UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

ARAGON

FACULTAD DE DERECHO

" DELITOS DE INFORMATICA "

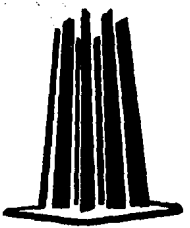
T E S I S

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN DERECHO

P R E S E N T A

BLANCA PATRICIA MEZA LEON



ENEP ARAGON MEXICO, D. F. 1994

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

A mis progenitores :

Blanca León Quintanar

Y

Daniel Meza Villaseñor

A ustedes, a quienes debo éste gran objetivo que he realizado en mi vida, agradezco sus cuidados, sus desvelos y consuelo durante tantas horas y noches de angustia y preocupacion en mi niñez.

A mi amado Padre por tus detalles de amor y ternura, tu tiempo y dedicación para unir a nuestra gran familia y por tu apoyo y comprensión.

A ti, Madre bendita que rasgue tu vientre para llegar a ser hoy mujer y realizarme, y por encontrar en ti una amiga.

Y gracias a Nuestro Padre Celestial que oro porque selle su matrimonio para volvernos a reunir en lo futuro como hoy, por permitirnos conocerle y saber que sin El nada somos.

A mi esposo :

Miguel Cuanalo Ibarra

Compañero inseparable de mi juventud, ternura, amor, confianza y comprensión que apoyo la terminación de éste objetivo que me traze a cambio de una linda familia, nuestros hijos.

A mis hijos :

Daphnis Miyel

Dyan Yufni

Miyoshi D'Franceli

Alegria de mi vida, gozo de grandes promesas hechas por el Señor y sueño interrumpido de constante preocupación, empero motivación deseos y animo de superación para afrontar el futuro.

A mis hermanos :

Con respeto y cariño por sus palabras de ánimo y preocupación, porque yo alcanze un desarrollo profesional. Que mi deseo es que ustedes tambien logren la excelencia con sus familias.

A Lic. Roberto Martín López

Con profundo cariño, respeto y agradecimiento por su tiempo en la formación de profesionales y por orientarme a concretar mi anhelo.

A mi maestro y amigo :

Lic. Cesareo Hernández Hernández.

Con admiracion y agradecimiento por todo lo que me ensenaste y en especial por tu tiempo y la amistad que me brindaste.

A mis maestros y revisores de ésta tesis:

Agradezco el tiempo de ensenanza en las aulas del saber y por su disposición en revisar éste trabajo sobre una materia relativamente nueva "Delitos de Informática"

A mi amigo :

Jorge Luis

Te agradezco tu ayuda en la realización de éste sueno y por haberte conocido.

DELITOS DE INFORMATICA

INTRODUCCION

Estamos viviendo una época de avances extraordinarios en cuanto al uso y sofisticación de la tecnología, hablando especificamente de las computadoras y el uso que se les ha dado en la actualidad.

La computadora, en otros tiempos se consideraba que sólo debia ser usada por gente muy inteligente o muy preparada, actualmente se ha ido adentrando en muchas actividades que el hombre realiza, no sólo en fábricas, oficinas, escuelas, hospitales, bancos y almacenes sino hasta en los propios hogares de un número cada vez mayor de personas, de ésta forma nos podemos dar cuenta facilmente que se han ido modificando muchas facetas sociales.

Gracias al uso de la computadora, muchos trabajos que anteriormente eran tediosos y muy tardados hoy con sólo una parte del esfuerzo aplicado al mismo trabajo y con ésta herramienta poderosa se ha disminuido grandemente el tiempo empleado en dichos trabajos. Esto coloca al hombre en posición de disfrutar un mayor tiempo libre que puede usar en actividades culturales y de entretenimiento, aunque tambien estas áreas han sufrido modificaciones debido a la informática.

Es precisamente debido al gran impacto que existe con respecto a la informática que hemos elegido el tema de "Delitos de Informática". Hablar de un tema como el mencionado puede parecer un tanto lejano de la realidad pero no es asi, debido a la fusion de la informática con las telecomunicaciones y a la creación de redes informáticas de las industrias y negocios, los delitos en éste campo han aumentado en forma alarmante, dicha situación se ve intensificada debido a la carencia de tipificación al respecto que se sofistica conforme la tecnología avanza.

Las consecuencias de los delitos cometidos en la informática son ya innumerables y no es el propósito de éste trabajo enumerarlos, ya que sería practicamente imposible, pero a manera de información mencionaré los siguientes:

1. Introducción de datos falsos.

2. Modificación de los resultados finales.

3. Empleo de fórmulas y programas que ejecutan instrucciones para borrar información importante.

4. Empleo de programas, como uno llamado "Salami" que redondea las cuentas bancarias y las carga a una cuenta determinada previamente y que ha enriquecido a los usuarios de una forma rápida y sin esfuerzo.

5. Robo del tiempo de la computadora que ocurre cuando los empleados la usan sin autorización, con la correspondiente depreciación.

Para una mejor comprensión de éste trabajo lo hemos dividido en cinco capítulos :

Capítulo primero. Trata sobre el tema del delito, sin embargo está dirigido a posibles lectores legos en Derecho.

Capítulo segundo. Se compone de tres partes que hablan sobre los aspectos técnicos, económicos y sociales de las computadoras, en éste último, la primera parte contiene una sección destinada a personas no adentradas en el conocimiento de dichas máquinas.

Capítulo tercero. Trata acerca de una nueva forma de criminalidad que se establece en los ilícitos denominados como "delitos de cuello blanco", nos referimos al que hemos llamado "abusos informáticos".

Capítulo cuarto. Presentamos la situación internacional relativa al aspecto legal, es decir, la forma en que legalmente se están enfrentando otros países a ésta situación.

Capítulo quinto. Se expone la situación nacional en su aspecto legal, que a falta de legislación expresa, se señalan las figuras jurídicas-penales existentes que podrían estar vinculadas a las conductas ilícitas derivadas del uso de la computadora.

Consideraciones finales.

Se presentan propuestas destinadas a la solución de los problemas expuestos.

Dichas propuestas se basan en el razonamiento lógico de la problemática en cuestión, teniendo como piedra angular el escaso material obtenido.

Las aplicaciones en México de la informática presentan una enorme cantidad de posibilidades y una gran cantidad de uso durante los próximos años, sin embargo se generarán a la par resultados por demás indeseables, por lo que considero estamos a tiempo de tomar las medidas apropiadas y estar preparados a fin de enfrentar los problemas que se presenten cuando estemos al nivel de los países altamente industrializados y se haya incrementado la cantidad y calidad de los delitos informáticos.

CAPITULO I

EL DELITO

I.1 DEFINICION

La palabra delito proviene de la voz latina 'delinquere', que significa abandonar, apartarse del buen camino, alejarse del sendero senalado por la ley.

Francisco Carrara, principal exponente de la Escuela Clásica, lo define así: "Es la infracción de la ley del estado promulgada para proteger la seguridad de los ciudadanos, resultante de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente danoso (1)".

A su vez, Rafael Garófalo, representante del Positivismo, lo define de la siguiente manera: "Es la violación de los sentimientos altruistas de probidad y de piedad en la medida media indispensable para la adaptación del individuo a la colectividad (2)".

Por su parte, el Artículo 7o. del Código Penal vigente para el Distrito Federal, establece: "Delito es el acto u omisión que sancionan las leyes penales".

De estas distintas definiciones, podemos resumir que el delito consiste en un conjunto de actos u omisiones que el Estado ha establecido previamente con el fin fundamental de proteger a la sociedad, castigando a quien se adecue a los mismos y, a su vez, esto sirva de ejemplo a la colectividad, pues al saber de la forma en que se es castigado, es menos probable que incurra en un ilícito penal.

---

(1) Citado por CASTELLANOS Tena, Fernando. Lineamientos Elementales de Derecho Penal. México, Edit. Porrúa, 1984, Vigésima ed., pp. 125 y 126.

(2) Ibidem, p. 126.

I.1.B. 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).

No obstante que los partidarios de la Corriente Atomizadora le atribuyen varios elementos al delito, aun entre ellos existen diferencias pues no para todos son los mismos. Así tenemos que a Raúl Carrancá y Trujillo dice: "Delito es el acto típicamente antijurídico, culpable, sometido a veces a condiciones objetivas de penalidad, imputable a un hombre y sometido a una sanción penal (3)".

De este concepto se desprenden los siguientes elementos:

- Acción: Es todo hecho humano voluntario o movimiento voluntario de organismo capaz de modificar el mundo exterior o de poner en peligro dicha modificación.

- Tipicidad: Encuadramiento de un conducta con la descripción hecha en la ley.

- Antijuricidad: Es la violación del valor o bien protegido a que se contrae el tipo penal respectivo.

- Imputabilidad: Es la posibilidad condicionada por la salud mental y por el desarrollo del autor para obrar según el justo conocimiento del deber existente.

- Culpabilidad: Es el nexo intelectual y emocional que liga al sujeto con su acto.

---

(3) CARRANCA y Trujillo, Raúl, Derecho Penal Mexicano. México, Edit. Porrúa, 15a. ed., p. 223.

- Punibilidad : Es el merecimiento de una pena en función de la realización de una conducta determinada, misma que se aplica por el Estado conforme a la Ley.

- Condiciones objetivas de penalidad: Son las exigencias ocasionalmente establecidas por el legislador para que la pena tenga aplicación.

Sin embargo, para Fernando Castellanos la imputabilidad, la punibilidad y las condiciones objetivas de penalidad, no son elementos esenciales del delito, en base a los siguientes razonamientos:

"la imputabilidad es un presupuesto de la culpabilidad en la que el sujeto no se rebela contra el derecho legislado (antijuricidad), sino que es una rebeldía anímica del sujeto (4)".

En cuanto a la punibilidad, considerada como componente de la norma en función de la calidad de la conducta, es decir, el merecimiento de una pena, este autor establece que "no es elemento esencial del delito porque la pena se merece por la naturaleza del comportamiento (5)".

Respecto a las condiciones objetivas de punibilidad, el Lic. Castellanos les niega el carácter de elementos esenciales del delito, toda vez que son sólo por excepción exigidas por el legislador como condiciones para la imposición de la pena.

Por lo tanto, para Fernando Castellanos, los elementos esenciales del delito son:

- Conducta
- Tipicidad
- Antijuricidad
- Culpabilidad (con imputabilidad como presupuesto necesario) (6)".

---

(4) CASTELLANOS Tena, Fernando. Op, cit. p. 130.
(5) CASTELLANOS Tena, Fernando. Loc. cit.
(6) CASTELLANOS Tena, Fernando. Op. cit. p. 132.

I.2 CLASIFICACION

Los delitos se ordenan en función de diferentes factores como son:

- Gravedad
- Conducta
- Resultado
- Dano que producen
- Duración
- Culpabilidad
- Estructura: simples y complejos
- Actos integrantes: Unisubsistentes y plurisubsistentes
- Sujetos: Unisubjetivos y plurisubjetivos
- Forma de persecución: Querella y oficio
- Comunes
- Federales
- Oficiales
- Militares
- Políticos
- Legal

GRAVEDAD: Aquí se considera la gravedad de la infracción penal, pudiendo ser:

- Faltas
- Delitos
- Crímenes

La legislación penal mexicana sólo habla de delitos, por lo tanto esta clasificación resulta inoficiosa.

CONDUCTA: De acuerdo con la manifestación de la voluntad, los delitos pueden ser de acción y de omisión:

- DELITOS DE ACCION: Este tipo de delitos se consuman a través de un comportamiento positivo, es decir, de un hacer, en los que se viola una ley prohibitiva.

- DELITOS DE OMISION: Estos consiten en una abstención, en un no hacer lo que la ley ordena, por lo tanto se infringe una ley dispositiva. Este tipo de delitos se subdividen a su vez en:

  a). DELITOS DE SIMPLE OMISION: Es la falta de una conducta ordenada por la ley en la que se castigan no tanto por el resultado que originen, sino por la propia omisión. Aquí existe una lesión juridica y un resultado formal, se viola una ley dispositiva.

  b). DELITOS DE COMISION POR OMISION: En éstos se causa un resultado material por el hecho de que el sujeto activo no lleva a cabo un comportamiento específico, es decir, por el solo hecho de no actuar se produce un resultado. Aquí se da una violación jurídica y un resultado material, infringiéndose una ley dispositiva y una prohibitiva.

RESULTADO: Esta clasificación atiende al resultado que producen:

- FORMALES: El tipo penal se colma con el movimiento corporal o por la omisión, aunque para su integración no se manifiesta un resultado externo; lo que se castiga es la conducta en sí.

- MATERIALES: Este sí requiere para su integración un resultado externo.

DANO QUE PRODUCEN: Este orden se da en base al dano sufrido por el sujeto pasivo:

- LESION: Provocan un dano directo y efectivo contra intereses jurídicamente tutelados por el mandato de la ley desobedecido.

- PELIGRO: Aunque no causen un dano directo a los intereses protegidos por la ley, sí los ponen en peligro (y de éste existe la posibilidad de que se cause un dano).

DURACION: Este orden procede en función al tiempo que se utiliza en su comisión. Es de gran importancia, pues de la determinación del mismo, se sabe a partir de qué momento empieza a correr el término para la prescripción. De acuerdo con el Artículo 7o. del Código Penal vigente para el Distrito Federal, el delito puede ser:

- INSTANTANEO: Es el que se produce en un solo instante. Dicho mumeral en su Fracción I expresa al respecto: Instantáneo: cuando la consumación se agota en el mismo momento en que se han realizado todos sus elementos constitutivos.

- PERMANENTE: En éste existe una continuidad tanto en la conciencia del sujeto activo como en su ejecución. El artículo mencionado en su Fracción II lo establece como: "cuando la consumación se prolonga en el tiempo".

El Lic. Castellanos Tena considera que "el delito permanente requiere esencialmente la facultad por parte del agente activo de remover o hacer cesar el estado antijurídico creado con su conducta (7)".

Al respecto, el Lic. Francisco Pavón Vasconcelos opina que "el estado antijurídico cesa en ocasiones por iniciativa del sujeto activo, en otras es el propio sujeto pasivo el que pone fin a dicho estado; en algunos casos puede ser un tercero. Por último, el estado antijurídico puede ser removido como consecuencia de la intervención ciega de fuerzas de la naturaleza o animales (8)".

Por nuestra parte, nosotros estamos de acuerdo con el Lic. Pavón, pues para que cese el delito permanente, como bien lo expresa él, no sólo depende de la voluntad del sujeto activo sino también de los otros factores señalados por este autor.

Es importante determinar en que momento se consuma el delito permanente. Para algunos autores, es en el instante en que tiene lugar la comprensión del bien jurídico, sin embargo este criterio no ha sido aceptado puesto que la consumación continúa después de iniciada la comprensión. Otros consideran que el delito permanente se consuma cuando cesa la comprensión del bien jurídico, más no toman en cuenta que el delito, en este caso, ya cesó.

---

(7) CASTELLANOS Tena, Fernando. Op. cit. p. 140.

(8) PAVON Vasconcelos, Francisco. Manual de Derecho Penal Mexicano. México. Edit. Porrúa, 1984, 6a. ed., p.232.

Otros juristas, entre ellos el Lic. Pavón Vasconcelos, estiman que "no hay un momento consumativo, sino un periodo de consumación que va desde el inicio de la compresión del bien hasta la cesación de la misma y, por tanto, en todo ese periódo, el delito se está consumando (9)".

Consideramos que es de gran trascendencia determinar el tiempo y lugar en que se consuma el delito permanente, pues de aquí se fijan, aparte del término para la prescripción, la competencia del tribunal que debe conocer del mismo.

- CONTINUADO: Este se produce a través de varias acciones y una sola lesión jurídica, es decir, es continuado en la conciencia y discontinuo en la ejecución. Sus elementos son:

a). Unidad de resolución
b). Pluralidad de acciones
c). Unidad de lesión jurídica

El Artículo 7, Fracción III mencionado, lo define como el que se da "cuando con unidad de propósito delictivo y pluralidad de conductas, se viola el mismo precepto legal".

CULPABILIDAD: atendiendo al factor culpabilidad, los delitos se clasifican en dolosos y culposos. El Código Penal vigente para el Distrito Federal en su Artículo 8 los ordena en:

- Intencionales (dolo)
- No intencionales (culpa)
- Preterintencionales

a). DOLOSOS: Estos se presentan cuando el sujeto activo dirige su voluntad consciente a la ejecución de un hecho típico y antijurídico.

---

(9) PAVON Vasconcelos, Francisco. Op. cit. p. 233.

b). CULPOSOS: Aquí el sujeto activo no quiere el resultado típico y antijurídico, sin embargo éste se origina por la falta de cuidado y precaución que el Estado exige para asegurar la vida en común.

c). PRETERINTENCIONALES: Estos se presentan cuando el resultado va más allá de la intención del sujeto activo.

ESTRUCTURA: Esta clasificación se deriva de la estructura del delito y se subdivide en:

- SIMPLES: Cuando existe una sola lesión jurídica.

- COMPLEJOS: En éstos la norma jurídica se compone de la fusión de dos delitos. Al integrarse en uno solo, se crea una nueva figura jurídica, por lo mismo, más grave.

ACTOS INTEGRANTES: Los delitos se agrupan de acuerdo al número de actos que los componen y así tenemos a los:

- UNISUBSISTENTES: Estos se integran por un solo acto.

- PLURISUBSISTENTES: Se forman por varios actos.

SUJETOS: En esta agrupación, la clasificación es en función de los individuos que participan en la ejecución de los delitos pudiendo éstos ser:

- UNISUBJETIVOS: Sólo requieren de un individuo para su ejecución.

- PLURISUBJETIVOS: Es menester la concurrencia de dos individuos para la ejecución del ilícito penal.

FORMA DE PERSECUCION: Este orden se da conforme al conocimiento que la autoridad tiene del delito para poder perseguirlo y que puede ser:

- QUERELLA : Son perseguibles por la autoridad sólo cuando así lo manifieste la parte agraviada, previa querella. En éstos surte efecto el perdón del ofendido.

- DE OFICIO: La autoridad tiene conocimiento de ellos a través de una denuncia y está obligada, por mandato de ley, a perseguir y castigar a los responsables. Aquí no procede el perdón del ofendido ya que no lo afectan sólo a él, sino también a la sociedad.

COMUNES: Son los que se establecen por legislaturas locales y que se aplican sólo en los estados correspondientes.

FEDERALES: Estos se expiden por el Congreso de la Unión, por lo tanto tienen aplicación en todo el territorio nacional.

OFICIALES: Esta clasificación se refiere a los delitos cometidos por un empleado público en el ejercicio de sus funciones.

MILITARES: Estos delitos se agrupan en función de la disciplina del Ejército, por lo tanto, sólo se aplica a los miembros de éste.

POLITICOS: El Artículo 144 del Código Penal vigente para el Distrito Federal establece como delitos políticos los siguientes:

- Rebelión
- Sedición
- Motín
- Conspiración para cometerlos

LEGAL : Esta clasificación se establece en base al bien jurídico tutelado, el cual da el nombre a cada uno de los 23 títulos de que se compone el Código Penal a partir del Libro Segundo.

I.3 LA CONDUCTA O HECHO

Todo delito se compone necesariamente por una conducta humana pero,?qué es la conducta?

CONDUCTA: Es el comportamiento humano voluntario, positivo o negativo, es decir, un hacer o un no hacer, encaminado a un propósito delictuoso. (Lato sensu).

HECHO: Si la acción u omisión producen un resultado de tipo material, a dicha actividad o inactividad se le denómina hecho.

I.3.A. SUJETO DE LA CONDUCTA

Siendo el derecho el conjunto de normas jurídicas que regulan la conducta del hombre en sociedad, la acción u omisión a que se refiere el Artículo 7o. del Código Penal vigente para el Distrito Federal, sólo corresponde al hombre, pues sólo él puede violar las normas legales.

I.3.B. LAS PERSONAS MORALES COMO SUJETOS DE LA CONDUCTA

Por lo que se refiere a las personas morales, éstas no pueden ser sujetos activos del delito pues carecen de voluntad y, por lo tanto, de conducta, elemento esencial del delito. Sin embargo, éstas se convierten en sujetos pasivos cuando las personas físicas que las constituyen infringen las normas jurídicas.

Sobre el particular, el Lic. Pavón Vasconcelos apoya el criterio que limita la responsabilidad de las personas jurídicas al campo del Derecho Privado y fundamentalmente al aspecto patrimonial, en orden a la inaplicación por cuanto a ellas respecta, del concepto de imputabilidad. La persona moral no delinque (10).

---

(10) PAVON Vasconcelos, Francisco. Op. cit. p. 165.

Sin embargo, continua diciendo "Ante hechos delictivos cometidos por personas físicas a nombre de aquellas o en beneficio directo de las mismas con independencia de las sanciones que correspondan a los autores, personas físicas cabe la imposición de medidas especiales o de seguridad que puedan señalar los jueces y que van de la simple suspensión a la disolución de dichas sociedades, como un recurso de defensa de parte del Estado, lo que lleva a considerar que si bien la persona moral o jurídica carece de capacidad para cometer delitos, sí la tiene, en cambio para sufrir penas (11)".

I.3.C. SUJETO PASIVO Y OFENDIDO

SUJETO PASIVO: Poseedor del derecho violado y jurídicamente protegido por la norma.

OFENDIDO: Es el que resiente el daño causado por la violación de la norma penal.

Por lo regular, siempre el sujeto pasivo y el ofendido son la misma persona.

I.3.D. OBJETO DEL DELITO

El objeto del delito se subdivide en:

a). MATERIAL: Persona o cosa que resiente el daño o peligro.

b). JURIDICO: Bien jurídicamente tutelado por la ley y que resulta perjudicado.

---

(11) Ibidem, p. 166.

I.3.E. LA ACCION

La palabra acción proviene de la voz latina "actio" que significa movimiento.

En strictu sensu, la acción es todo hecho humano voluntario o movimiento corporal capaz de modificar el mundo exterior o de poner en peligro dicha modificación.

Cuando se comete un delito de acción, se está haciendo lo prohibido, es decir, lo que la ley ordena que no se haga, por lo tanto, se viola una ley prohibitiva. Aquí el sujeto activo quiere que suceda un resultado, por lo tanto, encamina su acción a que éste se produzca. De ésto se desprenden los elementos de la acción:

- Manifestación de la voluntad
- Un resultado
- Relación de causalidad

I.3.F. LA OMISION

La omisión consiste en un dejar de hacer lo que se debe realizar, es decir, un abstenerse de actuar, una inactividad.

En los delitos de omisión se deja de hacer lo ordenado expresamente por la ley, por lo tanto, se viola una ley dispositiva. La omisión se divide a su vez en:

a). OMISION SIMPLE: Es el no hacer voluntario o culposo en el que se viola una norma preceptiva y se produce un resultado jurídico pero no material, por eso aquí no hay relación causal entre ambos.

b). COMISION POR OMISION: En ésta se presenta una doble violación de deberes; por un lado, está el de hacer y por el otro, el de no hacer, produciendo con ésto un resultado jurídico y otro material, existiendo entre ambos una relación de causalidad, por lo tanto se violan dos leyes, una prohibitiva y una preceptiva.

Para Sebastián Soler, la mera abstención causal se transforma en omisión causal y punible cuando el acto que hubiera evitado el resultado era jurídicamente exigible. Según este autor, ese deber de obrar subsiste en tres casos diferentes:

- Cuando emana de un precepto jurídico específico.
- Si existe una obligación especialmente contraída a ese fin.
- Cuando un acto precedente impone esa obligación (12).

Los elementos de la omisión son:

- Voluntad
- Inactividad
- Relación causal (en los de comisión por omisión)

I.3.G LUGAR Y TIEMPO DE LA COMISION DEL DELITO

Generalmente la actividad o la omisión se efectúan en el mismo tiempo y lugar en que se produce el resultado, pero en algunas ocasiones esto no siempre sucede.

En los delitos a distancia existe el problema de determinar qué ley es la que se va a aplicar. El problema se agrava cuando estos se cometen no sólo en un estado diferente al en que se produjo el resultado, sino en un país diverso.

Para la solución de este problema existen las siguientes teorías:

a). TEORIA DE LA ACTIVIDAD: Considera como cometido el delito en el tiempo y lugar de la acción u omisión.

b). TEORIA DEL RESULTADO: Establece que el delito se ha cometido en el tiempo y lugar en que se produce el resultado.

---

(12) Citado por CASTELLANOS Tena, Fernando. Op. cit. p. 160.

c). TEORIA DEL CONJUNTO: Manifiesta que el delito se comete tanto en el tiempo y lugar en que se realiza la acción u omisión, como en el tiempo y lugar en que se producen los resultados.

A falta de una norma expresa, por lo regular en México siempre se ha aplicado la Teoría del Resultado.

I.4 AUSENCIA DE CONDUCTA

Como ya se dijo, todo delito se compone necesariamente de una conducta humana y si ésta falta, no se configuraría el mismo.

Para que se dé el caso de que falte la conducta en la integración del delito, sería por:

a). VIS ABSOLUTA: Esta se contempla en el Artículo 15, Fracción I del Código Penal, pues quien comete un delito forzado físicamente a ello, no es su conducta la que impera, sino la de quien lo ha obligado, convirtiéndose así en un instrumento de quien lo ha obligado, convirtiéndose así en un intrumento de quien emplea la vis absoluta, por lo tanto, aquí opera la hipótesis "nullum crimen sine actione".

b). VIS MAIOR: Aunque ésta no se encuentra contemplada en la legislación penal, si se comete un delito bajo estas circunstancias, quien lo realiza no tuvo el deseo de hacerlo, es decir, faltó la voluntad, elemento necesario de la conducta humana, sino que fue empujado por fuerza de la naturaleza.

c). MOVIMIENTOS REFLEJOS: Estos son movimientos corporales involuntarios, o sea que el hombre no puede controlar, pero en caso de que ésto sea factible, existiría la voluntad del sujeto y, por lo tanto, conducta, elemento esencial del delito.

I.5 LA TIPICIDAD

Al disponer la Constitución Política de los Estados Unidos Mexicanos en su Artículo 14 que:

"En los juicios del orden criminal queda prohibido imponer por simple analogía y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trate", quiere decir que si no hay tipicidad, no hay delito, infiriendo que ésta es un elemento esencial del delito.

I.5.A. DEFINICION DE TIPICIDAD

Para Raúl Carrancá y Trujillo, "la tipicidad es la conformidad de una conducta con la hipótesis delictiva consignada en la ley penal (13)", es decir, es la coincidencia del comportamiento con lo descrito por el legislador y, por consecuencia, sólo podrá ser delictiva la acción que encaje en el tipo.

I.5.B. DEFINICION DE TIPO Y CLASIFICACION

TIPO: Es la descripción que el Estado realiza de una conducta prohibida en una norma jurídico-penal (14).

Los tipos se clasifican de varias maneras, a continuación se enlistan algunos:

a). NORMAL: Es el que utiliza conceptos totalmente objetivos.

b). ANORMAL: Es el que requiere ser valorado desde el punto de vista cultural o jurídico.

c). FUNDAMENTAL: Se da en cuanto que describe el bien jurídico tutelado.

---

(13) CARRANCA y Trujillo, Raúl. op. cit. p. 171.

(14) Instituto de Investigaciones jurídicas. Diccionario Jurídico Mexicano. México, Edit. Porrúa, 1985, Tomo VIII, p. 281.

d). ESPECIAL: Se presenta cuando se da el tipo fundamental más otras circunstancias excluyendo la aplicación del primero por el segundo.

e). COMPLEMENTADO: Es la adición del tipo fundamental más otros requisitos en los que se aplica tanto el tipo fundamental como aquel en que se encuentren contemplados dichos requisitos.

f). AUTONOMO: Es el que no necesita de otro tipo para existir.

g). SUBORDINADO: Requiere de la existencia de otro para tener vida propia.

h). CASUISTICO: Es el que describe varias formas de llevar a cabo el delito.

I.6 ATIPICIDAD

La atipicidad se entiende como la ausencia de adecuación de la conducta al tipo, es decir, que no se integren todos los elementos que describen el tipo y, por lo mismo, si la conducta no es típica, tampoco es delictuosa.

La atipicidad podría darse, entre otras causas:

a). Por no llevar a cabo el acto conforme lo señala el tipo.

b). Por no reunir los sujetos activo y pasivo las características establecidas en el tipo.

I.7 LA ANTIJURIDICIDAD

Existen diferentes opiniones acerca de una definición sobre este concepto:

Para Castellanos Tena, "la antijuridicidad radica en la violación del valor o bien protegido a que se contrae el tipo penal respectivo (15)".

Por su parte, García Máynez señala que "son conductas antijurídicas las que omiten un acto ordenado y las que ejecutan uno prohibido (16)".

En esencia, consideramos que ambos conceptos se refieren a lo mismo, es decir, a que la antijuridicidad se da en cuanto el sujeto activo encuadra su conducta con lo que expresa la norma penal.

Según Cuello Calón, la antijuridicidad tiene un doble aspecto:

a). FORMAL: Consiste en la rebeldía contra la norma jurídica.

b). MATERIAL: Daño o perjuicio social causado por esa rebeldía (17).

1.7.A AUSENCIA DE ANTIJURIDICIDAD

En algunas ocasiones, aunque el sujeto activo se haya apegado a la norma penal, puede suceder que su conducta no sea antijurídica. Esto sucede cuando existe alguna causa de justificación.

---

(15) CASTELLANOS Tena, Fernando. Op. cit. p. 178.
(16) GARCIA Máynez, Eduardo. Introducción al Estudio del Derecho. México, Edit. Porrúa, 1970, 17a. ed., pp. 221.
(17) Citado por CASTELLANOS Tena, Fernando. Op. cit. pp. 180 y 181.

I.8 CAUSAS DE JUSTIFICACION

Cuando se presenta una causa de justificación en una conducta típica, el delito no se configura pues faltaría uno de esos elementos esenciales como es la antijuridicidad. En otras palabras, existiendo una causa de justificación, no hay delito.

I.8.A. CARACTERISTICAS

a). Son objetivas
b). Se refieren al hecho (conducta externa de un sujeto capaz)
c). Son impersonales
d). Conllevan responsabilidad civil o penal
e). Requieren de declaración expresa del legislador

I.8.B. FUNDAMENTOS

Para que en una conducta típica opere una causa de justificación, ésta debe motivarse por dos razones:

a). AUSENCIA DE INTERESES: Se presenta cuando el ofendido da su consentimiento o cuando el Derecho considera como ilícita una conducta sin la aprobación del sujeto pasivo. Procede el consentimiento porque a través de la conducta típica no se quebranta la armonía colectiva, interés que trata de proteger el orden jurídico.

b). INTERESES PREPONDERANTES: Este se presenta cuando existen dos intereses incompatibles y no pudiéndose salvar ambos, se sacrifica el de menor valía, preservando el preponderante.

Cabe hacer mención que el exceso en una conducta legitimada por una causa de justificación da lugar a un delito y así lo establece el Artículo 16 del Código Penal vigente para el Distrito Federal que al efecto señala: "Al que se exceda en los casos de legítima defensa, estado de necesidad, cumplimiento de un deber, ejercicio de un Derecho u obediencia jerárquica..., será penado como delincuente por imprudencia".

I.8.C CAUSAS DE JUSTIFICACION

De acuerdo con el numeral antes transcrito, las causas de justificación son:

- Legítima defensa
- Estado de necesidad
- Cumplimiento de un deber
- Ejercicio de un derecho
- Impedimento legítimo

A continuación nos referiremos brevemente a las dos primeras por ser las de mayor importancia:

a). LEGITIMA DEFENSA: Carrancá y Trujillo define a la legítima defensa como "la repulsa de una agresión antijurídica y actual por el atacado o por terceras personas contra el agresor sin traspasar la medida necesaria para la protección (18)".

En base a ésto, la legítima defensa tiene su fundamento en que al haber un choque entre intereses incompatibles, el del injusto agredido tiene más valor, es el preponderante, y al defenderse obra con justo derecho.

La legítima defensa, valga la redundancia, se legitima en el Artículo 15 Fracción III, primer párrafo del multicitado ordenamiento penal al señalar: "Son circunstancias excluyentes de responsabilidad penal:

III. Obrar el acusado en defensa de su persona, honor o bienes de otro, repeliendo una agresión actual, violenta, sin derecho y de la cual resulte un peligro inminente...".

Conforme al texto de ley, la agresión debe ser actual, de presente, pues si ésta ya se realizó, no dará lugar a una defensa legítima, sino a una venganza prevista en el Artículo 17 constitucional que reza: "... Ninguna persona podrá hacerse justicia por sí misma ni ejercer violencia para reclamar su derecho...".

---

(18) CARRANCA Y Trujillo, Raúl. Op. cit. p. 531.

Como ya se dijo, al que sobrepase los límites de la defensa, se encuadra en una conducta ya tipificada por el Artículo 16 del ordenamiento penal ya mencionado.

De acuerdo con la definición mencionada, se desprenden como elementos de la legítima defensa los siguientes:

- Una agresión injusta y actual
- Un peligro inminente de daño derivado de la agresión sobre bienes jurídicamente tutelados
- Repulsa de esa agresión

b). ESTADO DE NECESIDAD: Para Liszt, el estado de necesidad "es una situación de peligro actual de los intereses protegidos por el Derecho, en la cual no queda otro remedio que la violación de los intereses de otro, jurídicamente protegidos; es, por consiguiente, un caso de colisión de intereses (19)".

A su vez, el Lic. Pavón Vasconcelos lo define como "la situación de peligro cierto y grave, cuya superación para el amenazado, hace imprescindible el sacrificio del interés ajeno como único medio para salvaguardar el propio (20)".

Ante estos dos bienes antagónicos, el Estado escoge el de más valor, es decir, el que tiene el interés preponderante.

Esta justificante cobra actualidad sólamente cuando el bien salvado es mayor que el sacrificado, pues si sucede lo contrario, se estaría configurando el delito ya que se lesionan bienes de un inocente.

El Código Penal para el Distrito Federal, describe el estado de necesidad en su Artículo 15, Fracción IV, el cual a la letra dice:

---

(19) Citado por CARRANCA Y Trujillo, Raúl. Op. cit. p. 569.

(20) PAVON Vasconcelos, Francisco. Op. cit. p. 321.

"El miedo grave o el temor fundado e irresistible de un mal inminente y grave en la persona del contraventor o la necesidad de salvar su propia persona o sus bienes o la persona o bienes de otro, de un peligro real, grave e inminente, siempre que no exista otro medio practicable y menos perjudicial".

De la definición anterior se desprenden los elementos del estado de necesidad y son:

- Situación de peligro real, grave e inminente.
- Que la amenaza recaiga sobre cualquier bien jurídicamente tutelado (propio o ajeno).
- Ataque de quien esté en el estado necesario.
- Ausencia de otro medio practicable y menos perjudicial.

I.9 LA IMPUTABILIDAD

Como ya se dijo al principio de este capítulo, el Lic. Castellanos Tena le niega el carácter de elemento del delito a la imputabilidad, considerándola, sin embargo, un presupuesto de la culpabilidad, pero ?qué es la imputabilidad?

I.9.A. DEFINICION

Según este autor, la imputabilidad "es la posibilidad condicionada por la salud mental y por el desarrollo del autor, para obrar según el justo conocimiento del deber existente. En pocas palabras, podemos definir la imputabilidad como la capacidad de entender y de querer en el campo del Derecho Penal (21)".

Sobre este punto, el penalista Pavón Vasconcelos señala: "El conocimiento de la ilicitud del hecho y del deber de acatamiento del mandato de hacer o de no hacer, contenido en la norma, es revelador de que el sujeto reúne, a tal fin, las condiciones mínimas de salud y desarrollo mental para aprehender, respecto del hecho concreto, su significación jurídica y su vinculación personal con ésta (22)".

---

(21) CASTELLANOS Tena, Fernando. Op. cit. p. 218.

(22) PAVON Vasconcelos, Francisco. Op. cit. p. 367.

En base a las definiciones anteriores, consideramos, en suma, que la imputabilidad se concreta fundamentalmente en el querer y entender del sujeto, así como la comprensión de lo que está haciendo en razón del suficiente desarrollo intelectual, por ser mayor de edad y de la salud mental que le permita elaborar una correcta valoración de lo jurídico y lo antijurídico.

I.10 LA INIMPUTABILIDAD

Si la imputabilidad se refiere al desarrollo y salud mental del sujeto, las causas de inimputabilidad, por ende, serían todas aquellas que invaliden dicho desarrollo y salud mental, quedando el sujeto sin aptitud y capacidad psicológica al momento de cometer el ilícito penal.

I.10.A. CAUSAS DE INIMPUTABILIDAD

El Artículo 15, Fracción II del Código Penal para el Distrito Federal, señala las causas de inimputabilidad al establecer: "Padecer el inculpado, al cometer la infracción, trastorno mental o desarrollo intelectual retardado que le impida comprender el carácter ilícito del hecho o conducirse de acuerdo con esa comprensión, excepto en los casos en que el propio sujeto activo haya provocado esa incapacidad intencional o imprudencialmente".

De este texto se derivan las causas de inimputabilidad:

a). Trastorno mental: Perturbación de las facultades psíquicas.

b). Desarrollo intelectual retardado.

c). Miedo grave: Se considera en la Fracción IV del mismno numeral. Afecta la capacidad psicológica del individuo, pues puede producirle inconciencia o automatismo.

Cabe mencionar que cuando existen causas de inimputabilidad, aunque se configura el delito, podría decirse que no hay delincuente.

I.11 LA CULPABILIDAD

I.11.A. DEFINICION

El Lic. Castellanos Tena define a la culpabilidad como "el nexo intelectual y emocional que liga al sujeto con su acto (23)".

Por su parte, el Lic. Pavón Vasconcelos la conceptúa como "el reproche hecho al autor sobre su conducta antijurídica (24)".

I.11.B. CLASES DE CULPABILIDAD

Para realizar esta división, se toma en cuenta la voluntad del sujeto para la consecución del resultado.

a). DOLO: Aquí el sujeto actúa en forma consciente y de manera voluntaria con el único propósito de producir un resultado típico y antijurídico.

Del concepto anterior se desprenden los elementos del dolo que son:

- Etico: Conciencia de que se viola una ley.
- Emocional: Deseo de realizar la conducta típica.

El Artículo 9 del multicitado Código Penal, en su primer párrafo describe este tipo de culpa: "Obrar intencionalmente el que conociendo las circunstancias del hecho típico, quiera o acepte el resultado prohibido por la Ley".

b). CULPA: Esta se presenta cuando el sujeto actúa sin la intención de causar un resultado típico, pero éste se produce a pesar de ser previsible y evitable, por no tomar las precauciones indispensables exigidas por el Estado para la vida en común.

---

(23) CASTELLANOS Tena, Fernando. Op. cit. p. 234.

(24) PAVON Vasconcelos, Francisco. Op. cit. p. 359.

Afirma el Lic. Castellanos que en la culpa "se ejecuta el acto con la esperanza de que no ocurrirá el resultado" (25).

También de esta definición se derivan los elementos de la culpa:

- Conducta voluntaria.
- Que ésta se realice sin las precauciones exigidas por el Estado.
- Que el resultado sea previsible, evitable y tipificado por la ley penal.
- Relación de causalidad entre la conducta y el resultado.

La culpa se clasifica, por cuestiones puramente relacionadas a la mayor o menor penalidad, de la siguiente forma:

- LATA: Cuando el resultado pudo preverlo cualquier persona.
- LEVE: Cuando éste pudo preverlo sólo una persona cuidadosa.
- LEVISIMA: Cuando el resultado sólo es previsible por sujetos sumamente diligentes.

El Artículo 9 citado se refiere a la culpa en su segundo párrafo al señalar: "Obra imprudencialmente el que realiza el hecho típico incumpliendo un deber de cuidado, que las circunstancias y condiciones personales le imponen".

c). PRETERINTENCION: Ocurre cuando el sujeto, dolosamente quiere causar un resultado típico menor y ocasiona culposamente uno más grave que sobrepasa su intención.

El referido Artículo 9 menciona este obrar en su último párrafo que a la letra dice: "Obra preterintencionalmente el que cause un resultado típico mayor al querido o aceptado, si aquel se produce por imprudencia".

d). CASO FORTUITO: Este se presenta cuando ocurre un hecho típico ejecutado por un sujeto que actúa lícita y cautelosamente, sin embargo, no quiso el resultado ni pudo preverlo puesto que no era previsible, sino que éste se dio por una causa independiente o ajena a él.

---

(25) CASTELLANOS Tena, Fernando. Op. cit. p. 247.

Esta situación está contemplada por nuestro Código Penal en su Artículo 15, Fracción X, el cual textualmente establece:

"Causar un daño por mero accidente, sin intención ni imprudencia alguna, ejecutando un hecho lícito con todas las precauciones debidas".

I.12. LA INCULPABILIDAD

Como ya se mencionó en el apartado anterior, los elementos de la culpabilidad son el conocimiento de que se viola una ley y el deseo de realizar la conducta típica. Por lo tanto, si no existen éstos, opera la inculpabilidad.

I.12.A. CAUSAS DE INCULPABILIDAD

Estas se presentan cuando existe el error esencial de hecho, el cual afecta el conocimiento del sujeto y la coacción sobre la voluntad, misma que se ve alterada.

a). ERROR: Es la falsa creencia de la realidad; es decir, ésta se conoce, pero equivocadamente. El error se divide en error de hecho y error de Derecho.

- ERROR DE DERECHO: El sujeto activo, por un error esencial de hecho insuperable cree, cuando realiza un hecho típico penal, que se encuentra amparado por una justificante, o ejecutar una conducta lícita sin que ésta lo sea.

En éste, el sujeto actúa de manera antijurídica creyendo que lo hace lícitamente, más no por eso se le excluye de responsabilidad, aunque sí la pena se ve disminuida conforme al Artículo 59 del ya tantas veces mencionado Código Penal que reza; "Cuando el hecho se realice por error o ignorancia invencible sobre la existencia de la ley penal o del alcance de ésta, en virtud del extremo atraso cultural y el aislamiento social del sujeto, se le podrá imponer hasta la cuarta parte de la pena correspondiente al delito de que se trate o tratamiento en libertad, según la naturaleza del caso".

- ERROR DE HECHO: A diferencia del error de Derecho, éste si es excluyente de responsabilidad penal, según lo dispone el Artículo 15 en su Fracción XI del ordenamiento señalado que textualmente dice: "Realizar la acción y omisión bajo un error invencible respecto de alguno de los elementos esenciales que integran la descripción legal o que por el mismo error estime el sujeto activo que es lícita su conducta. No se excluye la responsabilidad si el error es vencible".

b). COACCION SOBRE LA VOLUNTAD: Se presenta cuando el sujeto conscientemente pero con voluntad coaccionada, ejecuta una conducta o hecho típicos penalmente. Esta situación se contempla en la Fracción IV del Artículo 15 del Código Penal vigente la cual ya fue transcrita en apartados anteriores.

I.13. LA PUNIBILIDAD

I.13.A. DEFINICION

PUNIBILIDAD: Es el merecimiento de una pena en función de la realización de una conducta determinada, misma que se aplica por el Estado conforme a la ley.

Para el penalista Pavón Vasconcelos, la punibilidad, a la que considera elemento integral del delito, "es la amenaza de pena que el Estado asocia a la violación de los deberes consignados en las normas jurídicas, dictadas para garantizar la permanencia del orden social (26)".

I.13.B. ELEMENTOS

a). Merecimiento de penas.
b). Conminación del Estado de imposición de sanciones si se llenan los presupuestos legales.
c). Aplicación fáctica de las penas señaladas en la ley.

---

(26) PAVON Vasconcelos, Francisco. Op. cit. p. 421.

I.14. EXCUSAS ABSOLUTORIAS

Son las causas que impiden la aplicación de la pena, aún cuando la conducta sea completamente delictuosa.

Raúl Carrancá y Trujillo las define así: "Son circunstancias en las que, a pesar de subsistir la antijuridicidad y la culpabilidad, queda excluida desde el primer momento la posibilidad de imponer la pena al autor (27)".

Entre este tipo de excusas se encuentra la que opera en razón de la mínima temibilidad. Esta se establece en el Artículo 73 del multicitado ordenamiento penal que a continuación se transcribe y si se reunen las características que este numeral señala, no se impondrá sanción alguna, lo cual procede en razón del arrepentimiento del sujeto activo y de su mínima temibilidad: "Cuando el valor de lo robado no pase de 10 veces el salario, sea restituido por el infractor espontáneamente y pague éste todos los daños y perjuicios antes de que la autoridad tome conocimiento del delito, no se impondrá sanción alguna si no se ha ejecutado el robo por medio de la violencia".

Se puede decir que en caso de presentarse una excusa absolutoria, aunque se configure el delito y existe el delincuente, no hay pena.

I.15. LA VIDA DEL DELITO

I.15.A. FASES DEL DELITO

Para que un delito surja, éste primero se concibe en la mente del sujeto activo, naciendo como delito en el momento de su consumación. A este proceso se le conoce como inter criminis o camino del crimen y se integra por las siguientes fases:

---

(27) CARRANCA y Trujillo, Raúl. Op. cit. p. 651.

a). FASE INTERNA: Esta fase se compone a su vez de los siguientes aspectos:

- IDEACION: Es la etapa en la que el sujeto tiene la tentación de delinquir, pudiendo inducirse o disuadirse de ello.

- DELIBERACION: Cuando el sujeto persiste con la idea de delinquir, llega a esta etapa en la que valúa los puntos favorables y en su contra por la acción ilícita que piensa realizar.

- RESOLUCION: En esta fase, el sujeto está completamente decidido a delinquir, más no lo ha hecho todavía, es decir, su pensamiento no ha cambiado para nada el mundo externo y, por lo tanto, no puede ser incriminado por eso, de acuerdo al principio proclamado por Ulpiano: "Cogitationis poenam nemo patitur", el cual significa que nadie puede ser penado por sus pensamientos.

b). FASE EXTERNA: Se integra a partir del momento en que la idea del sujeto deja de ser tal, alterando ya el mundo exterior con la consumación del delito. Esta fase se compone de las siguientes etapas:

- MANIFESTACION: Se presenta cuando el sujeto exterioriza su pensamiento, más no por eso se le puede incriminar, ya que ésta es una garantía contemplada en el Artículo 6º de nuestra Carta magna que a la letra dice: "La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de terceros, provoque algún delito o perturbe el orden público, el derecho a la información será garantizado por el Estado".

- PREPARACION: Es la fase en la que el sujeto realiza ciertos actos preparatorios que por sí mismos no constituyen un delito, aunque estén encaminados a ello.

- EJECUCION: Es el instante preciso, el momento fundamental en el que se ejecuta el delito. Esta etapa puede presentar dos situaciones:

i). TENTATIVA: Se compone por los actos ejecutivos que realiza el sujeto para la consumación del delito, el cual no se ejecuta por causas ajenas a él. De aquí se desprenden los elementos de la tentativa:

-Intención dirigida a cometer un delito.

-Actos ejecutivos realizados por el agente.

-Resultado no verificado por causas ajenas a la voluntad del sujeto.

Como en la tentativa se ponen en peligro intereses juridicamente tutelados, ésta sí es punible, aunque no con la severidad con la que se castiga el delito consumado, de acuerdo con el Artículo 12 del Código Penal vigente para el Distrito Federal que dispone: "Existe tentativa punible cuando la resolución de cometer un delito se exterioriza ejecutando la conducta que debería producirlo u omitiendo la que debería evitarlo, si aquel no se consuma por causas ajenas a la voluntad del agente".

Sin embargo, si el sujeto espontaneamente desiste de su accion criminosa, no será punible la tentativa, de acuerdo con el último párrafo del mismo numeral.

ii). CONSUMACION: Es la ejecución propiamente dicha, que reune todos los elementos genéricos y específicos del tipo legal.

CAPITULO II

COMPUTADORAS

I. ASPECTO TECNICO

El uso positivo o negativo de las computadoras se ha extendido tan rápidamente que su presencia no puede ser negada o ignorada, pero ?qué es una computadora? ?qué hacen?.

I.1. DEFINICION

COMPUTADORA: Es un rápido y exacto sistema de manejo de simbolos electrónicos (datos) que es proyectado, diseñado y organizado para aceptar y almacenar automáticamente datos de entrada, procesarlos y producir resultados de salida bajo la dirección de un detallado programa almacenado de instrucciones (1).

De la definición anterior, se desprenden los siguientes términos:

- SISTEMA: Es un grupo de partes integradas que tienen el propósito común de lograr algún o algunos objetivos.
- GRUPO DE PARTES: Un sistema se compone por más de un elemento.
- PARTES INTEGRADAS: Debe existir una relación lógica entre las partes de un sistema.
- PROPOSITOS COMUNES PARA EL LOGRO DE ALGUNOS OBJETIVOS: Todos los elementos de un sistema deben ser controlados de tal modo que la meta del sistema sea alcanzada.

---

(1) SANDERS, H. Donald. Informática: Presente y Futuro. México, Edit. MacGraw-Hill, 1987, p. 9.

- DATO: (Data, en latín), significa 'hecho', por lo tanto, los datos son hechos o material original de información.

- INFORMACION: Es el conocimiento relevante producido como resultado del procesamiento de datos adquiridos por las personas para realizar el entendimiento y cumplir con propósitos específicos.

- PROCESAMIENTO DE DATOS: Consiste en la recolección de datos primarios de entrada que son evaluados y ordenados para ser colocados en la perspectiva necesaria para que se produzca información útil.

- PROGRAMA: Es un conjunto detallado de instrucciones preparado por el hombre y escrito en un lenguaje de programación que, introducido en una computadora, la dirige para que ésta funcione desempeñando un determinado cometido y produzca el resultado deseado.

I.2. ORGANIZACION BASICA DE UN SISTEMA DE COMPUTACION

Una computadora se compone fundamentalmente de dos partes:

a). HARDWARE: Se integra por las partes mecánicas, electromecánicas y electrónicas, como estructura física de las computadoras. Los elementos clave de este sistema incluyen dispositivos de entrada, de procesamiento y de salida.

b). SOFTWARE: Se compone por la estructura lógico-matemática que permite a la computadora la ejecución del trabajo a realizarse.

I.2.A. DISPOSITIVOS DE ENTRADA

Los sistemas de computación usan muchos dispositivos para la entrada de datos. Algunos permiten la comunicación directa entre los humanos y las máquinas y otros sólo entre estas últimas. Sin embargo, sin importar el tipo de dispositivo usado, todos son componentes para la interpretación y comunicación entre personas y sistemas de computación. A continuación se señalan algunos:

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: La cinta puede estar en un gran carrete o en un pequeno cartucho o cassette. Es una cinta de plástico cubierta por un lado con una capa de óxido de hierro que se puede magnetizar. Mediante impulsos electromagnéticos se graban pequenos puntos invisibles que representan datos en el lado de la cinta que está cubierto por óxido de hierro.

d). DISCOS FLEXIBLES: Se llaman así por estar fabricados con un material plástico flexible. Esta base plástica está recubierta con una substancia magnetizable de óxido de hierro sobre el cual se registran o graban los datos en forma de pequenos puntos magnéticos invisibles.

e). LECTORES DE CARACTERES DE TINTA MAGNETICA: Los documentos 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 entran a la unidad lectora, los datos pasan a través de un campo que magnetiza las partículas contenidas en la tinta, después, mediante cabezas lectoras, se pueden interpretar 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 transferisrse a cinta magnética para su procesamiento posterior.

f). LECTORAS DE CARACTERES OPTICOS: Las técnicas de caracteres ópticos permiten la lectura directa de cualquier carácter impreso y no se requiere tinta especial. Las lectoras de caracteres ópticos están hechas para interpretar marcas o caracteres manuscritos o impresos a máquina y códigos de barras especiales.

g). TERMINALES TELEIMPRESORAS: Para captar o introducir datos, cuentan con un teclado parecido al de una maquina de escribir y una impresora interconstruida para registrar lo que se haya teclado.

h). TERMINALES PORTATILES DE CAPTACION DE DATOS: Tienen teclados de tamano reducido, reciben energia de baterias y se emplean para enviar datos a una computadora y recibir información proveniente de la Unidad Central de Procesamiento.

i). TERMINALES PARA OPERACIONES FINANCIERAS: Por lo regular se utilizan en la transferencia electrónica de fondos.
El usuario introduce una tarjeta plástica en la que están grabados magnéticamente y en código sobre una tira de cinta adherida al reverso de la misma, el número de cuenta y el límite de crédito. La terminal lee y transmite los datos de la cinta a la Unidad Central de Procesamiento, que activa la cuenta del usuario. Siguiendo las instrucciones exhibidas en una pantalla y oprimiendo algunas teclas, se indica a la computadora que realice las operaciones deseadas.

j). TERMINALES DE DESPLIEGUE VISUAL: Se emplea el teclado de una terminal para introducir datos a la Unidad Central de Procesamiento (UCP) y se usa un tubo de rayos catódicos para mostrar los datos de entrada y recibir información procesada y mensajes 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.

La pluma luminosa es una fotocelda colocada en un pequeno tubo; cuando el usuario la mueve sobre la pantalla, ésta detecta la luz proveniente de un limitado campo de visión; la luz del tubo de rayos catódicos hace que la fotocelda responda cuando la pluma se apunta directamente a una área iluminada. Esta respuesta eléctrica se transmite a la computadora, la cual determina que parte de lo exhibido provoca la respuesta de la fotocelda.

k). 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.
También pueden almacenarse en la terminal pruebas programadas de detección de errores para verificar la validez de los datos de entrada.

l). SISTEMAS DE ENTRADA POR MEDIO DE LA VOZ: Se utiliza un micrófono o teléfono para convertir la voz a señales eléctricas; después los patrones de la señal se transmiten a una computadora en donde se comparan con un "diccionario" de patrones que previamente so han almacenado. Cuando se encuentra la coincidencia necesaria, se ha reconocido la voz y la computadora produce la salida adecuada.

I.2.B. UNIDAD CENTRAL DE PROCESAMIENTO

La Unidad Central de Procesamiento, mejor conocida como UCP, es el dispositivo en el que se ejecutan las operaciones lógico-matemáticas, por lo que se le considera como el corazón de un sistema de computación. La UCP se integra como sigue:

a). SECCION PRIMARIA DE ALMACENAMIENTO (MEMORIA): Se usa para cuatro propósitos:

- Los datos son alimentados en una área de almacenamiento de entrada donde son guardados hasta que se vayan a procesar.

- El área de almacenamiento de trabajo se emplea para retener los datos que están siendo procesados y los resultados intermedios de tal procesamiento.

- Area de almacenamiento de salida: Conserva los resultados finales de las operaciones de procesamiento hasta que puedan ser liberados.

- Area de programa almacenado: Guarda las instrucciones del procesamiento.

Además del almacenamiento primario o sección de memoria principal, la mayoría de las computadoras tienen capacidad de almacenamiento secundario, también conocidas como auxiliares o externas. Estas son máquinas generalmente conectadas en línea (directamente) al CPU; sirven como bibliotecas para aceptar datos en forma directa y regresar datos también directamente a la UCP sin intervención humana.

b). SECCION ARITMETICO-LOGICA: Aquí se ejecutan todos los cálculos y todas las comparaciones (decisiones). Una vez que los datos pasan de los dispositivos de entrada al almacenamiento primario, son guardados y transferidos conforme son necesitados, a la sección aritmético - lógica y es allí donde tiene lugar el procesamiento. No hay procesamiento en la sección primaria. Los resultados intermedios generados en la sección aritmético - lógica son colocados temporalmente en un área de almacenamiento de trabajo designada hasta que son necesitados después.

c). SECCION DE CONTROL: Aunque no ejecuta ningún procesamiento real de datos, la unidad de control actúa como un sistema nervioso central para los otros componentes de la computadora, pues si cada uno de los dispositivos sabe cuándo y cómo debe 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 a otra.

El hardware de una computadora también se integra por lo que se conoce como ROM (Read Only Memory). Memoria sólo para leer; es un programa fijo de la computadora en la que se contienen las instrucciones fundamentales para hacerla funcionar cuando es encendida y únicamente pueden ser leídas por la máquina. Este programa no puede ser cambiado.

El firmware llamado también lógica almacenada, forma parte del hardware de una computadora. Consiste en los microprogramas que están ya contenidos en la computadora y que son proporcionados por la empresa que las fabrica. Se encuentran almacenados en el ROM y su función es permitir que una computadora interprete y ejecute las instrucciones escritas para una máquina diferente, es decir, analiza y codifica instrucciones ajenas en operaciones elementales para las que cada UCP fue diseñada. El firmware es una parte del sistema de cómputo y no puede ser cambiado y alterado por los usuarios.

I.2.C. DISPOSITIVOS DE SALIDA

Los dispositivos de salida son instrumentos de interpretación y comunicación entre los humanos y el sistema de computación. Los dispositivos tomas los resultados de salida de la UCP en forma de código de máquina y los convierten a una forma que puede ser usada:

- Por una persona, como podría ser un reporte impreso.
- Como entrada para máquina en otro ciclo de procesamiento, por ejemplo una cinta magnética.

A continuación se señalan algunos de los dispositivos de salida. Como algunos de éstos funcionan también como mecanismos de entrada, ya se hizo referencia a ellos en el apartado correspondiente, concretándonos sólo a enunciarlos y explicar brevemente los no vistos:

a). TARJETA PERFORADA

b). CINTA DE PAPEL PERFORADO

c). CINTA MAGNETICA

d). DISCO MAGNETICO

e). IMPRESORA DE CARACTER: Este es uno de los dispositivos de salida que prepara documentos que serán usados por 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 líneas de información por minuto.

f). MICROFILM: Aquí se registra la información de salida de computadora en la forma de imagenes microscópicas filmadas. A una hoja de película de cuatro por seis pulgadas, se le conopce como microficha, la cual reproduce hasta 270 imágenes del tamano de una página, sin embargo, existen sistemas de ultrafichas que pueden almacenar mil páginas normales en el mismo espacio.

g). PANTALLA: Se le conoce como dispositivo de despliegue alfanumérico, por lo tanto sólo recibe información de salida en forma de letras, números y caracteres especiales, pudiendo desplegar en cada exhibición 24 líneas de hasta 80 caracteres cada una, es decir, se exhiben hasta 1,920 caracteres.

h). GRAFICADOR: Con una entrada de datos alfanuméricos, los usuarios pueden crear imágenes coloridas e informativas en las pantallas de sus terminales, pudiendo obtener copias permanentes por medio de la graficadora. Esta funciona como se indica a continuación: El papel se coloca sobre un tambor que gira en uno y otro sentido para producir un movimiento hacia arriba y hacia abajo. Un carro que sostiene una o más plumas con distinto color de tinta está montado a lo largo del tambor. Las plumas pueden moverse a lo largo de ese carro para producir un movimiento a través del papel. Bajo el control de la computadora, los movimientos del carro y del tambor funcionan simultáneamente para producir una imagen. El programa de computadora controla el color y la cantidad de tinta que se deposita sobre el papel.

i). 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 las preguntas, 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.

Cabe senalar que todas las unidades de entrada, salida y almacenamiento secundario son algunas veces llamadas dispositivos periféricos o sólamente periféricos. Esta terminología se refiere al hecho de que aunque dichos mecanismos no son parte de la UCP, casi siempre se localizan cerca de ella.

Dentro de este apartado destinado a describir lo que es el hardware de una computadora, consideremos que es permisible incluir un dispositivo que no podemos pasar por alto y que ha tenido gran injerencia debido al beneficio que reporta la unión de la computación con las comunicaciones, convergencia de la que resulta un nuevo término: Telemática, siendo ésta el conjunto de tecnologías de telecomunicación.

A las transmisiones por radio, televisión y teléfono, se han unido los satélites artificiales y las transmisiones por cables ópticos. La computadora se ha integrado a esta compleja red de telecomunicaciones, con lo cual multiplica enormemente sus funciones y, por ende, sus beneficios.

El dispositivo al que nos estamos refiriendo es el Modem, mecanismo de modulación-demodulación que transforma los impulsos eléctricos digitales utilizados por una computadora en impulsos de ondas análogas de variación continua utilizados para transmitir la voz humana a través de una línea telefónica.

Este dispositivo funciona de la siguiente manera: El modem de la localidad donde se encuentra la UCP modula la salida de la senal de digital a analógica, es decir, convierte los pulsos digitales en tonos auditivos que son recogidos por la bocina telefónica y otro modem en la localidad remota demodula la senal transmitida de analógica a digital, o sea, la transforma nuevamente en pulsos digitales. Una senal digital es una serie de 0 y 1 (encendido y apagado), conocidos como byte.

Los canales de transmisión de datos que se utilizan para transportar datos de una localidad a otra son clasificados en tres categorías, a saber:

a). Banda angosta: Su velocidad de transmisión es de cinco a 30 caracteres por segundo.

b). Banda de voz: Tienen mayor amplitud de banda, por lo que también aumenta su velocidad de transmisión hasta mil caracteres por segundo.

c). Banda ancha: Este canal se utiliza cuando se requiere transmitir grandes volúmenes de datos a altas velocidades, pues alcanza a emitir más de 100 mil caracteres por segundo. Esta función se realiza mediante el uso de cable coaxial, circuitos de microonda o satélites de comunicación.

Para transportar los datos a través de estos canales de transmisión, existen diversas organizaciones:

1. Redes de Transmisión Pública: Lo hacen a través de redes telefónicas y telegráficas.

2. Redes especializadas de Transmisión Pública: Emplean las facilidades de la banda ancha, tales como satélites, cable coaxial y circuitos de microonda.

3. Redes de Transmisión de Valor Agregado: Generalmente usan las líneas telefónicas y las facilidades de transmisión de otros proveedores.

De esta forma se transmiten los datos de un estado, de un país o, incluso, de un continente a otro.

Sin embargo, cuando la transmisión se realiza entre computadoras, terminales u otros dispositivos localizados en un área pequeña como un edificio de oficinas o una planta de producción, se efectúa a través de una red local propiedad de la empresa que la utiliza, empleando para ello cable coaxial o de fibras ópticas y unidades especiales de interfase.

Debido a la asociación de la computadora en las comunicaciones vía modem, la computadora se puede conectar fácilmente con cualquier parte del mundo.

I.2.D. SOFTWARE

Los componentes del sistema de computación, es decir, el hardware, puede aceptar datos, procesarlos y producir resultados de salida, sólo siguiendo un detallado conjunto de instrucciones contenidas en un programa almacenado (sistema operativo). El software es precisamente ese conjunto de instrucciones que le dicen a la computadora lo que tiene que hacer.

Por lo tanto, el software de una computadora es todo aquello que no se puede tocar en esta máquina; son sus pensamientos, por eso representa el trabajo intelectual del hombre. Es el programa que el programador realiza para poner a trabajar a la máquina para la solución de problemas.

Como ya se dijo, un programa es un detallado conjunto de instrucciones preparado por humanos y escrito en un lenguaje de programación que, introducido en una computadora, la dirige para que ésta funciones desempeñando un determinado cometido y produzca el resultado deseado (2).

Sin embargo los datos que las computadoras manejan deben estar organizados en agrupamientos lógicos para que los procesos sean efectivos y los resultados obtenidos sean útiles. A continuación se señala la jerarquía de agrupación:

1. Campo: Es un grupo de caracteres unidos tratados como una sola unidad.

2. Registro: Agrupación de campos unidos o grupos de datos tratados como una sola unidad.

3. Archivo: Es un número de registros relacionados que son tratados como una sola unidad.

4. Base de datos o banco de datos: Es una colección de datos lógicamente relacionados que pueden ser estructurados en diferentes formas para cumplir con las necesidades de proceso y que se pueden usar con múltiples propósitos.

Las operaciones que realizan las computadoras con los datos se clasifican en cuatro categorías:

a). Entrada/salida

b). Cálculo

c). Comparación/lógica

d). Almacenamiento recuperación

---

(2) SANDERS, H. Donald. Op. cit. p. 9.

Para que el software realice su función, es necesario ordenar y rastrear los datos desde la entrada, el manejo y salida. Para este trabajo se emplea una especie de mapa en el que se usan símbolos y direcciones conocidos como Diagramas de Flujo, es decir, "es una representación detallada en forma gráfica de como deben realizarse los pasos en una UCP para producir la salida necesaria (3)".

Un diagrama de flujo mejora la comunicación, el entendimiento y contribuye a un efectivo análisis del problema y su síntesis.

Una vez que se ha analizado la programación, se requiere codificar las instrucciones especificadas necesarias para procesar una aplicación en un lenguaje en forma aceptable para el sistema de cómputo, pero, ?qué es un lenguaje?

I.2.E. LENGUAJES DE PROGRAMACION

Un lenguaje es un sistema de comunicación. Un lenguaje de programación consta de todos los símbolos, los caracteres y las reglas de utilización que permite que las personas se puedan comunicar con las computadoras. Cada lenguaje de comunicación debe tener intrucciones comprendidas entre las siguientes categorías que permiten que un sistema de cómputo realice un número de operaciones conocidas:

1. Instrucciones de entrada/salida: Se requiere para permitir la comunicación entre los dispositivos de entrada/salida y el procesador central.

2. Instrucciones de cálculo: son las que permiten sumar, restar, multiplicar y dividir durante un proceso.

3. Instrucciones de lógica/comparación: Se utiliza para transferir el control del programa. Durante el proceso dos unidades de datos pueden compararse entre sí como resultado de la ejecución de una instrucción de lógica.

4. Instrucciones de almacenamiento/ consulta y movimiento: Estas instrucciones se utilizan para almacenar, consultar y mover los datos durante el proceso.

---

(3) SANDERS, H. Donald. Op. cit. p. 324.

Aunque todos los lenguajes de programación tienen instrucciones que permiten que estas operaciones comunes se realicen, existe una gran diferencia en los símbolos, los caracteres y la sintaxis de los lenguajes de máquina, lenguajes ensambladores y lenguajes de alto nivel.

a). LENGUAJES DE MAQUINA

El lenguaje de máquina de una computadora consiste en cadenas de números binarios donde cada carácter o Bit (Binary Digit), se representa en una posición de almacenamiento por un arreglo de números binarios (0 y 1) que se expresan con una carga eléctrica y que son tratados como unidad o Byte, compuesto por ocho bits que se pueden disponer de 256 formas diferentes y cada una de éstas secuencias puede codificar una letra, un número o un símbolo. Este lenguaje es el único que entiende la UCP directamente. Una instrucción preparada en cualquier lenguaje de máquina debe tener cuando menos dos partes:

1. Comando u operación: Es la que le dice a la computadora cual es la función que realizará. Todas las máquinas cuentan con un código de operación para cada una de sus funciones.

2. Operando: Esta le dice a la máquina en donde encontrar o almacenar los datos u otras instrucciones que vayan a ser manejadas.

b). LENGUAJES ENSAMBLADOR

Este lenguaje traduce el símbolo especificado del código de operación, es decir, de la función que va a realizar la computadora, a su equivalente en el lenguaje de máquina. Este programa está diseñado para un modelo de fabricación específica de procesador.

Un programa fuente se compone de las instrucciones escritas por el programador en lenguaje ensamblador y cuando éste se convierte a código de máquina se le llama programa objeto.

c). LENGUAJE DE ALTO NIVEL

Los programas en lenguaje de alto nivel pueden ser utilizados con diferentes fabricantes de computadoras, por lo tanto, su uso se ha hecho más popular. A continuación se mencionan los más usuales:

1. BASIC (Beginner's All-Purpose Symbolic Instruction Code). Es un lenguaje interactivo creado en 1964 que permite la comunicación directa entre el usuario y el sistema de cómputo durante la preparación y el uso de los programas. Debido a la facilidad de su uso, es el lenguaje de computadora más generalizado en el mundo.

2. FORTRAN (Formula Translator).Este lenguaje fué introducido en 1957 y tiene un enfoque científico/matemático. Un programa Fortran consta de una serie de enunciados que suministran la entrada/salida, el cálculo, la lógica/comparación y otras instrucciones básicas a la computadora, las cuales se ejecutan en forma sucesiva hasta que la secuencia es alterada por un enunciado-instrucción de transferencia de control.

3. COBOL (Common Busines Oriented Languaje). Fue diseñado en 1960 específicamente para el procesamiento de datos de tipo comercial. Este programa está estructurado en forma de oraciones que dirigen al procesador en la realización de las operaciones necesarias. Un número variable de oraciones que tratan con la misma operación se agrupan para formar un párrafo; los párrafos interrelacionados pueden ser organizados dentro de una sección y éstas se agrupan en una división donde las siguientes cuatro divisiones completan la estructura jerárquica que se requiere para cualquier programa en COBOL.

- Primera división: Identificación División
- Segunda división: Environment Division
- Tercera división: Data Division
- Cuarta division: Procedure Division

Por supuesto, un programa fuente escrito en un lenguaje de alto nivel como los mencionados, debe también ser traducido a un código utilizable por la máquina; ésta operación la realiza tanto el compilador que es un programa traductor, como el intérprete, el cual consiste en el programa fuente y los datos a procesar cargados en la computadora, estando el intérprete permanentemente alambrado por el hardware que convierte cada instrucción de programa fuente a la forma de lenguaje de máquina que se necesita durante el procesamiento de datos.

I.2.F. SISTEMA OPERATIVO

A pesar de que las computadoras son tan rápidas, se deja ociosa gran parte de su capacidad, por eso fueron desarrollados los sistemas operativos que permiten a las computadoras procesar más de una aplicación al mismo tiempo, pero, ?qué es un sistema operativo?

SISTEMA OPERATIVO. Es un conjunto integrado de programas especializados que se utilizan para administrar los recursos y operaciones en general de un sistema de computación, donde cada programa cumple tareas especificas (4).

La administración general de un sistema de computadora está bajo el control de un programa maestro del Sistema Operativo. Este programa maestro se conoce con nombres tales como supervisor, monitor o rutina ejecutiva. El programa supervisor coordina todas las partes de un sistema operativo y reside en la sección de almacenamiento principal de la UCP.

---

(4) SANDERS, H: Donald. Op. cit. p. 466.

FUNCIONES DEL SISTEMA OPERATIVO

- Dirige y coordina el tráfico de datos e instrucciones entre las distintas partes de la computadora.

- Permite al sistema de cómputo supervisar automáticamente sus propias operaciones llamando a los programas de aplicación, traduciendo cualquier otro programa de servicio y administrando los datos necesarios para producir los resultados deseados por el usuario.

- Controla las operaciones de mantenimiento de entrada y salida.

- Mantiene un inventario de los trabajos que han sido corridos. Estos trabajos son marcados con la hora de entrada y salida del sistema. Debe registrarse e imprimirse el tiempo requerido para compilar y/o correr los programas.

- Controla la seguridad del sistema. Registra los intentos de utilización de palabras de entrada (passwords) no autorizadas provenientes de una terminal en línea. Así mismo, pueden imprimirse mensajes si se detecta alguna actividad sospechosa en una o más de las terminales.

Consideramos permisible incluir dentro del Software de un sistema de computación a la pastilla de memoria conocida como RAM (Random Access Memory, equivalente en espanol a Memoria de Acceso Aleatorio o al Azar). Es la memoria interna en la que se almacenan las instrucciones del programa (software) y los resultados del mismo, pero se vacía si se apaga la máquina.

Como ya dijimos, un sistema es un grupo de elementos integrados que tienen el propósito común de alcanzar algún objetivo, por lo tanto, el hardware necesita de un software adecuado para poder funcionar y, a su vez, éste necesita del hombre, por lo que el elemento central más importante en cualquier sistema basado en computadoras, es el factor humano; éste es quien hace trabajar a las computadoras, es el quien determina las necesidades de procesamiento, proporciona los datos de entrada, proyecta los procedimientos de proceso, selecciona el hardware, escribe programas de computadora y utiliza la salida procesada.

II. ASPECTO ECONOMICO

II.1. GENERALIDADES

Nunca antes se había vivido una época como la actual con tanta velocidad de aplicación de los nuevos descubrimientos. Tal es el caso de la computadora, pues en un corto periodo ha habido reducciones sorprendentes en su tamaño y a medida en que ésta se ha reducido, también se ha decrecido el costo de su uso y ha aumentado su velocidad de operación, así como su capacidad de almacenamiento.

El empleo de la nueva tecnología es la causa de muchos de los cambios que ocurren; desde hace un siglo las transformaciones más espectaculares tienen bases técnicas, por lo que existe la facilidad de proyectar un futuro regido por la tecnología.

El creciente acceso a las computadoras personales que son más baratas, más pequeñas y más poderosas, provocarán un importante cambio pues éstas no se encuentran aisladas como en sus inicios, sino unidas entre sí en potentes redes.

Como las computadoras se utilizan tanto en la fabricación de bienes como en la prestación de servicios, desempeñan un preponderante papel económico. De ésta forma, dichas máquinas están permitiendo, mediante la integración y disponibilidad de numerosos bancos de datos, la consecución de uno de los cometidos principales de la informática: La adecuada toma de decisiones.

Entre más sirva una información para reducir la incertidumbre en las decisiones efectuadas, mejor será su valor; sin embargo, como todo recurso básico, la información no es gratuita. El costo de la información obtenida debe compararse con los beneficios conseguidos de su uso, por lo tanto, ésta debe ser exacta, oportuna, completa y concisa, con lo que se mejora la calidad de las decisiones. Si falta alguna de éstas caracteristicas y que se explican a continuación, la calidad de las decisiones puede verse afectada:

a). EXACTITUD: Es el porcentaje de información correcta respecto al total de información generada en un período.

b). OPORTUNIDAD: Se refiere a la puntualidad de la información, pues de nada sirve que ésta sea exacta si llega demasiado tarde para ser usada.

c). INTEGRIDAD: Es la reunión de los hechos disponibles que se encuentran diseminados con el objeto de proporcionar información más completa.

d). CONCISION: Es el resumen de los datos verdaderamente importantes para la toma de decisiones.

Consideramos a la información como un recurso porque cuenta con los atributos de un recurso físico:

1. Tiene valor como el dinero, las materias primas o la fuerza laboral.

2. Tiene caracteristicas que permiten su medición en términos de uso, duración y efectos sobre otros recursos.

3. Puede ser valorada en términos de recolección, almacenamiento y recuperación.

4. Puede ser presupuestada y controlada.

5. Puede valuarse en términos de costo y valor de uso con fines de administración.

A raíz de la gran trascendencia que ha adquirido la información, algunos autores como R. Hartley, aseveran que ésta puede ser medida de función de su utilidad, así la cantidad de información será proporcional al número de alternativas que se dispongan en un momento dado (5).

Por su parte, Claude Shannon, menciona que a mayor y mejor información, menor será el desconocimiento de las personas (6).

De aquí se desprende, como dice el Dr. Julio Téllez Valdés, "que la información es un verdadero bien susceptible de apropiación con un innegable valor patrimonial inherente (7)" por lo que la informática, dada su importancia económica, esté considerada como una parte medular en varios países que le conceden a su materia prima, la información, un verdadero valor. La información es poder.

La actual revolución informática, cuyo poder se funda en la computadora, está generando, entre otras cosas nuevos aumentos de productividad y cambios en la competencia, lo que provoca una intensa reorganización de la economía.

---

(5) TELLEZ, Valdés Julio. Derecho Informático. México, UNAM, 1987, pp 66.
(6) Loc. cit.
(7) Ibidem p. 68.

II.2. IMPLICACIONES ECONOMICAS DERIVADAS DEL USO DE LA COMPUTADORA

1. IMPLICACIONES POSITIVAS.

Dentro de las implicaciones positivas del uso de la computadora consideradas desde un punto de vista económico, se encuentran las siguientes:

a). AUMENTO EN LA PRODUCTIVIDAD.

La utilización de sistemas de computación en las companias evita el desperdicio y mejora la eficiencia, lo cual da como resultado productos de mejor calidad y de precios más bajos, así como un mejor servicio a los clientes.

La tendencia a la fabricación con computadora incrementa la productividad de manera significativa y el panorama resultante de éste incremento posibilitará que un mayor número de personas obtenga un nivel de vida más alto, semanas laborales más cortas y más tiempo libre.

b). MEJOR SERVICIO.

El empleo de las computadoras en los negocios repercute en un mejor servicio a los clientes; por mencionar algunos:

- Decremento en los precios de los productos, consecuencia de evitar el desperdicio y mejorar la eficiencia.

- Menos tiempo de espera en las oficinas de prestadores de servicios como venta de boletos de líneas aéreas, reservaciones de hoteles o renta de autos.

- Solución más rápida y precisa a las preguntas formuladas por personas a las que la empresa presta sus servicios.

c). CAMBIOS EN LA COMPETENCIA

El uso de sistemas de información, según opinión de Nora y Minc, "aportará un considerable incremento en la productividad, la cual pondrá en mejores condiciones de competividad y abrirá nuevos causes (8)", como serían las ventas al exterior. Así mismo, la competencia obligará a las empresas no informatizadas a alinearse con sus rivales nacionales o extranjeros o serán víctimas de competidores más eficientes.

2. IMPLICACIONES NEGATIVAS.

Sin embargo, económicamente también existen implicaciones negativas por el uso de éstas máquinas:

a). PROBLEMAS EN EL DISEÑO DE SISTEMAS DE INFORMACION

Este puede representar una tarea aparte de compleja, desafiante; además, el desarrollo del software continuará siendo más alto y más costoso que el del hardware.

b). PROBLEMAS EN LA ESTRUCTURACION DE LA EMPRESA

Cuando se introducen nuevos sistemas de computación en una compañía, se pueden reagrupar, crear o deshacer grupos de trabajo; los departamentos existentes se pueden fusionar o eliminar y tales cambios pueden producir una resistencia al cambio en los empleados y tensión en las empresas.

---

(8) NORA, Simon y MINC, Alain. La informatización de la sociedad, México, Fondo de cultura Económica, 1981, p. 19.

c). PROBLEMAS POR LA CONCENTRACION DE PODER.

Las empresas que no logren introducir herramientas controladas por computadora para mejorar su productividad, están condenadas a desaparecer en caso de que no se informaticen, pues no pueden permanecer estáticas en una sociedad tan dinámica como la actual; también es factible que sean absorbidas por empresas informatizadas. Sin embargo, el resultado sería el monopolio, es decir, concentración de poder.

d) PROBLEMA DE DESEMPLEO

Los efectos positivos de la informática sobre la productividad acarrea efectos negativos sobre el empleo, pues se está dejando de utilizar mano de obra. Muchas empresas, para evitar problemas de tipo sindical, no están despidiendo a sus empleados; su política actual es simplemente dejar de contratar personal nuevo, reduciendo considerablemente sus contrataciones. A pesar de todo, los efectos de la informática sobre el empleo son ineluctables.

II.3. SISTEMA ELECTRONICO DE TRANSFERENCIA DE FONDOS.

Dentro del aspecto económico del uso de las computadoras, no podemos dejar de mencionar el Sistema Electrónico de Transferencia de Fondos (EFT) por el papel tan importante que desempeñan en el dinámico mercado de dinero, pues a través de éste se realizan operaciones financieras de uso común durante las 24 horas de todos los días del año. Algunas de ellas son:

1. Identificar al individuo.
2. Recibir dinero en efectivo.
3. Entregar dinero en efectivo.
4. Transferir fondos entre cuentas.
5. Autorizar créditos.

6. Pagar cuentas en forma automática. A través de un teléfono digital o de una computadora personal, el usuario, desde su hogar u oficina, puede establecer una comunicación directa con la computadora del banco.

Una de las estaciones del EFT, es el cajero automático, dispositivo sin servidor que se localiza dentro o fuera de las instalaciones de las instituciones financieras para recibir y entregar dinero en efectivo y manejar operaciones financieras de rutina.

El usuario de un cajero automático introduce en éste una tarjeta plástica en cuyo reverso se encuentran grabados magnéticamente en código sobre una tira de cinta adherida, el número de cuenta y el límite de crédito. La terminal lee y transmite los datos de ésta cinta a una UCP activando la cuenta del usuario, quien al seguir las instrucciones exhibidas en una pantalla y oprimir algunas teclas, le indica a la computadora las operaciones que desea realizar.

Respecto a la trascendencia que éste sistema tiene, el INEGI menciona: "Incluidos en tales aspectos económicos, debe considerarse el tratamiento internacional de la información financiera que a través de redes especializadas y a través de los sistemas de transferencia electrónica de fondos, se realizarán en el futuro inmediato cada vez en mayor medida (9)".

(9). Instituto Nacional de Estadística, Geografía e Informática. La Informática y el Derecho. Informática Jurídica y Derecho Informático para México. México, Secretaría de Educación Pública, 1983, p. 50.

III. ASPECTO SOCIAL

III.1. GENERALIDADES

Como ya se dijo, aunque actualmente las computadoras se usan tanto en la fabricación de bienes como en la prestación de servicios, el elemento central más importante en cualquier sistema de computación es el factor humano. Es el hombre quien hace trabajar a éstas máquinas.

Su gran uso presente y que indudablemente se incrementará en el futuro, permite predecir que las computadoras ejercerán un profundo efecto social, tanto en las personas como en las empresas. Dicho efecto se debe en gran parte a la cada vez mayor facilidad de comunicación entre el ser humano y la máquina, consecuencia de la evolución de los lenguajes de programación convirtiéndose en lenguajes corrientes o casi corrientes, así como a la multitud de computadoras existentes en el mercado que cada vez son más potentes, más baratas y, por lo mismo, ya al alcance de un agente económico medio, lo que ha provocado una informática de masas que invadirá a toda la sociedad, quitándole así el carácter elitista que la investía en sus inicios.

Respecto al uso de las computadoras, Simon Nora y Alain Minc, en su libro Informatización de la Sociedad, dicen: "Ayer las posibilidades de la informática estaban delimitadas; eran comerciales, industriales o militares. De aquí en adelante, al dispersarse en una infinidad de pequeñas máquinas y ocultarse tras una red de ramificaciones ilimitadas, la informática se aduenará de la sociedad (10)".

La actual tecnología de computación anuncia innovaciones que modificará sustancialmente el curso de la civilización futura; se crearán herramientas y artefactos maravillosos; los cuales afectarán a los medios de comunicación, la salud, la educación y las actividades de recreo, por mencionar algunas, pero también provocarán desórdenes, repercutiendo, sobre todo, en el empleo.

---

(10) NORA, Simon y MINC, Alain. Op. cit. p. 50.

III.2. EFECTOS SOCIALES DE LA INFORMATIZACION SOBRE EL EMPLEO

Toda revolución tecnológica provoca una intensa reorganización de la sociedad y la actual Revolución Informática, basada en el poder tanto de la computadora como de las telecomunicaciones, está generando cambios. A continuación se senalan algunos efectos tanto positivos como negativos provocados por el uso de las computadoras en el empleo:

a). EFECTOS POSITIVOS

1. NUEVAS OPORTUNIDADES DE TRABAJO. Se han creado cientos de miles de nuevos empleos en áreas como la programación, la operación de computadoras y la administración de sistemas de información, donde la demanda actual de personas calificadas para hacer éstos trabajos es muy superior a la oferta.

   Por lo general se dan cifras de las personas que han quedado desempleadas como resultado de la automatización, pero no de las que carecerían de trabajo de no haber llegado la nueva tecnología.

2. MAYOR SATISFACCION EN EL TRABAJO. Se pueden resolver problemas sumamente complejos por medio de las computadoras en tiempos relativamente breves o, también, dejarle al procesamiento de la máquina las tareas peligrosas, repetitivas o aburridas, liberando así a la mente humana de tareas desagradables y de ésta forma el hombre dispondrá de tiempo libre para concentrarse en aspectos más atractivos de su propia existencia.

b). EFECTOS NEGATIVOS

1. DESEMPLEO. Debido al mejoramiento de la productividad lograda gracias al uso de las computadoras, habrá un considerable despido de mano de obra. Así mismo, a mayor eficiencia que se logre por su uso, puede resultar una mayor supresión de la actividad de algunos trabajadores, es decir, las computadoras reemplazan a las personas, por lo que el trabajador vive con el temor de perder el empleo o sufrir sino una reducción en el salario, si en la periodicidad del aumento de éste por méritos personales. Cuando el empleado cree que ha perdido el control sobre su trabajo, el resultado puede ser, aparte de un decremento en su rendimiento, un sabotaje a la computadora o al sistema.

2. DESCUALIFICACION. El uso generalizado de la computadora acarrea la descualificación de muchos trabajos que hasta ahora eran ejecutados por una mano de obra muy experta, restándole importancia a su quehacer y convirtiendo al trabajador especializado en un simple supervisor, lo cual probablemente signifique la desaparición de su oficio y de su gremio.

3. INADAPTACION. Mientras la computadora eleva la productividad, también incrementa la tensión nerviosa del empleado creando el aburrimiento en el trabajo, minando la lealtad a la empresa y disminuyendo su producción, lo que provoca que éste sienta que sus capacidades y méritos se vean opacados por ésta máquina y empiece a considerarse insignificante y agobiado.

La informatización y trivialidad de las pocas tareas de carácter impersonal y repetitivo que todavía realice el empleado no preparado en la automatización, vendrán acompañadas de nuevos aspectos penosos como el tedio y la monotonía, lo cual le acarreará al trabajador problemas más psicológicos que físicos al tener que vivir el trabajo de una manera distinta a la que ha estado habituado.

4. DESPLAZAMIENTO. El uso de robots controlados por computadoras está acelerando el desplazamiento, pues éstos realizan sin quejarse labores monótonas, sucias y peligrosas. Los problemas que se derivan de los puestos afectados por el desplazamiento son graves, pues se tiende a eliminar a los trabajadores de mayor edad o a reubicarlos en puestos para los que no están preparados; la falta de experiencia y conocimiento sobre los mismos, les ocasiona una pérdida de confianza en sí mismos, aparte del temor a la posibilidad de no tener capacidad para adquirir las habilidades necesarias para desempeñar su nueva actividad, reduciendo así su autoestima, pues empiezan a sentirse no sólo viejos sino también inútiles.

Sobre los efectos que la automatización impone sobre el empleo, Nora y Minc expresan: "La informática permite y acelera el advenimiento de una sociedad de altísima productividad: menos trabajo para una mayor eficacia y unos puestos de trabajo muy diferentes de los que impone la vida industrial. Esta mutación ha empezado ya: fuerte disminución de la mano de obra en los sectores primarios y secundarios, alza de los servicios y, sobre todo, multiplicación de las actitudes en las que la información es la materia prima. La acompañarán un cambio en la estructura de las organizaciones y una mudanza de las actitudes hacia el trabajo (11)".

---

(11) NORA, Simon y MINC, Alain. Op. cit. pp. 175 y 176.

Los efectos de ésta informatización sobre el empleo, modificarán sustancialmente las condiciones de trabajo como la duración de la jornada, los días de descanso y vacaciones, el nivel de remuneración, la cualificación y descualificación de las tareas, entre otras cosas.

Como ya se dijo, el uso de las computadoras está produciendo un gran efecto social influyendo tanto en la vida privada de las personas como en los propios países. A continuación se señalan algunas formas de ésta influencia:

III.3 IMPLICACIONES EN LOS INDIVIDUOS POR EL USO DE LAS COMPUTADORAS

1. DESPERSONALIZACION. En la mayoría de los sistemas basados en las computadoras, la clave que se usa para identificar a un individuo es un número, sucediendo lo mismo a medida que éstos tienen contacto con más sistemas de cómputo y aunque la mayoría entiende que ser tratados como un número da como resultado el trabajo eficiente de la computadora, preferirían que los sistemas los identificara como personas y no como numerales.

   Además, existe el posible peligro de utilizar un identificador universal que consiste en que los registros separados de datos sobre una persona que se han establecido con fines específicos, puedan consolidarse más fácilmente con el uso de un número común y que ésta información combinada se fusione en un gran expediente personal. Esta tendencia a unificar a todos bajo un mismo modelo, puede, naturalmente, dar al individuo un sentimiento de impotencia al relacionarse con organizaciones frías, impersonales y lejanas.

2. PRIVACIA. El público tiene la creencia de que la informática es como un fichaje que atenta contra la vida privada y las libertades. La falta de control en el almacenamiento, la recuperación y la transmisión de los datos, ha permitido que se abuse del legítimo derecho a la privacía, es decir, mantener en privado o en forma confidencial las costumbres o hechos de la vida privada, creencias religiosas o políticas y sentimientos que el individuo no desea hacer públicos.

La sociedad sufriría un gran golpe si ésta parte quedara expuesta, sin embargo, opina Donald H. Sanders en su libro Informática : presente y futuro, "la pérdida de la privacidad es frecuentemente consecuencia de la acción de fuerzas tecnológicas complejas e interrelacionadas que intervienen en una sociedad cuya densidad de población está en aumento. (12)".

3. VIGILANCIA. A través de un sistema de computación o red de información, se puede efectuar una continua vigilancia o crear un clima que restrinja la libertad del individuo.

Esto se puede realizar a través de los sistemas Electrónicos de Transferencia de Fondos, EFT (13). Cuando se utiliza una tarjeta de crédito, se registra además de la naturaleza y monto de la transacción, la información referente a la fecha, hora y lugar en que ésta se realiza, de tal manera que si todas las transacciones de una persona se procesan normalmente por medio de las computadoras que usan los sistemas EFT, es factible la preparación de un registro diario de todo lo que hizo un individuo y en donde lo hizo.

---

(12) SANDERS, H. Donald. Op. cit. p. 554
(13) Supra, pp. 57 y 58.

III.4. IMPLICACIONES DE LOS ESTADOS POR EL USO DE LAS COMPUTADORAS (FLUJO DE DATOS TRANSFRONTERIZOS)

La informática pasó a ser un sector estratégico en un gran número de países conscientes de la especificidad de su materia prima: la información. Aunado a ésto, los satélites convierten en simbólicas a las fronteras que constituyen actualmente las líneas de separación entre los mismos.

Los bancos de datos cambian las condiciones de acceso a la información que guardan y hacen posible las preguntas a distancia, siempre que estén conectados a una red. Aunque dicha información existía antes de crearse éstos, casi siempre estaba dispersa, siendo por ello poco manejable y difícil de usar. La facilidad de acceso es la que crea su necesidad. Dichos bancos de datos suelen ser internacionales y el desarrollo de las transmisiones los hará asequibles desde cualquier punto de la tierra.

Tal facilidad de acceso a los bancos de datos internacionales que permite que otros países se valgan de ellos, ha contribuido a que éstos pierdan interés en construir su propio banco de datos en su territorio nacional. Sobre éste punto, Nora y Minc afirman que "dejar en manos ajenas el cuidado de organizar esa "memoria colectiva" dándose por satisfechos con abrevar en ella, equivale a aceptar una alineación cultural (14)", lo que debemos evitar con la creación de bases de datos con información local y en territorio nacional.

Así como los bancos de datos proporcionan la facilidad de tener acceso a una información, con igual facilidad un organismo público o privado puede procesar un extenso archivo de información sobre hogares de un país en un centro de datos localizado en otro país o continente. Si un estado permite publicar a través de este proceso una gran cantidad de información acerca de sus ciudadanos, se podría no solamente violar el derecho a la privacidad individual, sino comprometer a la seguridad nacional.

---

(14) NORA, Simon y MINC, Alain. Op. cit. p. 114.

Este flujo de datos a través de las fronteras, el cual es definido por la Organización de Naciones Unidas como "la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y recuperación (15)" y por Carlos M. Correa como "la circulación a través de las fronteras nacionales de datos tratados por computadora y/o en medios magnéticos y/o capturados vía satélite que pueden ser consultados, procesados o almacenados (16)", el cual es factible debido a las posibilidades tecnológicas, está considerado como un problema muy grave, al grado de que algunos países están promulgando leyes de protección de datos; postulan la necesidad de una intervención reguladora del Estado mediante recursos legales y técnicos apropiados. En cambio otros, los industrializados, consideran que dichas leyes sería barreras a la transferencia internacional de datos y, por lo mismo, una forma de restricción comercial y un obstáculo al libre intercambio de información cultural y científica, por lo que abogan por la vigencia de un principio de libre circulación de los datos.

Los flujos internacionales de datos se han clasificado atendiendo diferentes criterios:

1. Medios de transmisión:

   - Electrónicos
   - No electrónicos (discos, cintas magnéticas)

2. Tipos de información:

   - Científico - técnica
   - Económica y social
   - Educativa y cultural
   - Comercial y financiera
   - Administrativa
   - Seguridad
   - Sobre las personas

---

(15) TELLEZ Valdés, Julio. Op. cit. p. 78
(16) CORREA M., Carlos. Derecho Informático, Buenos Aires, Ed. Depalma, 1987, p. 48.

3. Función técnico - económica:

- Comunicaciones personales y comerciales
- Transferencia de software
- Acceso a banco de datos
- Procesamiento de datos

4. Naturaleza de la relación:

- Redes cerradas
- Venta de servicios
- Venta o licencia de software
- Transacciones intrafirmas.

En función de la información contenida, las implicaciones positivas o negativas de este flujo de datos más allá de las fronteras nacionales, pueden ser no solamente políticas, sino también sociales, culturales y económicas. A continuación se señalan algunas:

- IMPLICACIONES POSITIVAS.

a). Favorecimiento de la democracia. El libre intercambio de mensajes y opiniones entre los hombres, es esencial para la democracia, de lo contrario se atentaría contra una de las garantías individuales de todo ser humano: la libertad de expresión.

b). Favorecimiento del progreso técnico. La comunicación entre los científicos de todos los países de la tierra favorece la difusión de los conocimientos y técnicas y, por ende; el progreso de cada nación, pues aislada de información tan importante se iría quedando a la zaga con respecto a los estados entre los que fluye un libre intercambio de información.

c). Favorecimiento de la economía. Los organismos nacionales con sede en el extranjero así como la especialización de actividades nacionales, podrían verse seriamente afectadas si en un momento determinado carecieran de la información proveniente de otros países, provocando graves consecuencias a su economía. Sobre este punto, el Dr. Téllez afirma: "Es imposible concebir hoy en día a algún país que goce de una independencia total en el plano económico (17)".

- IMPLICACIONES NEGATIVAS

a). Mal funcionamiento técnico. Existe la posibilidad de que en el flujo de datos transfronterizos se presente alguna falla técnica provocada por una catástrofe natural o por intervención humana, dando lugar a acciones tales como el sabotaje o el terrorismo, con lo cual se infringe la soberanía de la nación afectada.

b). Amenaza a la identidad cultural. El libre fluir de la información a través de las fronteras nacionales trae consigo una forma de ser, de hablar, de pensar, y de vestir diferentes, sólo por mencionar algunas, lo que podría provocar una pérdida de la identidad nacional. Nora y Minc expresan: "la telemática, lenta pero seguramente, empezará a pesar sobre los elementos principales de la cultura: el lenguaje, en sus relaciones con el individuo e incluso en su función social; el saber como prolongación de las memorias colectivas y como instrumento de igualización o de discriminación de los grupos sociales (18)".

---

(17) TELLEZ Valdés, Julio. Op. cit. p. 80.
(18) NORA, Simon y MINC, Alain. OP. cit. p. 179.

c). Dependencia tecnológica exagerada. Las compañías internacionales dedicadas a la manufactura de tecnología con el propósito de ampliar sus ventas, crean necesidades en países, por lo regular en desarrollo, para luego satisfacerlas mediante la venta de tecnología obsoleta que a la postre les resulta onerosa e inútil.

Acerca de este tema, el DR. Téllez afirma que el flujo de datos transfronterizos, dada su falta de control jurídico, "puede atentar contra la soberanía de los estados y no sólo desde el aspecto político, sino también desde el punto de vista social, cultural y económico (19)".

Sin embargo, a pesar de los perjuicios que acarrean las nuevas tecnologías, son más y mejores los beneficios que aportan, por lo que éstas acaban imponiendose y dan por resultado cambios irrevocables, positivos o negativos, que es imposible detener. Nora y Minc dicen al respecto: "Ninguna tecnología, por innovadora que sea, acarrea a la larga consecuencias fatales. Sus efectos son dominados por la evolución de la sociedad más de lo que la constrinen (20)".

---

(19) TELLEZ Valdés, Julio. Op. cit. p. 82.
(20) NORA, Simon y MINC, Alain. Op. cit. p. 25.

CAPITULO III

DELITOS INFORMATICOS

I. GENERALIDADES

Asi como la tecnologia informática ha traido grandes beneficios a la sociedad, también ha acarreado una nueva forma de criminalidad que se encuadra dentro de los ilicitos conocidos como "delitos de cuello blanco".

Nos referimos al que hemos llamado **"Abuso Informático"**, cuya comisión, aparte de estar incrementándose, se está perfeccionando casi en la misma proporción en que lo hacen los componentes electrónicos.

El perfeccionamiento de la tecnologia informática hace que cada vez sean menos complejos los componentes de las computadoras y, por lo mismo, más accesibles. Tal desarrollo, la difusión de estas máquinas, el creciente acceso a computadoras personales y baratas y la proliferación de centrales de cómputo a las que es factible tener acceso a través de lineas telefónicas, ha incrementado la comisión de nuevas figuras criminales en las que existe una victima que sufre un daño y un autor que intencionalmente obtiene un provecho, por lo que los efectos de la informática sobre el funcionamiento de la sociedad serán decisivos y pueden ser temibles.

Como estas conductas antijurídicas se realizan con y mediante la computadora, Simon Nora y Alain Minc opinan que "si la sociedad es lo suficientemente móvil como para organizar la lucha contra una eventual 'nueva delincuencia' permitida por las técnicas del ordenador, el peligro no radica en la transparencia. Se oculta en otra parte: en la fragilidad de la sociedad entera (1)", refiriéndose a la vulnerabilidad accidental o deliberada en que queda la sociedad que cada vez tiende a multiplicar centros de cómputo en donde la informática es demasiado centralizada, demasiado estructurada y demasiado jerarquizada.

A pesar de que las computadoras son el origen de nuevas figuras delictivas, debe tenerse presente que estas máquinas no hacen el mal, pues son objetos inanimados; lo comete quien las utiliza: El hombre. Al respecto, la Dra. Lima dice que "la tecnología electrónica y sus inventos serán tan honorables y deshonestos como la persona que los utilice (2)".

II. DEFINICION

Considerando que ésta es una nueva forma de delinquir, todavía no ha sido posible que los pocos autores que han tratado acerca del tema coincidan sobre una definición única. A continuación se mencionan algunas:

Carlos Sarzana define a los delitos electrónicos como:

"Cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo (3)".

Por su parte, Donn B. Parker los denomina "Abusos de Computadora" y los define como:

"Cualquier acto intencional asociado de cualquier manera con las

---

(1) NORA, Simon y MINC, Alain. La Informatización de la Sociedad, México, Fondo de Cultura Económica, 1981, p. 97.

(2) LIMA, Ma. de la Luz. Delitos Electrónicos, México, Revista Criminalia No. 50, 1984, p. 34.

(3) Citado por TELLEZ Valdés, Julio. Derecho Informático, México, Universidad Nacional Autónoma de México, 1987, p. 105.

computadoras, donde una víctima sufrió o pudo haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia (4)".

A su vez Klaus Tiedemann expresa que:

"Son los delitos que protegen cualquier acción ilegal en el que la computadora es el instrumento o el objeto del delito (5)".

El Dr. Julio Téllez Valdés señala que para hablar de delito, por lo menos en México, es necesario que las conductas que se describen estén contempladas en textos jurídico-penales y en nuestro país no han sido tipificados. No obstante, este autor los denomina como "Delitos Informáticos" y nos proporciona dos conceptos:

"Concepto Atípico: Actitudes ilícitas en que se tiene a las computadoras como instrumento o fin".

"Concepto Típico: Conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (6)".

La Dra. María de la Luz Lima dice que el "Delito por computadora" es:

"Cualquier acto ilícito penal en el que las computadoras, su técnica y funciones desempeñan un papel ya sea como método, como medio o como fin (7)".

---

(4) PARKER B., Donn. Fighting Computer Crime, New York, Charles Scribner's Sons, 1983, p. 16.

(5) Citado por ROJAS, Pérez Palacios Alfonso. Delitos de Cuello Blanco, México, Joaquín Porrúa, S.A., 1986, p. 78.

(6) TELLEZ Valdés, Julio. Op. cit. p. 105.

(7) LIMA, Ma. de la Luz. Op. cit. p. 29.

Para el jurista argentino Carlos M. Correa, el delito informático es:

"Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos (8)".

Considerando tanto las definiciones mencionadas como las funciones que se pueden realizar mediante la computadora, nosotros proponemos la siguiente denominación:

"Abuso Informático", el cual consistiría en:

Examinar, modificar, alterar, interceptar, transferir, borrar, interferir, introducir y extraer todo tipo de información contenida en la Unidad Central de Procesamiento de cualquier computadora.

A continuación se justifica el uso de cada uno de los términos empleados en esta definición:

ABUSO: Con esta palabra se define un uso indebido o mal uso que se hace, en este caso, de la información.

INFORMATICO: Este término es de reciente acunación, creado precisamente para definir algo nuevo. Es un neologismo derivado de los vocablos información y automatización, es decir, información automatizada, siendo ésta el bien a tutelar.

EXAMINAR: Es mirar atentamente. Tal atención se requiere al inquirir sobre información específica.

---

(8) CORREA M., Carlos. Derecho Informático, Buenos Aires, Ed. Depalma, 1987, pp. 295 y 296.

MODIFICAR: Significa cambiar la forma. Una persona malintencionada bien puede efectuar cambios en la información contenida en la Unidad Central de Procesamiento (UCP) de una computadora ajena, dándole una forma diferente a la que tiene.

ALTERAR: Es cambiar la esencia. Con propósitos perniciosos, una persona puede accesarse a la UCP de una computadora perteneciente a otra y variar la información en cuanto a su fondo.

INTERCEPTAR: Quiere decir apoderarse de una cosa que se envía a otro. En este caso, lo que es objeto de envío y de 'apoderamiento' es la información sobre la cual existe un derecho de propiedad. A este respecto, Carlos M. Correa afirma que "es un 'derecho frágil' debido a la 'inmaterialidad' de su objeto y a la facilidad con que puede ser vulnerado (9)", sin embargo, sigue siendo un derecho para su legítimo titular.

TRANSFERIR: Significa pasar de un lugar a otro y ésto se puede realizar con la información contenida en la UCP de otra computadora, no sólo en la misma ciudad, sino, como ya se ha mencionado, a través de las fronteras.

BORRAR: Quiere decir hacer desaparecer lo escrito. A través de una terminal localizada tanto cerca como lejos de la UCP de una computadora ajena, se puede destruir toda la información que ésta contenga con los consecuentes perjuicios para su legítimo poseedor.

INTERFERIR: Significa producir perturbaciones (entropía), lo cual puede llevarse a cabo en la emisión o recepción de la información contenida en la UCP de una computadora con el propósito de que no se comprenda ésta pues las interferencias la harían incoherente.

INTRODUCIR: Es hacer entrar. Mediante ciertos dispositivos es

---

(9) CORREA M., Carlos. Op. cit. p. 288.

posible accesarse a la UCP de otra computadora con la intención de incluir o intercalar datos que pueden afectar a la información contenida en ésta.

EXTRAER: Quiere decir hacer salir. Al igual que es posible introducir datos en una UCP, se pueden sacar a través de los diferentes dispositivos de salida ya mencionados (10).

INFORMACION: "Son todos los sonidos, imágenes, documentos, datos o mensajes de cualquier naturaleza comunicables a otro por cualquier medio (11)".

UNIDAD CENTRAL DE PROCESAMIENTO: "Unidad de una computadora compuesta por un conjunto de medios técnicos capaces de almacenar la información y procesar los datos de acuerdo con las instrucciones senaladas en el programa (12)".

COMPUTADORA: "Complejo de medios técnicos capaces de procesar automáticamente ciertos datos de entrada y obtener resultados como información de salida (13)".

Tomando en consideración que la definición es de naturaleza compleja porque es complejo el producto en cuestión y con base en el desglose anterior, proponemos como denominación y definición para este nuevo delito los siguientes:

Comete el delito de **abuso informático** el que examine, modifique, altere, intercepte, transfiera, borre, interfiera, introduzca o extraiga todo tipo de información contenida en la Unidad Central de Procesamiento de cualquier computadora, sino cuenta con el permiso de la persona legalmente autorizada para disponer de ella.

---

(10) Supra. Dispositivos de salida pp. 40 a 42.

(11) CORREA M., Carlos. Op. cit. p. 288.

(12) DIAZ Llorca, Carlos. Introducción a la Computación, La Habana, Edit. Pueblo y Educación, 1980 p. 49.

(13) Ibidem, p. 50.

III. CLASIFICACION

La Dra. Lima los clasifica de la siguiente manera:

- COMO METODO:

Para llegar al resultado ilícito usan algún método electrónico. La máquina o instrumento mismo realiza la infracción penal dirigido por su autor como:

a). Falsificar una tarjeta de crédito. Se programa que por cada tarjeta se imprima un duplicado que se se usará ilícitamente.

b). Defraudar a una compañía alterando activos, pasivos, etc.

c). Fraude con técnica salami que consiste en extraer pequeñas cantidades de dinero de miles de cuentas bancarias; los afectados generalmente no lo perciben o se conforman con hacer sólo una reclamación intrascendente.

- COMO MEDIO:

Son las conductas criminógenas que para realizar un delito se valen de un objeto electrónico como medio o símbolo, como los siguientes:

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

b). Lectura de ficheros judiciales para extorsionar.

c). Lectura de datos confidenciales para chantajear (14).

---

(14) LIMA, Ma. de la Luz. Op. cit. p. 29.

El Dr. Julio Téllez Valdés integra en una sola las dos clasificaciones anteriores. Ambos autores coinciden en la siguiente:

- COMO FIN:

Son las conductas criminógenas que van dirigidas en contra de la entidad física del objeto o máquina electrónica o de su material. El fin de la conducta es dañar al objeto, máquina o su material.

a). Destrucción de un programa.

b). Dañar una memoria.

c). Quemar la computadora (15).

Respecto a este orden, nosotros consideramos como el Dr. Téllez que la primera englobaría la clasificación como método y como medio, pues mediante el manejo de la máquina y con la máquina misma, se lleva a cabo la conducta antijurídica.

Por su parte, Carlos M. Correa clasifica los delitos informáticos en las siguientes categorías:

a). Fraude por manipulaciones de una computadora contra un sistema de procesamiento de datos.

b). Espionaje informático y robo de software.

c). Sabotaje informático.

d). Robo de servicios.

---

(15) TELLEZ Valdés, Julio. Op. cit. pp. 106 y 107.

e). Acceso no autorizado a sistemas de procesamiento de datos.

f). Ofensas tradicionales en los negocios asiatidos por computadora (16).

En el "Reporte del Crimen por Computadora" realizado en Junio de 1984 por la Sección de Justicia Criminal de la American Bar Association, se dividió el concepto en dos partes:

a). Actividades criminales dirigidas contra las computadoras: Estas máquinas son las víctimas de la ofensa (sabotaje y vandalismo).

b). Actividades criminales en las cuales las computadoras son utilizadas como instrumentos para perpetrar el crimen: Las computadoras facilitan la realización de la ofensa (robo, fraude, peculado) [17].

IV. CARACTERISTICAS DEL DELITO INFORMATICO

Este ilícito presenta una serie de peculiaridades que lo separan de las demás conductas punibles y son precisamente esas características las que lo hacen diferente:

1. La conducta de este delito es en contra de la propiedad, donde el bien jurídico tutelado es la información, bien intangible susceptible de apropiación y con un valor patrimonial inherente, entendiendo a la información como todo mensaje comunicable a otro por cualquier medio.

2. Son delitos de cuello blanco. Edwin Sutherland, criminólogo estadounidense en 1943 utilizó el término "White Collar

---

(16) CORREA M., Carlos. Op. cit. p. 296.

(17) ROSTOKER, Michael y RINES, Robert. Computer Jurisprudence. Legal Responses to the Information Revolution, New York, Oceana Publications, Inc., 1986, p. 334.

Crimen" definiéndolo como "aquel que es cometido por una persona de alto status socioeconómico en el transcurso de su ocupación (18)", es decir, se realizan por sujetos con preparación especial y, generalmente, cuando se encuentran trabajando. Tal es el caso del delito informático.

3. El daño económico que ocasiona uno solo de estos delitos supera en exceso la cuantía de todos los robos y fraudes convencionales cometidos en un año. Sus consecuencias económicas son generalmente considerables.

4. Son acciones ocupacionales, por lo tanto, se cometen en el ejercicio empresarial o gestión económica y realizados durante el despacho o profesión que desarrollan.

5. Los límites geográficos han sido anulados, de tal suerte que con solo una terminal de computadora es posible perpetrar por teléfono un ilícito al otro lado del mundo. El delincuente que realiza un crimen por computadora no tiene la necesidad de estar en el lugar de los hechos.

6. El tiempo utilizado en esta tarea delictiva es tan raudo como lo es el usado normalmente como medida de las computadoras, es decir, el nanosegundo que equivale a una billonésima parte de un segundo. La velocidad para cometer este crimen es impactante.

7. Presentan grandes dificultades para su comprobación. Debido al poco tiempo invertido en su comisión y al largo período que transcurre para su detección, el criminal cuenta con tiempo más que suficiente para disponer de los objetos

---

(18) ROJAS Pérez Palacios, Alfonso, Op. cit. p. 7.

materiales que adquirió, por lo que la mayoría de las veces estos delitos quedan impunes, pues aunque se descubran, es difícil comprobar la evidencia o formular la presunción delictiva.

8. Existe un riesgo psíquico reducido para el autor del delito, pues justifican su comportamiento argumentando que éste no es muy grave pues lo cometen en contra de una máquina y no de una persona.

9. Particularmente en esta conducta delictiva falta la percepción de peligrosidad general que alarma en los delitos de violencia, pues en la mayoría de los casos, éste se ejecuta precisamente sin violencia.

10. Su preparación es muy singular debido a la creatividad y sofisticación técnica necesaria para su realización.

11. La personalidad del delincuente es muy original. Este ilícito, como el robo o el homicidio, no puede ser ejecutado por cualquier persona, sino que para su comisión, el delincuente necesita reunir ciertas características específicas como, por ejemplo, una inteligencia superior a la normal y una preparación especial que no se encuentran al alcance de la mayoría de la población.

V. PERSONALIDAD DEL DELINCUENTE

Como ya se ha dicho en múltiples ocasiones, este tipo de delito, al igual que la tecnología que se utiliza para su comisión y la persona que lo realiza, son nuevos en el ámbito criminal, por lo mismo, no se ajustan a la imagen estereotipada del delincuente (pobre, inculto, adicto a las drogas, etc.). No obstante que son muchos los casos, han sido pocas las denuncias precisamente por su

falta de tipificación, sin embargo, con los datos empíricos existentes, se puede realizar un perfil del delincuente:

a). Son individuos que se caracterizan por no tener antecedentes penales y por haber desarrollado un modo de vida aparentemente adaptado sin una marcada agresividad, con una vida laboral y familiar estable.

b). El delincuente tiene un aspecto y un carácter agradables que le son necesarios para conquistar la confianza indispensable para una más fácil realización de su delito.

c). Es despierto, impaciente, muy motivado, audaz y aventurero; entre sus rasgos más acentuados se encuentra una imaginación exhuberante, un sentido exagerado de la propia personalidad y una gran codicia.

d). Este tipo de delincuente es instruido y posee una inteligencia superior a la normal, por lo que para él representa un reto desactivar todas las medidas de seguridad que se va encontrando en el trayecto hacia la comisión del ilícito. Cuanto más inteligente y mal intencionado sea el individuo, tanto mayor y sutil al daño que pueda ocasionar.

e). Por su comportamiento seguro, por la facilidad y naturalidad con que se expresa, por la forma en que viste, proyecta una imagen que representa un status social elevado. Esta imagen de solvencia que exhibe tiene el efecto de que se rechazen las sospechas hacia él.

f). A pesar de que este nuevo crimen ha proliferado, su comisión se hace posible a nivel de los empleados. Los nuevos sistemas de información son manejados por profesionales especialmente

capacitados para ello, personas por lo general muy bien preparadas: Presidentes de las corporaciones, ingenieros en sistemas, programadores, analistas, etc.

Aunque el universo del criminal se reduce, pues no cualquiera puede cometer un delito informático ya que se requieren determinadas condiciones tales como la preparación técnica, el acceso a los sistemas y el espíritu de aventura que representa el reto de enfrentarse a los dispositivos de seguridad de los programas de computación, existe un mayor número de personas que ha recibido ahora la capacitación requerida para programar, penetrar y manipular los sistemas de computación. Además, por las ventajas que representa en cuanto a la cuantía que se puede obtener y a su impunidad por falta de tipificación, cada vez hay una mayor proliferación de expertos en informática de alto nivel.

Carlos Sarzana afirma que "la criminalidad de computadoras es cometida por la élite de la delincuencia (19)".

Dentro de esta nueva delincuencia existen diferentes clases de individuos, tales como:

1. AMATEUR: Son gente ordinaria colocada en puestos de confianza o con una experiencia obtenida por el manejo constante del equipo de computación que se encuentra en dificultades económicas por apuestas, drogas, etc. para la solución de sus problemas utiliza sus capacidades especiales violando la confianza en ellos depositada. Cabe aclarar que estos individuos no son necesariamente inteligentes, pero si expertos en las funciones propias de sus labores.

2. PROFESIONALES: Son personas sumamente inteligentes, cuentan

---

(19) LIMA, Ma. de la Luz. Op. cit. p. 35.

con una preparación especial y generalmente están colocadas en puestos de alta dirección dentro de las corporaciones, como vicepresidentes, directores o gerentes. Precisamente por el puesto que desempenan, se dan cuenta del valor de la información confidencial que manejan, por lo que conjuntando su inteligencia, experiencia en la operación de los sistemas de información y alta jerarquía, para ellos es relativamente fácil transferir, alterar o extraer, entre otras funciones, información contenida en la Unidad Central de Procesamiento de la computadora de la organización en la que laboran, obteniendo a cambio un enorme beneficio.

3. EXPLORADORES DE SISTEMAS: por lo regular, son estudiantes de universidades que nunca han sido arrestados; no son extremistas ni terroristas; tampoco son vándalos o saboteadores. Son intrusos atrevidos que no buscan destruir nada ni tampoco les interesa la información contenida en los sistemas a los que se accesan; lo único que pretenden es traspasar la tecnología, demostrar su superioridad sobre los complejos controles de seguridad que guardan a estos sistemas y que su hazana sea reconocida. Su intrusión a los sistemas es el reto; que su logro se haga público reconociendo su inteligencia suprema, es su recompensa.

4. PARTIDARIOS EXTREMISTAS: Son personas que se dedican a luchar por los derechos humanos y por sus ideales políticos, económicos y religiosos. Por lo regular, están involucrados en actividades criminales y son protegidos por pequenos grupos rebeldes. Se les conoce como extremistas o terroristas, pero son diferentes a las corporaciones criminales organizadas, pues ellos se dedican a "cambiar" positivamente a la sociedad.

Este cambio implica el ataque a las multinacionales e identifican a las computadoras como instrumentos de éstas debido al monopolio que ejercen en los sistemas computacionales. Afirman que el sector electrónico es el sector estratégico del avance del capitalismo, pues no sólo exportan su alta tecnología, sino también su ideología, idioma y cultura y a través de las redes de computación realizan un espionaje total sobre las personas.

5. ORGANIZACIONES CRIMINALES: La mafia es el prototipo del crimen organizado. Estas, aparte de utilizar las computadoras en sus negocios a gran escala como son sus operaciones financieras con los bancos o con los corredores de apuestas y de drogas, las utilizan para cometer otros delitos en contra de organizaciones que cuentan con sistemas de cómputo como herramienta de trabajo. El crimen organizado está utilizando la computadora como una arma muy poderosa y efectiva.

En cuanto a las víctimas, el universo se amplía, pues la dependencia de la nueva tecnología nos hace más susceptibles de convertirnos en víctimas.

Las víctimas más frecuentes de este tipo de delito son el sector bancario y económico. Sin embargo, al contrario de lo que cualquier persona denunciaría, a estas instituciones no les preocupan dichas infracciones, pues cuentan con partidas presupuestales previamente creadas precisamente para absorber tales desfalcos, por lo que no denuncian dichas conductas ilícitas.

Sin embargo, no todas las personas afectadas por estos delitos cuentan con la misma capacidad de absorción de semejantes pérdidas, no obstante, al no estar tipificada esta acción ilícita, el sujeto pasivo queda imposibilitado de exigir justicia y que se castigue al delincuente, ya que como están las cosas actualmente, éste, a pesar de saber quien se está beneficiando en su perjuicio y como lo está haciendo, queda impotente de activar el órgano de la justicia, pues no hay delito que perseguir por la propia ausencia de tipo (nullum crimen sine lege) y el sujeto activo queda en libertad y en posibilidad de continuar delinquiendo.

VI. DELITOS INFORMATICOS MAS FRECUENTES

Las medidas de seguridad para proteger la confidencialidad e integridad de los programas y los datos almacenados en línea por los usuarios, generalmente no resisten la habilidad de los intrusos que intentan penetrar la red. Entre los ilícitos más frecuentes cometidos con y mediante la computadora, se encuentra el siguiente:

El uso de ciertas prácticas dudosas de procesamiento de datos. Muchas organizaciones capturan rutinariamente datos sobre los ciudadanos, datos que son procesados y almacenados por computadora, los cuales pueden ser recopilados por quienes no tienen una razón justificada para hacerlo, dando origen a un abuso al derecho de privacía.

La falta de control en la seguridad de los datos de un sistema de cómputo ha permitido que no sólo las personas no autorizadas, sino que también las facultadas para ello pero mal intencionadas, tengan acceso accidental o intencionalmente, a información confidencial de naturaleza privada, lo que posibilita que se abuse del legítimo derecho a la privacía, como el de mantener en privado los hechos que las personas no desean hacer públicos.

También les ha traído consecuencias indeseables como pérdidas económicas, un acoso constante por parte de vendedores, aseguradores, etc., o aun a que se ejerza presión sobre sus personas para obligarlos a hacer cosas que de otra forma no hubieran hecho.

Debe tenerse presente que la capacidad de tratamiento de la información con la informática y las telecomunicaciones actualmente posibilitan en mayor medida la adquisición de datos sobre los particulares, su intercambio, su procesamiento y su difusión de manera relevante, no sólo en el país, sino también allende las fronteras nacionales.

Los registros guardados en grandes bases de datos integrados son más precisos y más completos, lo que los hace más atractivos para quienes desean descubrir hechos confidenciales. Los datos registrados aparentemente son inofensivos, pero al correlacionarse con otros obtenidos de fuentes diferentes y en distintos momentos, revelan información potencialmente perjudicial acerca de las personas.

Los registros más codiciados por este tipo de personas mal intencionadas son los referentes a:

- Información económica y financiera
- Información referente a las condiciones de salud
- Información sobre la vida personal o familiar
- Información política y relativa a la seguridad

El avance de la tecnología hace necesaria la creación de nuevas reglas de Derecho que tutelen situaciones actuales como son los derechos y libertades fundamentales que se ven amenazadas por la informática, la cual debilita la capacidad de dominio de las personas sobre los datos que les conciernen.

Debido precisamente al mal manejo de los bancos de datos personales en el que se ha acentuado la posibilidad de afectar el derecho a la privacidad como consecuencia de la divulgación a terceros de datos sobre su vida personal o familiar, varios países han establecido regulaciones, inclusive a nivel constitucional, para impedir que se afecten negativamente la libertad y los derechos humanos.

Tales países han elaborado sus regulaciones conforme a los siguientes principios fundamentales:

1. PRINCIPIO DE LA JUSTIFICACION SOCIAL: La recolección de datos deberá tener un propósito general y usos específicos socialmente aceptables.

2. PRINCIPIO DE LA LIMITACION DE LA RECOLECCION: Los datos deberán ser recolectados por medios lícitos, es decir, con conocimiento y consentimiento del sujeto de los datos o con autorización legal y deberán limitarse al mínimo necesario para alcanzar el fin perseguido por la recolección.

3. PRINCIPIO DE LA CALIDAD O FIDELIDAD DE LA INFORMACION: Los datos personales que se recolecten y conserven deberán ser exactos, completos y actuales.

4. PRINCIPIO DE LA ESPECIFICACION DEL PROPOSITO O LA FINALIDAD: En el momento en que se recolecten los datos, deben estar especificados los fines para los cuales son recolectados, no pudiendo ser usados para fines diferentes.

5. PRINCIPIO DE LA CONFIDENCIALIDAD: El acceso a los datos por parte de terceros sólo podrá ser llevado a cabo con consentimiento del sujeto de los datos o con autorización legal.

6. PRINCIPIO DE SALVAGUARDA DE LA SEGURIDAD: Obligación de la entidad responsable del registro de datos personales de adoptar las medidas de seguridad adecuadas para protegerlos contra posibles pérdidas, destrucciones o acceso no autorizado.

7. PRINCIPIO DE LA POLITICA DE APERTURA: Garantiza la transparencia de la acción de la administración pública y privada con relación a los procedimientos, desarrollo y prácticas concernientes al procesamiento de datos personales. Esta transparencia queda asegurada por el conocimiento por parte del público de la existencia, fines, usos y métodos de operación de los registros de datos personales.

8. PRINCIPIO DE LA LIMITACION EN EL TIEMPO: Los datos no deben conservarse más allá del tiempo requerido para alcanzar los fines para los cuales fueron recolectados.

9. PRINCIPIO DEL CONTROL: Existencia de un organismo de control responsable de la efectividad de los principios contenidos en la legislación.

10. PRINCIPIO DE LA PARTICIPACION INDIVIDUAL: Consagra el derecho de acceso a los datos, que se concede al individuo, el cual comprende el derecho a:

    a). Obtener información de la entidad responsable de los datos acerca de la existencia de datos que le conciernen.

    b). Ser informado dentro de un tiempo razonable y de manera comprensible.

    c). Oponerse a cualquier dato que le concierna y a que esa oposición quede registrada.

    d). Obtener que los datos relativos a su persona, en caso de prosperar su oposición, sean suprimidos, rectificados o completados.

    e). Ser informado de las razones por las cuales se deniega su derecho de acceso o éste no se le concede en lugar, tiempo y forma razonables.

    f). Oponerse a toda negativa a darle las razones mencionadas precedentemente.

Aunque México todavía no alcanza un grado de informatización preocupante, creemos que a manera de prevención, sería favorable legislar en materia de datos personales con disposiciones relativas al Flujo de Datos Transfronterizos de esta misma índole, teniendo por objeto la protección de todos los derechos y libertades fundamentales, tomando como pauta los principios señalados.

VII. MEDIDAS PREVENTIVAS

La Sociedad Americana para la Seguridad Industrial (ASIS) ha expedido un catálogo de recomendaciones específicas para mejorar la seguridad de las computadoras. Algunas de ellas son:

1. "Separación de conocimiento" a través de grados de responsabilidad, rotación de trabajos, incomunicación física, acceso controlado, cortes de fin de página e interrupciones.

2. Instrucciones de programas escritos con amenazas de monitoreo y pruebas de auditoría integradas.

3. Contabilidad cuidadosa de todos los documentos introducidos.

4. Cambios periódicos en códigos y claves de acceso; y

5. Empleo de criptografía en la transmisión de datos (20).

Por lo regular, en las compañías se han tomado ciertas medidas para prevenir el mal uso tanto de la máquina como entidad física como de la información que ésta conserva. A continuación se señalan algunas de ellas:

1. Protección física del recinto donde se encuentran las computadoras. Sin embargo, esta medida parece producir el efecto contrario, pues el típico centro de computación de algunas empresas presenta una especie de invitación al individuo con inclinación al mal uso de ellas, ya que precisamente por estar tan aisladas del resto de las oficinas y por lo regular, sino solas con poco personal, es relativamente fácil el acceso a ellas. Además, hay que considerarse que para tener acceso a la información, puede hacerse desde el lugar en que se encuentra la computadora o desde una terminal lejana.

   Consideramos que esta medida no es efectiva, pues el daño que puede causar un visitante ocasional es mínimo comparado con el que podría desatar un miembro bien informado y mal intencionado de la propia compañía.

2. Como medida preventiva de carácter administrativo se encuentra la celebración de contratos especiales de trabajo con los empleados encargados del manejo de las máquinas en los que se precisen funciones específicas, información a controlar y acciones consideradas como faltas.

   Respecto a esta medida, creemos que el contrato, el cual se refiere a elementos objetivos, aunque contenga una cláusula penal, no puede en y por sí mismo prevenir la comisión de

---

(20) ROSTOKER, Michael y RINES, Robert. Op. cit. p. 355.

ilícitos por parte de los empleados informáticos desleales, frustrados o agobiados auxiliados con el uso de la computadora. El contrato no abarca elementos tan subjetivos como la ética de los contratados.

Por lo tanto, en caso de presentarse la violación a su clausulado, aparte de proceder la rescisión de la relación de trabajo conforme a la Fracción IX del Artículo 47 de la Ley Federal del Trabajo que se transcribe a continuación, se puede ejercitar la acción penal:

"Art. 47.- Son causas de rescisión de la relación de trabajo sin responsabilidad para el patrón:

"IX. Revelar el trabajador los secretos de fabricación o dar a conocer asuntos de carácter reservado con perjuicio de la empresa."

Ya que tocamos el tema laboral, cabe hacer mención que también la Ley Federal del Trabajo, tal vez completa en su momento, carece en la actualidad de disposiciones que regulen las situaciones recientes de carácter laboral originadas con motivo de la nueva tecnología tanto en lo que se refiere a condiciones de trabajo como a los riesgos y enfermedades derivados de éste.

Consideramos que así como el Derecho respondió ante las necesidades sociales imperantes durante la Revolución Industrial creando figuras jurídicas que solucionaran los problemas que ésta conllevó, es menester que ahora se enfrente al reto que le presenta la Revolución Informática creando una nueva legislación que no sólo comprenda la situación actual, sino, de ser posible, prevea las consecuencias de la informatización sobre el trabajo.
Dentro de los aspectos que para la nueva legislación sería conveniente contemplar, se encuentran, entre otros, los siguientes:

- Los empleados informáticos laboran en lugares adaptados a temperaturas de entre 10 y 12 grados C., lo que es adecuado para las computadoras, pero no para el hombre y, menos aún cuando tienen que salir de sus áreas de trabajo, enfrentándose bruscamente a otro clima, con el consecuente perjuicio para su salud.

- También se debe tener presente el largo periodo en que estos empleados se encuentran ante la pantalla de la terminal de computadora observando con la vista fija letras muy pequeñas aparentemente inmóviles (tienen una vibración casi imperceptible) y en colores verde óptico, ambar o blanco y negro, luminosidad que es lesiva para sus ojos.

- Aparte de los transtornos físicos que estas condiciones les pueden ocasionar, se encuentran también las perturbaciones de carácter psicológico a los que se hacen vulnerables después de permanecer grandes interválos en contacto con una máquina fría e impersonal que los hace sentir opacados, insignificantes y agobiados u homo faber; así como la tensión con la que laboran, sobre todo cuando "se cae el sistema", es decir, cuando se detiene el procesamiento y ya no se realiza ninguna operación hasta en tanto no se corrija la falla que le dio origen.

Dentro de las condiciones de trabajo convendría revisar las disposiciones relativas a jornadas de trabajo, vacaciones y días de descanso:

- Jornada: Como consecuencia del uso de la computadora en el trabajo, éste se realiza no sólo más eficazmente, sino de manera más rápida, lo que podría dar lugar a jornadas de trabajo más cortas.

En este rubro también podrían considerarse descansos intermedios en el desempeño de las labores, recesos necesarios para el trabajador informático dadas las condiciones en las que labora y que ya fueron senaladas.

- Vacaciones: Debido al desgaste físico y especialmente mental que sufre el empleado informático en el desarrollo de sus actividades por los factores arriba apuntados, es menester que para una adecuada recuperación de tales aptitudes se les otorguen más días de vacaciones y en periodos menos largos que los actualmente contemplados por la Ley Federal del Trabajo, así como días de descanso adicionales.

3. Dentro de las medidas preventivas de orden técnico, está el cifrado o la criptografía para encubrir la información de tal forma que si ésta es interceptada, no será comprensible para quien la ha obtenido de manera inapropiada.

Esta medida resulta bastante onerosa para la corporación que la utiliza y las más de las veces es ineficaz, pues debe tenerse presente que la persona que llega a la información tuvo que desactivar varios sistemas de seguridad pasando desapercibido, por lo tanto, es lo suficientemente inteligente como para poder descifrarla.

Otra de las medidas preventivas de tipo técnico que se han propuesto para evitar que se tenga acceso a la información contenida en las computadoras, está la de leer las huellas de las personas que utilizan la máquina y si no es una de las autorizadas, marcar sus dedos con una sustancia morada y suspender el servicio. Esta marca permite más tarde detectar al sujeto.

Como creemos que esta medida sólo es aplicable cuando se utiliza la UCP de una computadora por medio de una terminal cercana a ésta y perteneciente al mismo propietario, carece de efectividad para la persona que tiene acceso a la misma UCP pero desde una terminal lejana e independiente del sistema de cómputo al cual se introduce.

En vista de lo anterior y como asistencia técnica al Derecho, estamos planteando la idea de que para evitar este tipo de delitos informáticos, se haga obligatoria la utilización de un dactiloscopio integrado a las computadoras complementado con un programa de identificación de huellas digitales, aditamentos que serían parte de su hardware para que sólo tengan acceso a la información contenida en las UCP de las computadoras las personas que estén debidamente autorizadas mediante el previo registro de sus huellas y su posterior verificación. De esta forma, si la identificación es positiva, la computadora permitiría el acceso a la información requerida; en caso contrario, automáticamente la máquina suspende la penetración a su memoria.

4. Como medida preventiva de tipo social, se propone la educación de la población respecto a los usos y abusos que se pueden llevar a cabo con las computadoras y las consecuencias de cualquier acción con y contra éstas, educación que se debe impartir desde la primaria, pues los niños en edad escolar ya tienen contacto con estas máquinas y están creciendo junto con el desarrollo de las computadoras, lo que les ofrece facilidades para su uso o abuso. La computadora es una herramienta muy poderosa y el poder debe estar siempre acompañado de responsabilidad.

5. Nosotros consideramos que de nada sirve que las computadoras y la información confidencial que éstas almacenan estén supuestamente protegidas contra daño o penetración o contra la diseminación de dicha información ya sea de manera accidental o maliciosa, si continúan siendo falibles y al no existir tipificación expresa que sancione tal conducta antijurídica, por lo mismo, el que la comete queda impune de acuerdo al principio "nulla poena sine lege".

Por lo tanto, ante la incapacidad para resguardar los sistemas de información, las medidas preventivas de tipo jurídico que por su carácter punitivo funcionarían como correctivas que se proponen, son las siguientes:

- La tipificación del delito como delito nuevo que es, ya que hasta la fecha se vienen aplicando por analogía, aunque la Constitución expresamente lo prohibe, el robo o el fraude y esta nueva conducta antijurídica no se adecua cabalmente a dichas figuras.

- Obligar a quien lo sufre a denunciar el delito, pues generalmente no se efectúa porque las compañías afectadas que en la mayoría de los casos son bancos o empresas financieras, temen que de divulgarse éstos, acarrearían su desprestigio y generarían la desconfianza de sus clientes

- Para que la integración del cuerpo del delito se efectúe eficazmente y el proceso correspondiente sea justo, es necesario que todas las personas implicadas en dichas tareas como los agentes del ministerio público, jueces, abogados, etc., cuenten con los conocimientos elementales sobre el uso de la computadora y que en la realización de un peritaje jurídico - informático intervengan expertos en ambas materias.

De lo anteriormente expuesto, concluímos que para la prevención del abuso informático, como lo hemos denominado, se requiere:

1. Instruir al público acerca de los usos, abusos y consecuencias que se pueden realizar con las computadoras.

2. Instalar dispositivos de seguridad efectivos para evitar la intrusión a las computadoras.

3. Desarrollar medidas de seguridad proyectadas para detectar a los infractores de la ley.

4. Promulgar leyes específicas a este caso y exigir su observancia.

VIII. MEDIDAS CORRECTIVAS

Si bien el grado de informatización en nuestro país es incipiente, son claras las tendencias a una mayor incorporación de las nuevas tecnologías y toda vez que en México, al igual que en muchos países no existe un tipo específico que sancione las nuevas conductas delictivas, estamos seguros de que la única medida correctiva que se puede imponer a esta situación es precisamente su tipificación.

El Derecho se halla hoy en una instancia histórica en la que debe responder a los nuevos y complejos problemas que le plantea la amplitud y profundidad del avance tecnológico en general y de la informática en especial, por lo tanto, para salvar los vacíos normativos, se deben dictar medidas penales especialmente referidas a los delitos informáticos, medidas que sean lo suficientemente generales y flexibles para ser aplicadas a pesar de la rápida evolución de la tecnología computacional.

Creemos que la inclusión en el Código Penal de una figura jurídica creada expresamente para este fin, sería de gran utilidad no sólo por su carácter correctivo, ya que de existir una sanción para quien incurra en su comisión, se evitaría caer en ella, funcionando de esta manera también como medida preventiva.

Cabe aclarar que la existencia de una ley que sancione esta nueva delincuencia no puede en y por sí misma detener la comisión de lo que hemos llamado **"Abuso Informático"**, pero consideramos que a la larga la nueva legislación reduciría el número de esta clase de ilícitos.

CAPITULO IV

DELITOS INFORMATICOS: SITUACION INTERNACIONAL

Dado que esta nueva delincuencia lo es así para todo el mundo, ha sido objeto de estudio para su eventual tipificación, sobre todo en los países industrializados y, por ende, más informatizados.

A continuación presentamos algunos de los elementos más significativos a este respecto en tres países de nuestro continente como son los Estados Unidos de Norteamérica, Canadá y Argentina.

IV.I. ESTADOS UNIDOS DE NORTEAMERICA

a). LEGISLACION FEDERAL

A falta de una ley específica en este país, desde 1979 existen alusiones a los delitos informáticos en la legislación federal, por lo que se han dado 40 reformas federales directa o indirectamente vinculadas al tema. Algunas de las más relevantes son las siguientes:

- Fraude postal (Mail fraud)
- Fraude telegráfico (Wire fraud)
- Peculado o robo de dinero, propiedad o archivos públicos (Embezzlement or theft of public money, property or records).
- balances falsos en solicitudes de préstamo o crédito (False statements on a loan or credit application)
- Robo o peculado de una institución financiera (Theft or embezzlement from a financial institution)
- Asientos falsos en los archivos de instituciones bancarias o de crédito (False entries in bank or credit intitution records).

- Transportación interestatal de mercancía robada (Iterstate transportation of stolen goods)
- Comercio interestatal de mercancía robada (Theft of goods intertate commerce)
- Destrucción o daño malicioso a propiedad pública (Malicious destruction or damage to gobernment property)
- Incendio premeditado (Arson)
- Ocultación, remoción o mutilación de archivos públicos (Concealment, removal or mutilation of public records)
- Ley sobre socalíneros y organizaciones corruptas (Racketers influenced and corrupt organizations Act)
- Leyes antimonopolio (Antitrust laws)
- Revelación de información confidencial (Disclosure of confidential information)
- Defensa nacional (National defense)

Aparte de los preceptos alusivos a la violación de secretos, otras de las figuras aplicables son las concernientes a:

- Robo (hurto)(Theft [Larceny])
- Fraude de tarjetas de crédito (Credit card fraud)
- Abuso telefónico (Telephone abuse)
- Robo con escalo (Burglary)
- Falsificación (Forgery)
- Daño malicioso (Malicious mischief)

Si bien es cierto que estas disposiciones sirvieron como paliativo en la problemática de los delitos informáticos, no fueron suficientes para resolverla, por lo que el 12 de Octubre de 1984 fue adoptada por el Congreso Norteamericano la "Ley que regula el Acceso Fraudulento a las Computadoras y el Fraude y Abuso Computacionales"(Counterfeit Access Device and Computer Fraud and Abuse Act) que introdujo en el Código Penal Federal un conjunto de disposiciones bajo el rubro "Fraude y Actividades relacionadas con respecto a las Computadoras (Fraud and Related Activity in Connection with Computers), el cual tipifica penalmente el acceso no autorizado a sistemas informáticos operados por el Gobierno y en particular los relacionados a la defensa nacional, las relaciones externas y la energía atómica así como a las instituciones financieras.

Dicho texto impone una multa de 10 mil dólares ó 10 años de prisión, pudiendo ser las dos penas a la vez, a quién conforme a la letra "...whoever, knowingly accesses a computer without authorization or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend...",es decir, "...aquel que con conocimento de causa tenga acceso a una computadora sin autorización o aún teniendo permiso se valga de la oportunidad que le ofrece tal acceso para propósitos no contemplados por dicha autorización..." y que por ese medio se lleven acabo acciones tales como:

- Obtener información "protegida" a título de interés nacional concernientes, por ejemplo, a la defensa nacional o a la considerada por la ley de Energía Atómica de 1954.

- Obtener información de carácter financiero referida a la ley de Privacidad Financiera de 1979 (Fair Credit Reporting Act).

- Modificar, destruir, divulgar información o impedir un uso autorizado de la computadora, tratándose de computadoras bajo el control del Estado.

Este ordenamiento también sanciona la tentativa con las mismas sanciones que impone al delito consumado. Las penalidades dependen del tipo de información accesada y del valor de la misma.

---

(1) VIVANT, Michel y otros. Droit de l'Informatique. Paris, Edit. Lamy, S.A., 1986, p. 1028.

Sin embargo esta ley, no obstante de ser la única legislación federal que específicamente prohibe el comportamiento ilegal de una persona al usar una computadora para efectuar un delito, adolece de un gran defecto. Como ya se dijo, sanciona penalmente el acceso no autorizado a sistemas informáticos operados por el Gobierno, por lo que haciendo una interpretación a contrario sensu de la disposición en cuestión , si el acceso indebido es a sistemas de cómputo operados por el sector privado, no constituye delito.

b). LEGISLACION ESTATAL

Las leyes estatales que tratan sobre este tema son tan numerosas (cerca de 40) como variadas. A continuación se enlistan algunos de los estados de la Unión Americana que cuentan con este tipo de ley y el ano en que se promulgaron:

- Alaska, 1983
- Arizona, 1978
- California, 1983
- Colorado, 1982
- Delaware, 1982
- Florida, 1983
- Georgia, 1983
- Illinois, 1983
- Massachusetts, 1980
- Michigan, 1981
- Minnesota, 1983
- Missouri, 1983
- Ohio, 1982
- Rhode Island, 1981
- Tennessee, 1985
- Pennsylvania, 1985
- Washington, 1985 (2)

Como podrá observarse, la preocupación de estos estados por tratar de resolver la problemática ante la que se enfrentaron por carecer de una ley especifica que regulara esta conducta antijurídica surgió a principios de la década de los 80.

Aunque estas leyes son diferentes entre sí en cuanto a las técnicas de incriminación, todas insisten en el carácter intencional y malicioso del comportamiento que pretenden reprimir, a pesar de que los textos no ofrecen semejanza:

El Código Penal de California, en su Artículo 502, reformas de 1979, t 191, senala que será objeto de una sanción "...toda persona que intencionalmente o maliciosamente, según el caso, acceda...".

---

(2) VIVANT, Michel. Loc. cit.

Por su parte, el ordenamiento de Delaware en su Artículo 858, reforma de 1982, Fraude Informático, menciona que "...aquel que con conocimiento de causa o en forma deliberada, directa o indirectamente...".

La Ley de Delitos Computacionales de 1978 de Florida contempla que "...aquel que en forma deliberada, con conocimiento de causa y sin autorización...".

De igual forma, en el Estatuto 18, enmienda de 1984 sobre el Uso Inadecuado de las Computadoras de Pennsylvania, encontramos la fórmula "intencionalmente y sin autorización".

En cuanto a las diferencias, el Código Penal de California en su Art. 502b incrimina a toda persona que intencionalmente acceda o permita el acceso a un sistema o a una red informática con el propósito de idear o ejecutar toda maquinación o artificio a fin de obtener dinero, propiedades o servicios.

Por su parte, el Art. 502c del ordenamiento citado incrimina a toda persona que maliciosamente acceda o permita el acceso a un sistema o red informática a fin de obtener información no autorizada concerniente a la reputación de terceros o que introduzca información falsa a fin de afectar para bien o para mal la reputación de un tercero.

Así mismo, el Art. 502d del texto señalado sanciona a toda persona que maliciosamente acceda, altere, borre, provoque perjuicio o destruya todo sistema informático, red informática, programa o datos.

Por su lado, Florida organiza su ley en tres grandes cuerpos de reglas en los que sanciona:

1. Los delitos contra los datos y programas.

2. Los delitos contra el equipo y las provisiones informáticas.

3. Los delitos contra los usuarios.

Cada uno de estos rubros es objeto, a su vez, de una organización interna. Es así que entre los delitos contra la propiedad intelectual figuran tres clases de comportamientos:

- la modificación
- La destrucción
- La divulgación y aprehensión de datos intelectuales

Cabe precisar que en esta última subdivisión, divulgación y aprehensión, no se sanciona la conducta delictiva a menos de que se atente contra los datos en un sentido amplio, pudiendo constituir un secreto de fábrica o confidencial en los términos de la legislación de florida.

Otro aspecto interesante es el relativo a las definiciones, las cuales tienen un gran valor en la interpretación de las disposiciones legales:

La ley de Pennsylvania define el programa (computer software) como "un conjunto organizado de instrucciones" y al software como "los programas, procedimientos y documentación asociada".

En cuanto a los datos, la palabra nos remite por regla general a información, conocimientos, hechos, conceptos, instrucciones y al respecto ciertos textos precisan que la "forma" en que éstos se encuentren no es importante, como es el caso de la Ley de Delaware que cita de manera enunciativa más no limitativa, microfilms, microfichas, procedimientos magnéticos, etc.

Así mismo, tenemos el término "propiedad", el cual puede suscitar controversias, pues en la noción tradicional de este concepto, la tangibilidad era integral a su definición.

El texto californiano senala que por propiedad se comprenden, sin ser limitativa esta definición, los instrumentos financieros, datos, programas de computación, documentos asociados con los sistemas y programas de cómputo o copias de éstos ya sean tangibles o intangibles, incluyendo tanto el sistema humano como el de cómputo capaces de leer la información y los datos que estén en tránsito.

En el caso del estado de Virginia, el Código criminal considera "propiedad" "el tiempo de computadora o de servicios de procesamiento de datos" y, por tanto, incrimina su uso no autorizado.

Por su parte, en el Distrito de Columbia se trató de incluir los bienes intangibles tales como los programas de computación en la definición tradicional de propiedad que contempla la prohibición de la venta no autorizada de cualquier "cosa de valor (3)". Sin embargo, la Corte concluyó que si los datos al ser copiados o extraídos no se trasladaban a una forma tangible, no encuadraban en las normas de definición de propiedad.

(3) VIVANT, Michel. Loc. cit.

IV.2. CANADA

En este país, el texto adoptado en Abril de 1985 fue resultado de los trabajos de un Comité Especial reunido para estudiar "las infracciones relativas a las computadoras".

Con la voluntad manifiesta de respetar "el principio fundamental del Derecho Penal, según el cual la definición de las infracciones debe ser precisa y justa de manera que permita una interpretación conveniente de las disposiciones legislativas e indique adecuadamente al público las actividades que están precisamente prohibidas (4)", el legislador canadiense creó dos nuevas infracciones:

1. El uso no autorizado de un sistema informático.

2. La modificación o destrucción no autorizada de datos informatizados.

Así mismo, ha hecho evidente su preocupación por las medidas preventivas que se pueden aplicar. Una de las recomendaciones hechas por el Comité es que "los profesores de informática estén debidamente 'calificados' en el ámbito de la ética en informática (5)". consideramos que con esta medida pretenden crear conciencia en el personal especializado en la materia en cuestión, pues normalmente incurren en el delito informático debido a la facilidad de su comisión y al uso de la máquina, factores que los orillan a minimizar el daño provocado a terceros.

El texto al que nos referimos al inicio de este punto nos remite a un nuevo artículo inserto en el Código Criminal, el 301.2, el cual en su primera parte menciona:

"Cualquiera que fraudulosamente y sin apariencia de derecho:

(a) Obtenga cualquier servicio computarizado directa o indirectamente.

(b) Por medio de un dispositivo electromagnético, acústico, mecánico o de cualquier otro tipo, directa o indirectamente intercepte o haga interceptar toda función de un sistema de cómputo; o

(c) Directa o indirectamente utilice o haga utilizar un sistema de cómputo con la intención de cometer una falta de las señaladas en las Fracciones (a) o (b) o una de las infracciones previstas en el Artículo 387 concernientes a los datos o a los sistemas de cómputo;

---

(4) Ibidem, p. 1029.
(5) Loc. cit.

es culpable de un acto criminal y sujeto a una pena de privación de la libertad que no excederá de 10 anos o es culpable de una infracción castigable sobre declaración sumaria de culpabilidad".

La parte Dos de este artículo se encarga de precisar las definiciones que son de gran importancia en la interpretación de los tipos penales alusivos, tales como:

"PROGRAMA DE COMPUTO": Significa datos que representan instrucciones o estados de cuenta que cuando son ejecutados en un sistema de cómputo, dan lugar a que éste realice una función.

"SERVICIO DE COMPUTO": Incluye el procesamiento de datos y el almacenamiento o recuperación de los mismos.

"SISTEMA DE COMPUTO": Significa un dispositivo o grupo de éstos que estén interconectados o relacionados, los cuales

(a) Contengan programas de cómputo u otros datos; y

(b) Conforme a los programas de cómputo,
(i) Realicen lógica y control; y
(ii) Puedan realizar cualquier otra función.

"DATOS": Significa la representación de información o de conceptos que están siendo preparados o han sido preparados en una forma adecuada para usarse en un sistema de cómputo.

"APARATOS ELECTROMAGNETICOS, ACUSTICOS, MECANICOS U OTROS": Significa cualquier dispositivo o aparato que sea usado o sea factible de ser usado para interceptar cualquier función de un sistema de cómputo, pero no incluye al audífono utilizado para corregir la audición deficiente del usuario que no perciba una audición mejor que la normal.

"FUNCION": Incluye lógica, control, aritmética, supresión o borraduras, almacenamiento, recuperación y comunicación o telecomunicación a, de o dentro de un sistema de cómputo.

"INTERCEPTAR": Incluye escuchar o registrar una función de un sistema de cómputo o captar la sustancia, significado o esencia del contenido".

El Artículo 387 a que se refiere el Inciso (c) de la Sección 1 del Artículo 301.2, trata de proteger la esencia de los datos informatizados, haciendo acreedora a una pena no mayor de 10 anos 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; o

(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.

En cuanto a las definiciones utilizadas en el Código Criminal de Canadá respecto a los delitos informáticos, estimamos que algunas de ellas no son las apropiadas debido a su falta de precisión, característica que el gobierno canadiense considera fundamental en el Derecho Penal, como ya se dijo, para una interpretación conveniente de sus disposiciones.

Respecto a la forma en que este país está enfrentando el problema derivado del mal uso de las computadoras y de la información que éstas contienen, consideramos que aunque de manera concisa, está siendo substancioso y el hecho de que ya cuenten con una figura jurídico-penal que sancione estas conductas, ha sido benéfico pues su comisión ha disminuido.

IV.3. ARGENTINA

Argentina es uno de los pocos países que se ha preocupado por resolver la problemática de los delitos informáticos, tan és así que en Mayo de 1986 se propuso la aprobación de un proyecto de ley denominada "Ley Nacional de Informática" (6). Este proyecto contiene en su Capítulo VI una serie de disposiciones alusivas a los delitos informáticos:

El Artículo 21 de dicho proyecto sugiere un agregado al numeral 163 del Código Penal Argentino, el cual regula el hurto calificado. La adición que se propone es la siguiente:

"Será reprimido con prisión de tres a cinco anos e inhabilitación por igual término al que accediere por medios fraudulentos a un programa de informática. Igual recibirá quien desviare, alterare o usare un tratamiento informatizado con vistas a obtener ganancias ilícitas".

El Artículo 22 del mencionado proyecto sugiere la incorporación de un tercer inciso en el Artículo 215 del referido código penal, el cual prevee los delitos contra la seguridad de la Nación. Dicho inciso se transcribe a continuación:

(6) TRAMITE PARLAMENTARIO NO. 19. Ley Nacional de Informática. (525-d-86). Argentina, 1986, pp. 474 y ss.

"Será reprimido con reclusión o prisión de 10 a 25 anos o reclusión o prisión perpetua a quien alterare, desviare, usare o destruyere un soporte físico y/o soporte lógico para informática en razón de espionaje que pusiere en peligro la paz interior para alterar el orden constitucional o , en caso de guerra, significare colusión con el enemigo".

A su vez, el Artículo 23 del proyecto en cuestión propone que se incluya un sexto inciso al Artículo 184 del Código Penal, mismo que sanciona el daño calificado. Este inciso se cita en los siguientes términos:

"Será reprimido con prisión de seis meses a cinco anos a quien destruyere intencionalmente el contenido de información y conocimiento alojado en un soporte físico para informática".

Por último, el Artículo 24 del multicitado proyecto menciona los siguientes agregados al Artículo 249 del Código penal, el cual sanciona la omisión de deberes de los funcionarios públicos. Estos agregados textualmente dicen:

1. "Será reprimido con prisión de seis meses a dos anos el que habiendo reunido en ocasión de su registro, clasificación, transmisión y otra forma de tratamiento, informaciones sobre particulares, sus datos personales, bienes y cualquier otra información que hagan a su perfil social, económico, psicológico y/o ideológico cuya divulgación tuviere como efecto atentar contra la reputación, consideración de la persona y/o intimidad de su vida privada, hubiere, sin autorización del interesado y a sabiendas, puesto tales datos y/o informaciones en conocimiento de una persona que no estuviere habilitada para recibirlos de acuerdo con las disposiciones legales".

2. "Será reprimido con prisión de uno a cinco anos la autoridad de un registro de datos públicos o privados que negare su acceso a dicho registro a una persona física o jurídica para su conocimiento, aclaración o rectificación de la información allí almacenada, siempre y cuando que con dicha negativa causare un perjuicio irreparable".

De los artículos mencionados se puede notar que a falta de figuras jurídicas específicas, Argentina ha tratado de salvar los vacíos de su legislación penal equiparando los delitos informáticos a figuras tradicionales ya existentes en su cuerpo normativo como el hurto,daño, etc., arriba señaladas.

Sin embargo, consideramos que les hace falta precisar algunos términos empleados en los agregados que proponen, tales como:

- Programa de informática
- Tratamiento informatizado
- Soporte físico
- Soporte lógico

En materia penal, estas definiciones podrían ser trascendentales para una correcta interpretación de la norma.

Como puede observarse, estos países, conscientes de la problemática a la que se enfrenta la sociedad por los efectos negativos que vienen aparejados con el avance informático, ya legislaron en materia penal sobre los delitos informáticos.

Otros, por su parte, han tocado este asunto, aunque en forma muy incipiente pero, de alguna manera ya están sentando las bases para que en un futuro no muy lejano y apoyándose en datos empíricos, puedan perfeccionar las figuras jurídico-penales que regulan esta nueva modalidad delictiva.

En cambio otros más, creemos que están a la expectativa de como los países más informatizados resuelven esta situación para que, de cierto modo, sirvan de pauta para la creación de su legislación local en lo que se refiere a esta materia, y estén preparados para cuando alcancen un grado de información relevante.

CAPITULO V

DELITOS INFORMATICOS: SITUACION NACIONAL

La problemática de los delitos informáticos requiere de un estudio especial en nuestro país a fin de determinar la medida en que las leyes penales vigentes constituyen un cuerpo normativo suficiente para prevenir y reprimir este tipo de conductas delictivas o si es menester la creación de figuras jurídico-penales que expresamente regulen esta nueva modalidad delictiva.

Aunque en México ya ha sido vislumbrado incipientemente este asunto desde el punto de vista jurídico, a la fecha no ha sido tipificada ninguna conducta ilícita derivada del avance tecnológico, más bien, se ha pretendido asimilar la conducta delictiva realizada con las computadoras a los diversos tipos de delitos que actualmente regula el Código Penal para el Distrito Federal,empero,no se debe olvidar que en materia penal no es aplicable la analogía, sino que el delito debe estar perfectamente tipificado en un ordenamiento legal, según se desprende del Artículo 14 constitucional que a la letra dice:

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

I. TIPOS PENALES DIRECTAMENTE VINCULADOS AL DELITO INFORMATICO

En un análisis de los artículos del mencionado ordenamiento penal, nos referiremos a los siguientes numerales que de alguna forma han sido vinculados con el delito informático. También proporcionaremos una base que consideramos constructiva para hacer distinciones y comparaciones con tales tipos penales:

REVELACION DE SECRETOS. "Art.210.- Se aplicará multa de cinco a cincuenta pesos o prisión de dos meses a un ano al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto".

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

Consideramos que este delito se refiere principalmente a la obtención por parte de competidores de fórmulas, inventos o resultados de investigaciones.

Debido a las dos partes básicas que integra a una computadora (hardware y software), esta situación también se ve protegida tanto en su idea como en su uso no autorizado. El hardware, por su diseno, se adecua a la Ley de Invenciones y Marcas. Por su parte, el software o programa de computación, es protegido por la Ley Federal de Derechos de Autor. Sin embargo, ambas legislaciones sólo brindan al creador, inventor o disenador de la obra, derechos exclusivos dentro de ciertos límites temporales y geográficos.

No obstante, ninguna de estas leyes son aplicables cabalmente al delito que resulta de obtener información utilizando una computadora y su posterior divulgación por las siguientes razones:

En primer lugar, una persona puede revelar "un secreto o comunicación reservada" que obtiene pero no con motivo de su empleo, sino que se allegó a ella por medio de una computadora y sin tener relación laboral ni de otra clase con el sujeto pasivo.

En segundo lugar, el software, al ser utilizado no se compone en su totalidad de información considerada como una "obra intelectual", pues viene a ser una especie de esqueleto con espacios a llenar; una vez cubiertos, puede tratarse de información confidencial, más no de secretos industriales ni de obras intelectuales cuya divulgación puede ser perjudicial para el sujeto pasivo más allá del tiempo que las leyes mencionadas senalan. En cuanto al hardware, éste no se ve afectado cuando una persona se introduce indebidamente desde una terminal remota e independiente al sistema de cómputo ajeno.

FALSIFICACION: "Art. 239.- Al que cometa el delito de falsificación de títulos al portador y documentos de crédito público, se le impondrá de cuatro a diez anos 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 de dividendos de esos títulos.
"II. Las obligaciones de la deuda pública de otra nación, cupones de interés o de dividendos de otros títulos.

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

"Art. 244.- 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 una 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 sociedad, el Estado o a un tercero;

"III. Alterando el contexto de un documento verdadero después de concluído y firmado, si ésto cambiare su sentido sobre alguna circunstancia o punto sustancial, ya se haga anadiendo, enmendando o borrando, en todo o en parte, una o más palabras o claúsulas, o ya variando la puntuación;

"IV. Variando la fecha o cualquier otra circunstancia relativa a al tiempo de la ejecución del acto que se exprese en el documento.

"V. Atribuyéndose al 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. Anadiendo o alterando claúsulas 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 contenido 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".

El aumento en el volumen y la complejidad de las actividades a realizar, ha traído como consecuencia que varias de estas tareas sean efectuadas por la computadora. Por razones de orden práctico, la elaboración de documentos escritos es una de las actividades asignadas a tales máquinas.

Actualmente se emiten por computadora documentos tales como cheques, letras de cambio, pagarés, facturas, etc. Y, con fines de prontitud, la mayoría de éstos vienen con la firma impresa.

Desafortunadamente las características y uso de las computadoras que son utilizadas para el beneficio del hombre, son las mismas que se aprovechan en su perjuicio. Así tenemos que también es práctica común la producción indebida de originales, y no de copias, de los documentos mencionados.

Con el uso de dichas máquinas, es relativamente fácil emitir tantos originales de un mismo documento como se desee. Simplemente se programa a la máquina para que, por ejemplo, por cada determinada cantidad de títulos de crédito o documentos que emita, expida uno de más. Una vez echo lo cual, a través de las instrucciones correspondientes, se ordena a la maquina borrar el programa mediante el cual se le dieron tales órdenes no autorizadas y de esta forma se destruye todo indicio que pueda incriminar al delincuente.

Creemos que un documento indebidamente emitido por esta vía, reune todas las características de un original, más aún cuando cuenta con la firma impresa; por lo tanto, consideramos que el tipo penal que se analiza no encuadra enteramente con esta nueva forma de delinquir. Tal vez lo que debería ponerse en tela de juicio no es la originalidad, sino la voluntad del firmante a comprometerse mediante un documento que se expide sin su conocimiento y, mucho menos, sin su consentimiento.

ROBO. "Art, 367.- Comete el delito de robo: el que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que pueda disponer de ella con arreglo a la ley".

Es cuestionable si la figura de "robo" que requiere la privación permanente de un bien mueble a la víctima se adecua a esta acción delictuosa porque, primeramente, este numeral habla de un "apoderamiento", mismo que debe ser material. Como ya se ha apuntado, una persona puede tener acceso desde un lugar lejano a la unidad central de procesamiento de una computadora ajena y, entre otras cosas, 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 esto exista apoderamiento de la misma. La sigue dejando donde está, sin embargo, aunque no haya un desposeimiento, sí se da una disminución en el valor de la información, lo cual le para un perjuicio a su propietario.

Ahora bien, otra de las causas por las que creemos que es improcedente la aplicación de este artículo a dicha nueva conducta delictiva, es porque el robo se refiere a bienes muebles. La información es un bien intangible; es susceptible de apropiación, pero no es mueble.

Por lo tanto, si se insiste en adecuar las figuras jurídico-penales tradicionales como el robo a esta nueva modalidad delictiva, se tendrán entonces que modificar dos conceptos: el de "apoderamiento" en el que se considere no sólo el desposeimiento del bien, sino también la disminución de su valor; y el de "bien mueble" en el que se incluyan bienes intangibles como la información que si puede ser susceptible de apropiación, también debe ser susceptible de protección jurídica.

ROBO DE FLUIDO. "Art. 368.- se equiparan al robo y se castigarán como tal:

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

Respecto a este numeral, también estimamos que es dudosa su aplicación ya que se refiere al "aprovechamiento de energía eléctrica o de cualquier otro fluido" sin embargo, la información no es energía eléctrica ni tampoco es un fluido.

El individuo que se accesa a la unida central de procesamiento de una computadora ajena, lo hace generalmente desde su terminal, por lo que está utilizando energía eléctrica a la que él 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" (1). De aquí se desprende que la información no es un fluido, pues lo que fluye a través de estos sistemas es energía electrica y aunque la información allí contenida es representada mediante impulsos eléctricos, ésta, per se, no es un fluido.

El acceso a una computadora ajena vía telefónica, es una de las formas más socorridas para allegarse indebidamente de información perteneciente a otras personas cuya obtención, como ya se dijo, no implica necesariamente la privación de la misma de su legítimo propietario, sin embargo, si se le ocasiona un gran daño a este pues la información pierde gran parte de su valor y en algunos casos, quizá todo, con su simple divulgación.

En esta acción no sólo se comete ese ilícito, sino que también se desprenden los relacionados con el acceso ilegal a dicha máquina, aparte del uso no autorizado de la computadora ajena y el perjuicio que resulta para el dueño de la misma por el tiempo de servicios en que ésta es distraída por la realización de funciones no autorizadas por él.

En un caso como éste, el delincuente queda impune pues el tipo penal en cuestión no es de ninguna manera aplicable a esta nueva conducta delictiva.

ROBO DE USO. "Art. 380.- Al que se le imputare el hecho de haber tomado una cosa ajena sin el consentimiento del dueño o del legítimo poeedor y acredite haberla tomado con carácter temporal y no para apropiársela o venderla, se le aplicarán de uno a seis meses de prisión, 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".

Consideramos que este artículo tampoco es adecuado a la conducta ilícita que resulta de utilizar a una computadora ajena, pues lo que se toma no es un bien, sino un servicio que es realzado por una máquina.

Aquí el robo consiste en servicios de procesamiento, es decir, en utilizar las funciones propias de una computadora y ésto ocurre frecuentemente en las empresas; esta acción es cometida por los empleados para efectuar trabajos personales utilizando dicha máquina sin autorización. Sin embargo, este ilícito también puede ser perpetrado a distancia por personas ajenas a los entes físicos o morales propietarios de las computadoras.

(1) Pequeño Larousse en Color, Ediciones Larrouse,España,1981,p. 411.

Como ya hemos mencionado, el uso de la computadora tiene un costo en el que se implican tanto las funciones que ésta realiza (robo de servicios), como el tiempo en que las lleva a cabo (robo de tiempo), factores inseparables de la entidad física de la máquina misma,

El acceso no autorizado a una computadora ajena da lugar a varias acciones delictuosas no contempladas por los tipos penales existentes, tales como:

- Enterarse de la información intangible allí almacenada.

- Copiar, modificar o destruir la información que esta contiene.

- Realizar servicios de procesamiento.-

El avance tecnológico ha hecho posible la comisión de estos ilícitos y muchísimos más. La zaga negligente en la que se ha quedado el Derecho, los ha soslayado.

ABUSO DE CONFIANZA. "Art. 382.- Al que, con perjuicio de alguien, disponga para sí o para otro, de cualquier cosa ajena mueble de la que se le haya transmitido la tenencia y no el dominio, se le sancionará con prisión...".

Creemos que este tipo penal no encuadra cabalmente en su aplicabilidad al delito informático, toda vez que la "disposición" no recae sobre un bien mueble, sino sobre un bien intangible,la información, misma que no se ajuste al concepto de "mueble" por las razones antes apuntadas al analizar el delito de robo.

Por otra parte, este numeral menciona la previa transmisión de la tenencia sobre el bien que va a ser objeto de posesión, situación que no se presenta en la comisión del ilícito informático, pues el ofendido generalmente desconoce al sujeto activo que dispone de la información de la que él es propietario, por lo tanto, no es factible la celebración de un acuerdo sobre dicha transmisión.

FRAUDE. "Art. 386.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido...".

En esta disposición tampoco es enteramente aplicable pues se requiere que una persona sea enganada o se dé un aprovechamiento en virtud del error en que ésta se encuentra y en el delito informático no hay tales. El sujeto activo que indebidamente entra a la unidad central de procesamiento de una computadora ajena, lo hace sin conocimiento de su propietario, por lo tanto, sin enganarlo y sin inducirlo al error. Simplemente se introduce,examina,transfiere,extrae,destruye,etc. la información que ésta contiene y como intruso que es, sale subrepticiamente.

Por otra parte, en la comisión del delito informático la que es objeto de engano es la computadora pero, cabe hacer mención que sólo las personas son capaces ante la ley, por lo tanto, enganar a una máquina no constituye delito.

DANO EN PROPIEDAD AJENA. "Art. 397.- Se le impondrán de cinco a diez anos de prisión y multa de cien a cinco mil pesos, a los que causen incendio, inundación o explosión con dano o peligro de:

"I. Un edificio ,vivienda o cuarto donde se encuentre alguna persona.

"II.Ropas, muebles u objetos en tal forma que puedan causar graves danos personales;

"III. Archivos públicos o notariales;

"IV. Bibliotecas, museos, templos, escuelas o edificios y monumentos públicos, y

" V. Montes, bosques, selvas, pastos, mieses o cultivos de cualquier género".

"Art. 399.- Cuando por cualquier medio se causen dano, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones del robo simple".

Aunque estos numerales protegen a la propiedad, se refieren a ésta pero sólo en su aspecto tangible, en su integridad física.

En el caso de delito informático, este tipo penal sería suficientemente aplicable ya sea para el equipo en sí, es decir, para la computadora como entidad física, como bien mueble, o para los dispositivos materiales de almacenamiento como cintas magnéticas, discos duros y flexibles, etc.

Sin embargo, este tipo penal no prevee las consecuencias que su comisión puede ocasionar en tales objetos, herramientas fundamentales de la Revolución Informatica, pero no en su aspecto fisico, sino en el alma de su objeto, pues en caso de dano de,por ejemplo, una cinta magnética, el valor material de ésta como continente, es irrisorio comparado con el de su contenido, es decir, de la información que almacenan, cuya elaboración pudo haber implicado mucho tiempo, mucho trabajo y mucho dinero.

II. TIPOS PENALES INDIRECTAMENTE IMPLICADOS CON EL DELITO INFORMATICO

Actualmente existen determinadas figuras contempladas en nuestro ordenamiento penal que, de acuerdo con su texto, no tienen ninguna relación con el delito informático, sin embargo, dadas las caracteristicas de éste como de sus resultados, estimamos conveniente ya sea la inclusión de una fracción alusiva a esta nueva conducta delictiva o la creación de un tipo penal especifico. Tal es el caso de los siguientes articulos:

SABOTAJE: "Art. 140.- Se impondrá pena de dos a veinte anos de prisión y multa de mil a cincuenta mil pesos, al que dane, destruya o ilicitamente entorpezca vias de comunicación, servicios públicos, funciones 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 articulos de consumo necesario, de armas, municiones o implementos bélicos, con el fin de trantornar la vida económica del pais o afectar su capacidad de defensa...".

Primeramente, este tipo penal sólo protege bienes y servicios públicos, de tal suerte que si se trata de bienes no pertenecientes a este sector, no constituirán, por lo menos, el delito de sabotaje.

Por otra parte, por sabotaje, palabra francesa, se entiende "la acción de perjudicar el obrero al patrono ejecutando mal un trabajo o provocando desperfectos en los talleres y máquinas" (2). La Revolución Informática ha permitido que no sólo el empleado inconforme y deseoso de venganza perjudique al patrón, sino también personas ajenas a él, ya sea con el fin de demostrar su superioridad intelectual o con propósitos terroristas, perjuicios de enormes proporciones y que puede ejecutarse a distancia.

El sabotaje informático bien puede perpetrarse contra los datos, contra los programas o contra la misma computadora. Su comisión puede hacerse de múltiples maneras. A continuación se señalan algunas:

1. Bomba de tiempo: Es un programa contenido dentro de otro con instrucciones precisas de destruir al legítimo.

2. Rutina cáncer: Este programa se encuentra incluído en otro y su fin es distorsionar mediante instrucciones que se autorreproducen, el funcionamiento ya sea del programa autorizado o del equipo informático en sí.

3. Caballo de Troya: Consiste en la introducción de instrucciones aparentemente relacionadas con el programa autorizado, en las que se ordena realizar funciones no aprobadas como acreditar a una cuenta previamente designada por el delincuente el producto de sus fechorías o borrar todos los archivos de datos de la computadora.

4. Programa virus: Se lleva a cabo mediante la introducción de instrucciones que se infiltran automáticamente en otros programas y archivos. Estas instrucciones permanecen en la memoria de la computadora hasta en tanto no se apague, alterando o destruyendo los datos almacenados en todos los discos que se inserten en ésta, los que a su vez, quedan infectados y en posibilidad de propagar el virus.

   Y éste no es todo el daño que ocasionan, ya que estos diminutos pedazos de código computarizado también están diseñados para cambiar a otros sistemas contagiando a aquellos a los que están interconectados. Por su gran dispersabilidad, constituyen verdaderas pandemias que llevan consigo enormes pérdidas, principalmente de carácter económico.

5. Técnica Salami : En programas autorizados se introducen instrucciones veladas para que se redondeen cuentas bancarias y las fracciones resultantes se acrediten a una cuenta señalada previamente por el programador. Esta nueva manera de delinquir no es nada desdeñable, pues así se han formado enormes fortunas.

Una de las características del sabotaje informático es que generalmente no hay signos visibles de infección hasta que el daño está hecho, pues el virus está diseñado para permanecer latente por mucho tiempo. Llegado el momento, se activa a sí mismo orientándose con el reloj calendario que tienen la mayoría de las computadoras; se apodera del control de la máquina e inicia su destrucción, por lo regular, con un aviso cáustico.

---

(2) Pequeño Larousse en Color, Ediciones Larousse, España 1981, p. 801.

Otra, es que el acto delictivo se repite automáticamente indefinidas veces sin ulterior intervención del saboteador.

A través del sabotaje informático, aparte de que se ocasionan daños de enormes proporciones, los delicuentes quedan impunes, factores que erigen paradigmas deplorables y lastimeros ejemplos a seguir, por lo que es menester que nuestra legislación contemple este tipo penal de acuerdo con las necesidades sociales prevalecientes actualmente.

DELITOS COMETIDOS POR SERVIDORES PUBLICOS. Consideramos que es necesaria la inclusión de un artículo específico al delito informático dentro del Título Décimo de nuestro Código Penal, pues siendo el Estado el principal usuario del más grande y mejor equipo de computación y la información que procesa tan innumerable como variable: fiscal, policial, política, electoral, etc., el daño que ocasionaría un servidor público al usar indebidamente una computadora, sería de consecuencias de enorme trascendencia en donde no se daña sólamente a una persona física o moral, sino a toda una nación.

Por ejemplo, en la vida política de nuestro país, la computadora ha jugado un papel preponderante, concretamente en las elecciones pasadas.

Cuando viejas fórmulas como "el afeite del padrón electoral"(eliminación del listado de un porcentaje de electores), "la operación carrousel" (acarreo masivo de votantes) y "las urnas embarazadas" (introducción de boletas cruzadas en favor del partido en el poder al inicio de la votación), entre otras, no dieron los resultados esperados, se tuvo que declarar oficialmente que el sistema de computadoras del Registro Nacional de Electores "se había caído", mientras se preparaba un programa adecuado para que el recuento final de los sufragios favoreciera a un partido en especial.

La computadora fue el instrumento para evitar la legalidad en el proceso electoral. Así, podemos ver que el uso indebido de esta máquina puede variar el destino de un país.

Estimamos que ya se ha dejado establecido que este tipo de delincuencia es reciente, producto de la tecnología moderna, la cual ha provocado que instituciones sociales que permanecieron estables durante siglos estén a punto de caer bruscamente.

Las figuras jurídico-penales tradicionales que han sido posibles de aplicar a los delitos informáticos, no son suficientes; "a nuevos males, nuevos remedios...". Existe una imperiosa necesidad de que se tipifique esta nueva conducta delictiva, pues su comisión ha ido en aumento.

CONSIDERACIONES FINALES

Después de la investigación que hemos realizado para la elaboración de este trabajo, nos hemos dado cuenta de que la informática, aparte de los beneficios que nos aporta, también ha traído consigo problemas con implicaciones sociales y criminales, por lo que llegamos a las siguientes concluciones:

1. Que existe la necesidad imperiosa de renovar la legislación penal de nuestro país con medidas específicas a los problemas que ha traído aparejado el avance tecnológico y, de esta forma, estar en posibilidades de brindar una mejor y más completa protección social.

2. Que dentro de la clasificación legal de los delitos, se incluya un título especial para el que hemos denominado abuso informático en el que se consideren por lo menos los siguientes tipos y establezcan sanciones para desalentar su comisión, pues si se dejan sin castigo aumentarán considerablemente causando un daño sensible a la sociedad:

   (a) Comete el delito de Abuso Informático el que examine, modifique, altere, intercepte, transfiera, borre, interfiera, introduzca o extraiga todo tipo de información contenida en la unidad central de procesamiento de cualquier computadora sino cuenta con el permiso de la persona legalmente autorizada para disponer de ella, y sin perjuicio de que pueda determinarse cualquier otro ilícito por el beneficio o lucro que pudieren obtenerse.

   (b) Independientemente del tipo y valor de la información que se obtenga y del delito que resulte, el mero acto de introducirse a una unidad central de procesamiento de una computadora ajena, constituye el delito de Allanamiento Computacional.

   (c) Comete el delito de Robo de Servicios Computacionales el que:

      I. Utilice las funciones de una computadora ajena para otros fines diferentes a los que está autorizado.

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

III. Intercepte las líneas de transmisión de una base de datos, computadora, sistema o red de computadoras, sin perjuicio de que pueda determinarse cualquier otro ilícito que resulte de esta acción.

(d) Comete el delito de Sabotaje Informático el que:

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

II. Introduzca instrucciones dentro de un programa de computación propio y lo utilice para causar daño a otros programas o sistemas de cómputo.

Para los efectos de este título, se entiende por

-COMPUTADORA: Dispositivo electrónico, magnético, óptico o electroquímico de alta velocidad de procesamiento de datos que ejecutan funciones de lógica, aritmética o almacenamiento e incluye cualquier posibilidad de almacenamiento de datos o de comunicación directamente relacionados con la operación en conjunto de tal dispositivo.

-UNIDAD CENTRAL DE PROCESAMIENTO: Unidad de una computadora compuesta por un conjunto de medios técnicos capaces de almacenar la información y procesar los datos de acuerdo con las instrucciones señaladas en el programa.

-FUNCION: Son las operaciones que realiza una computadora y que incluye lógica, control, aritmética, supresión, almacenamiento, recuperación y comunicación o telecomunicación a, de o dentro de un sistema de cómputo.

-BASE DE DATOS: Conjunto de datos organizados e interrelacionados según atributos comunes, en función de posibles requerimientos.

-RED DE COMPUTO: Red de comunicación de datos que opera mediante una estructura física (conexión física de datos) y una lógica (conexión lógica de datos).

-PROGRAMA DE COMPUTACION: Conjunto de instrucciones para ser usadas, directa o indirectamente, en una computadora a fin de obtener un resultado determinado.

-INSTRUCCIONES: Conjunto de órdenes dirigidas a una computadora con el fin de que ésta ejecute una función particular.

3. Que se obligue al sujeto pasivo que sufre este ilícito a denunciarlo ante las autoridades, pues generalmente no lo hace para evitar el desprestigio, la desconfianza y, sobre todo, que se revele la vulnerabilidad de su sistema a posibles delincuentes informáticos en potencia.

4. Que los fabricantes de computadoras se les imponga la obligación de integrar como parte del hardware de estas máquinas, un dactiloscopio complementado con un programa de identificación de huellas digitales para que sólo tengan acceso a la información contenida en las unidades centrales de procesamiento de las computadoras, las personas que estén debidamente autorizadas mediante el previo registro de sus huellas y su posterior verificación, con lo que se evitaría en gran medida la comisión del Abuso Informático.

5. Como la mayoría de los casos de acceso ilegal a una computadora ajena han sido detectados por mero accidente, también es preciso que desarrollen medidas de seguridad tendentes a descubrir a los infractores de la ley.

6. Que se capacite al personal que investiga, persigue y previene los delitos, pues no basta con que tengan conocimientos jurídicos, sino que debe contar con capacitación y equipo informático adecuado para poder combatir esta nueva modalidad delictiva.

7. Que se instruya al público no sólo sobre los usos que ofrecen las computadoras, sino también sobre los abusos que se pueden cometer con estas máquinas y las consecuencias respectivas, haciéndoles saber de igual modo, las medidas de seguridad que se pueden tomar para enfrentar este problema.

8. Crear bases de datos en territorio Mexicano con información local así como redes nacionales de transmisión de datos para evitar que recurramos a bancos de datos internacionales con el probable peligro de sufrir una alineación cultural.

9. Que desde el ámbito internacional se tomen medidas proyectadas a la búsqueda de soluciones a este problema criminológico moderno, pues como ya se ha mencionado, su comisión puede ser intercontinental y aunque en México la teleinformática se introduce gradualmente, nuestro país empieza a insertarse en las corrientes de cambio tecnológicas que predominan hoy en el mundo.

10. Que se instaure un centro de investigación jurídico-informático destinado al estudio de los cambios sociojurídicos que se van haciendo necesarios conforme avanza la tecnología, pues por la velocidad con que ésta se desarrolló, no dio tiempo para que paralelamente se fueran creando cuerpos normativos suficientes para prevenir y reprimir las nuevas modalidades delictivas o se adecuaran éstas a las leyes penales vigentes.

Como los ilícitos que se cometen con y a través de las computadoras son muchos y variados, nosotros sólo estamos tratando de que se brinde protección a la información que se encuentre en la unidades centrales de procesamiento, las cuales funcionan como el corazón y cerebro de las computadoras. Sin embargo, estamos dejando fuera de esta investigación todos aquellos ilícitos que se pueden cometer con los datos, información o programas de cómputo que no se encuentren dentro de estas máquinas y que están contenidos en dispositivos físicos de almacenamiento tales como cintas magnéticas, discos duros o flexibles, tarjetas perforadas, etc. , cuyo valor es independiente del de la información que almacenan.

En vista de que el crimen está en continua evolución y cambia conforme se transforma la sociedad y avanza la ciencia, exhortamos a los estudiosos del Derecho a realizar investigaciones jurídicas sobre este tema tan nuevo, tan amplio y de tal magnitud que cada vez está cobrando una mayor importancia debido a la penetración de la informática en todos los ámbitos de la vida social.

B I B L I O G R A F I A

ALLEN,Brandt,Peligro a la Vista, Proteja su Computadora, Articulo 105, México,Biblioteca Harvard de Administración de Empresas,1976.

BAROUSSE B.,Felipe,Asesinos Silenciosos, Revista Decisión Bit, México, D.F., No. 11, Agosto,1988.

CARRANCA y Trujillo, Raúl, Derecho Penal Mexicano, 15a. ed., México, Edit. Porrúa, 1986.

CASTELLANOS Tena,Fernando,Lineamientos Elementales de Derecho Penal, 20a. ed., México, Edit, Porrúa, 1984.

CORREA M., Carlos Derechos Informático,Buenos Aires,Ed. Depalma,1987.

CHAVEZ,Elías,Jornadas de Titubeos del Secretario de Gobernación,Revista Proceso,México,D.F:,No. 610,Julio,1988.

DEL POZO y Contreras,Luz María,El Derecho Informático y su Primer Capítulo,La Posible Protección del Soporte Lógico (Software),México,Edit. de Oportunidades, 1987.

DIAZ,Llorca Carlos,Introducción a la Computación,La Habana, Edit. Pueblo y Educación,1981.

GARCIA MAYNEZ,Eduardo,Introducción al Estudio del Derecho,17a. ed., México,Edit. Porrúa,1970.

GITIERREZ-ALAVIZ y Armario, FAustino,Diccionario del Derecho Romano,3ra. ed.,Madrid,Reus,S.A.,1982.

Instituto de Investigaciones Jurídicas,Diccionario Jurídico Mexicano,México,Edit. Porrúa,Vol. VIII,1985.

Instituto Nacional de Estadística,Geografía e Informática,La Informática y el Derecho,Informática Jurídica y Derecho Informático para México,Secretaría de Programación y Presupuesto,1983.

HAFNER M.,Katherine,Is Your Computer Secure?,Revista International Business Week,New York, N. Y.,No. 3059-389,Agosto,1988.

LIMA,Ma de la Luz,Delitos Electrónicos,Revista Criminalia,México, No. 50, 1984.

MARCHIORI,Hilda,Personalidad del Delincuente,3ra. ed.,México, Edit. Porrúa,1985.

NORA,Simon y MINC,Alain,Informatización de la Sociedad,México, Fondo de Cultura Económica,1980.

PARKER B.,Donn,Fighting Computer Crime,New York,N. Y., Ed, Scribner's Sons,1983.

PAVON Vasconselos,Francisco,Manual de Derecho Penal Mexicano,6a. ed.,México,Edit. Porrúa,1984.

ROJAS Pérez Palacios,Alfonso,Delitos de Cuello Blanco,México,Edit. Joaquín Porrúa,1986.

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

TELLEZ Valdés,Julio,Protección Jurídica de los Programas de Cómputo,México,1985.

. Derecho Informático,México,Universidad Nacional Autónoma de México,1987.

TOFFLER;Alvin,La Tercera Ola,Bogotá,Círculo de Lectores,1981.

VIVIANT,Michel y otros,Droit de l'Informatique,París,Lamay, S.A., 1886.

L E G I S L A C I O N

CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS.

CODIGO PENAL PARA EL DISTRITO FEDERAL.

COMPUTER LAW.

CRIMINAL CODE.

CODIGO PENAL DE LA NACION ARGENTINA.

TRAMITE PARLAMENTARIO NO. 19,Ley Nacional de Informática.