6) Idem.

Para salvar algunos vacíos normativos, se han dictado - normas penales especialmente referidas a los fraudes informáti-- cos en Suecia (es condenable la persona que ilegalmente obtiene acceso a registros de datos sujetos a procesamiento o altera, -- destruye o ingresa esos datos en un archivo); numerosos Estados de los Estados Unidos, Gran Bretaña, Australia (penan cualquier persona que ilegalmente altere, falsifique, borre o destruya cualquier material de procesamiento de datos con una intención --- fraudulenta); Canadá, Alemania (no requieren la presencia de una persona engañada para tipificar el delito fraude); y Dinamarca.

El sabotaje informático, está previsto en algunas le-- gislaciones, ejemplo; Suiza y Portugal, que procuran paralizar - el daño cometido aun cuando sólo abarque bienes intangibles.

Robo de servicios, por ejemplo, el Código Criminal de Virginia, considera propiedad el tiempo de un computador o de -- servicios de procesamiento de datos, y por tanto, incrimina su uso no autorizado. La Ley sueca de 1983 castiga el mero acceso a un procesamiento de datos. En los Estados Unidos la " Counterfeit Acces Device and Computer fraud and Abuse " tipifica penalmente el acceso no auutorizado a sistemas informáticos operados por el gobierno, y en particular a los asociados a la defensa nacional, las relaciones externas y la energía atómica, así como a -- los de instituciones financieras.

Carlos Correa citando por su parte, un proyecto de ley de Informática del Ministerio de justicia de Chile (abril de 1986) la cual prevé que " cometerá delito informático la persona -

que maliciosamente use o entre a una base de datos, sistema de - computadores o red de computadoras o a cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. También comete este tipo el que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, refiere, recibe, usa, altera, daña o destruye una computadora, un sistema o - red de computadoras, un soporte lógico o programa de la computadora o los datos contenidos en la misma, en la base, sistema o - red."(I7)

En algunos países, las precauciones en falsificaciones requieren una redacción y declaración visual de las exposiciones que contiene el documento y por ésta razón, no cubre el almacenamiento electrónico de datos. Ejemplo: Grecia, Japón, Inglaterra y Noruega, establecen o proponen nuevos estatutos de falsificación hacen a un lado la percepción visual.

Algunas restricciones específicas por medio del uso de la computadora son propuestas en algunos países, verbigracia: Homicidio cometido por la manipulación del sistema de supervición computarizado dentro de un hospital, las precauciones legales son formuladas en términos de completa relevancia si los resultados son archivados dentro de una computadora o no.

En el campo de la manipulación financiera es diferente la definición impuesta por la Ley del robo y hurto en muchos sistemas legales, como Grecia, Luxemburgo y Japón requieren que la

(I7) Carlos M. Correa, Derecho Informático, pág. 298-9, Edit. - Depalma, Buenos Aires, I987.

persona que comete el ilícito tome una pertenencia de la otra -- persona. No hay aplicación si el perpetrador se adueña de dinero depositado; en muchos países éstas precauciones también causan - dificultades como la manipulación de los "cajeros automáticos."

Países como Grecia e Italia, se sienten rechazados a las aplicaciones de las precauciones tradicionales en hurto o robo de la inautorizada abstracción de la información que éstas leyes requieren generalmente esa propiedad corporea, que ha sido - tomada con la intención de impedir que la víctima la posea.

En los países bajos, la aplicación tradicional de precauciones de robo o hurto, son posibles en ciertos casos.

En E.U.A., por ejemplo, algunas Cortes toman los datos de computadora como propiedad en el sentido de latrocinios - tradicionales y en muchos Estados, las legislaturas los han definido "como propiedad o le dan el valor de cosa", para facilitar la aplicación de los robos de prevención o nuevas precauciones - generales en el crimen por computadora.

La legislación canadiense como israelita, siguieron - una aproximación de propiedad, como resultado de los problemas,- que aplican la Ley de Propiedad General, para cubrir los secretos.

Ciertos países (como Suiza y Finlandia), tienen la intención de reformar los estatutos tradicionales:
Vandalismo o daño a la propiedad tangible; también otros países crean precauciones específicas para la información. Pocos países especialmente Japón, cubren todo tipo de documentos y no solamente datos ya almacenados en la computadora.

En varias leyes de E.U.A., hay más sanciones determinadas para la inserción o entremetimiento de un virus en las computadoras.

Acceso ilegal de los datos archivados (procesamiento de datos y sistema de almacenamiento), en lo concerniente a la intercepción de datos y a la comunicación clandestina donde los sistemas legales se refieren únicamente (comunicación oral), como fue bautizada en Israel, Italia, los países bajos, Suiza y en los Estados Unidos, no pudiendo aplicarse similarmente a la falsificación.

Las nuevas propuestas legislativas, concernientes al acceso inautorizado, cubren la conexión teléfonica clandestina, así como al procesador de datos y sistema de comunicación tanto, han sido establecidas en Canadá, Alemania, Francia, Noruega, Suecia, E.U.A. y el Reino Unido y han sido propuestas por la Comisión de Reforma en Inglaterra, Israel, los países bajos, Escocia y Suiza. Unicamente los antes mencionados (junto con Japón y Austria), los crímenes por computadora no tuvieron precauciones contra el acceso ilegal al Sistema-DP.

CONCLUSIONES

I.- Con los avances de la tecnología computacional, ha sido menester la creación de almacenamientos de datos en diversos sectores, dado que han proliferado fácilmente sus aplicaciones en éstos, vemos que el crecimiento de dicha tecnología, aunado a algunos intereses, inducen a demandas legales de leyes de información, que -- hasta ahora esta esfera se encuentra desprovista de una normatividad acorde.

2.- Debido a la aplicación de los sistemas electrónicos de información y el flujo de datos, han permitido transferir por cable información a algunos usuarios, otras veces exploradores de sistemas han podido identificar algún código confidencial de información a la cual no cuentan con autorización, con la idea de convertir datos a dinero y viceversa, otras con fines de reproducción - de algún soporte para la informática, alterar los datos memorizados, desviarlos, sustraerlos, etc. Todas éstas vulneraciones demandan respuestas legales de leyes de información.

3.- En vista de éstas necesidades legislativas, planteo reformar el Código Penal, congruente con la Política Criminal despenalizando las conductas inoperantes, y considerar la necesidad de criminalizar nuevas formas de conductas delictivas que han surgido en la periferia de la informática, y que en algunos casos se encuentran impunes.

4.- Que la legislación penal, incluya en el libro segundo, Título Vigesimoquinto, un nuevo capitulado de derecho penal informático, relativo a todas las conductas que han aparecido por el uso indebido de la informática, separando de los tipos penales tradicionales, que sólo equiparan dichas conductas o aplican flagrantemente a éstas acciones, por lo tanto propongo los siguientes delitos informáticos, cuyo bien jurídico tutelado es la información, para - quedar como sigue: Capítulo I

Espionaje Informático

ART. 4II.- Comete el delito de espionaje informático, el que va--

liendose de accesarse a una Unidad Central de Procesamiento de alguna computadora ajena, altere, desvie, capte, copie o use un soporte físico y/o soporte lógico para la informática, para cualquier fin, inautorizadamente, realizado por algún medio de ésta, se le impondrá pena de prisión de 3 a 8 años. Debiendose entender por espionaje informático, toda pirateria que cause una persona sin contar autorización, en los soportes mencionados en este precepto.

Capítulo II

Terrorismo Informático

ART. 412.- Comete el delito de terrorismo informático, la persona que:

Por cualquier medio violento, deteriore o se apodere de algún centro neurálgico computarizado, se le impondrá pena de prisión de 4 a 10 años. Debiendose entender por terrorismo informático, causar una persona, la destrucción violenta de algún sistema computarizado o apoderamiento del mismo.

Capítulo III

Sabotaje Informático

ART. 413.- Comete el delito de sabotaje informático, la persona que:

I.- Provoque trastornos al buen funcionamiento de los medios de comunicación públicos como privados, por algún medio programado, creando también un peligro para las personas;

II.- Introduzca instrucciones no autorizadas dentro de un programa de computación ajeno, mediante los cuales se cause un daño al mismo programa, a otros o a los sistemas de cómputo, o

III.- Introduzca instrucciones no autorizadas dentro de un programa de computación propio y lo utilice para causar daño a otros programas o sistemas de cómputo, se le impondrá una pena de 3 a 8 años de prisión. Debiendose entender por sabotaje informático, los trastornos ocasionados por una persona, a un sistema computarizado, por algún medio programado.

Capítulo IV

ART. 4I4.- Comete el delito de ultraje informático, la persona que: Distorcionando, algún medio de la informática, haga alguna propuesta indecorosa, a otra, se le impondrá pena de 6 meses a 2 años de prisión y de veinte a cincuenta días multa. Debiendose entender - por ultraje informático, como la propuesta indecorosa, realizada - por la vía de la informática; por una persona, a otra.

Capítulo V

Falsificación de Datos Electrónicos

ART. 4I5.- Comete el delito de falsificación de datos electrónicos la persona que accesandose a una Unidad Central de Procesamiento - de alguna computadora ajena:

I.- Modifique ilegalmente datos electrónicos, magnéticos u otros - memorizados no visibles o no legibles directamente, inautorizada-- mente, o bien

II.- Proceda a tal falsificación inautorizada de datos memorisados licita o ilícitamente.

Se le impondrá pena de 3 a 7 años de prisión y de doscientos a cuatrocientos días multa. Debiendose entender por falsificación de datos electrónicos, la alteración de cualquier dato electromagnético, memorizado en algún sistema de cómputo, sin autorización,- que realize una persona, por algún medio de la infórmática.

Capítulo VI

Difamación Informática

ART. 4I6.- Comete el delito de difamación informática, la persona que accesandose a una red informativa ajena, por medio de un dispositivo electromagnético:

Varie un soporte de lo escrito; de una palabra, o de una ima-- gen.

Se le impondrá pena de 3 a 6 años de prisión y de doscientos - cincuenta a cuatrocientos días multa. Debiendose entender por difamación informática, toda alteración de la realidad en un escrito,- en una palabra o en una imagen, que realice alguna persona, por medio de algún dispositivo electromagnético.

Capítulo VII
Robo Informático

ART. 417.- Comete el delito de robo informático, la persona que - accesandose por cualquier medio a la Unidad Central de Procesa--- miento de cualquier computadora, inautorizadamente:

Extraiga,interfiera o transfiera todo tipo de información.

Se le impondrá pena de 4 a 7 años de prisión y hasta trescientos días multa. Debiendose entender por robo informático, toda -- sustracción, interferencia o transferencia de información, de la unidad señalada en este precepto, realizada por una persona por - cualquier medio.

Capítulo VIII
Abuso de Servicios Computacionales

ART. 418.- Comete el delito de abuso de servicios computacionales la persona que accesandose a una Unidad Central de Procesamiento de alguna computadora ajena:

I.- Obtenga cualquier servicio computarizado o utilice las funciones de la computadora señalada en este precepto, para otros fines diferentes a los que está autorizada,

II.- Utilice las funciones de la computadora ajena sin autorización de la persona que legalmente pueda disponer de ella, independientemente del delito que resulte por el acceso a tal sistema -- computacional.

Se le impondrá pena de 3 a 6 años de prisión y hasta doscientos días multa. Dediendose entender por abuso de servicios computacionales, la obtención, utilización de las funciones de una computadora ajena, por alguna persona que sin derecho e inautorizadamente, dispone de tales.

Capítulo IX
Fraude Informático

ART. 419.- Comete el delito de fraude informático, la persona que

accesandose a la Unidad Central de Procesamiento de alguna computadora ajena:

Con el ánimo de procurarse un beneficio, ya sea que cambie, añada o borre informaciones o trate de manipular el resultado de un proceso de datos.

Se le impondrá pena de 5 a IO años de prisión y de quinientos a setecientos días multa, dependiendo del monto de dicho fraude.- Debiendose entender por fraude informático, toda manipulación que realice una persona, a un sistema computacional; con el ánimo de obtener un beneficio.

Capítulo X
Acceso Inautorizado

ART. 420.- Comete el delito de acceso inautorizado, la persona -- que sin autorización o permiso:

I.- Ilegalmente tenga acceso a la información, a los programas informáticos de una tercera persona, o bien

II.- Deliberadamente tenga acceso a informaciones o programas informáticos de alguna otra persona.

Se le impondrá pena de 3 a 5 años de prisión y hasta doscientos días multa. Debiendose entender por acceso inautorizado, toda entrada a un sistema computacional, realizado por una persona sin autorización para ello, por algún medio de la informática.

Por otra parte;

5.- Instrumentar, los fabricantes de sofware y hardware, Seguros para Compañias, Universidades, Institutos de Investigación, Instituciones Bancarias, Servicios de Inteligencia, etc., estrategias de seguridad lógica, de seguridad física, de seguridad manual, de seguridad prudencial y de seguridad social.

6.- Instruir a los ciudadanos, respecto de sus libertades civiles

ésto basado primeramente en el hecho de que los sistemas de telecomunicación y los escuchadores o soplones de la computadora, generalmente es una intrusión permanente y clandestina; que interfieren la libertades civiles.

7.- Reformar la ley adjetiva, creando nuevos preceptos que establescan como elementos probatorios el deber de traspasar la captura de objetos de evidencia y el deber de testificar ante éstas nuevas incriminalidades, ya que en lo que concierne a la prueba se levantaran grandes dificultades, cabe mencionar el adagio latino " verva volant, scripta manent " es más real que nunca para las informaciones tratadas por la computadora cuya volatibilidad no faltara.

Boletín de Política Informática, México, Año XIII- Núm. 4, -- I.N.L.G.I., Abril de 1990.

Burgoa Orihuela, Ignacio, Las Garantías Individuales, México, 22a. ed., Edit. Porrúa, S.A., 1986.

Carranca y Trujillo, Raúl, Derecho Penal Mexicano, México, -- XVIa. ed. Porrúa, S.A., 1988.

Castellanos Tena, Fernando, Lineamientos Elementales de Derecho Penal, México, 31a. ed., Edit. Porrúa, S.A., 1992.

Correa, Carlos M, Derecho Informático, Buenos Aires, Edit. De palma, 1987.

Del Pont K, Luis Marco, Manual de Criminología, México, Edit. Porrúa, S.A., 1987.

Diccionario Pequeño Larousse, España, Ediciones Larousse, --- 1981.

Gasein, Raymond, Derecho Penal de la Informática: Relación -- presentada al Congreso de la Asociación Europea de los Magistrados, Niza, Mayo- 1985.

Lima, Ma. de la Luz, Delitos Electrónicos, México, Revista -- Criminalia, Año L, Nos. 1-6, Edit. Porrúa, S.A., 1984.

Masse, Michel, VIII Congreso de la Asociación Francesa de derecho Penal, Grenoble, 1985

Mompin Poblet, Jóse, Telemática, Barcelona, Edit. Marcombo,-- S.A. de Boixareú Editores, 1986.

Norton, Peter y Nielsen, Paul, Norton Antivirus, México, Edit. Prentice Hall Hispanoamericana, S.A., 1992.

Prado, Pedro Antonio, La Informática y el Abogado, Buenos Aires, Argentina, Editorial Abeledo-Perrot, 1988.

Pérez Carrillo, Agustín, Derechos Humanos, Desobediencia Civil y Delitos Políticos, México, Cuaderno del inacipe Núm. 39, 1991.

Revista Méxicana de Comunicación, LA GUERRA ELECTRONICA Y DE PAPEL, México, Año seis- Núm. 34, Abril- Mayo de 1992.

Roszak, Theodore, El Culto a la Información, México, Edit. Grijalbo, S.A., Consejo Nacional para la Cultura y las Artes, 1990.

Sanders H., Donald, Informática: Presente y Futuro, México, Edit. McGraw- Hill, 1987.

Sinonetti, Jóse M. y Virgolini, Julio E. S, Del Delito de Cuello Blanco a la Economía Criminal, México, Cuaderno del inacipe Núm. 35, 1991.

Telléz Valdes, Julio, La Protección Jurídica de los Programas de Computación, México, Segunda edición, U.N.A.M., 1989.

Telléz Valdes, Julio, Derecho Informático, México, Primera edición, U.N.A.M., 1987.

Tocaven, Roberto, Psicología Criminal, México, Cuaderno del inacipe No. I, 1990.

Uhlrich, Sieber, XIII Congreso Internacional, de Leyes Comparadas, Montreal, Canadá, 1990.

LEGISLACION

CODIGO PENAL PARA EL D.F., México, 52a. Ed., Edit. Porrúa, S.A. 1994.

Compilación de Legislación Comparada de actos ilícitos informáticos de Alemania, E.U.A., Dinamarca y Canadá, sin autor, y sin fecha de publicación.

CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS, México, 103 a ed., Edit. Porrúa, S.A., 1994.