UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

ARAGÓN

LICENCIATURA EN DERECHO

TRABAJO POR ESCRITO QUE

PRESENTA:

ALEJANDRO REYNA LUCIO

"LOS MEDIOS INFORMÁTICOS COMO AGRAVANTE DEL DELITO DE FRAUDE"

EN LA MODALIDAD DE "SEMINARIO DE TITULACIÓN COLECTIVA"

PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

ASESOR
LIC. MARTÍN LÓPEZ VEGA

FES Aragón

MÉXICO, ARAGÓN, A 04 DE DICIEMBRE DE 2007.

A DIOS NUESTRO SEÑOR
Y A LA VIRGEN MARÍA

(QUIENES TODO LO PUEDEN, TODO LO DAN, POCO AGRADECEMOS Y MUCHAS VECES DEFRAUDAMOS)

Por permitirme avanzar otro escalón de mi vida, y culminar con ello parte de una promesa. GRACIAS por haberme dado a mis padres y hermanos pues ellos son mi verdadera familia, con quien puedo contar en las buenas y en las malas y me llenan de dicha en todo momento. GRACIAS por todo cuanto me dan, en primer lugar por darme la vida y mantenerme con salud, por regalarme este momento tan significativo en mi existencia, gracias les doy por lo que de mi ser han hecho; una cosa más les pido iluminen y guíen mis pasos, mis pensamientos, mis acciones y concédanme por mucho tiempo convivir con mi familia.

A MI AMADO PADRE

ALEJANDRO REYNA MENDOZA

(QUE DIOS QUIERA Y ESTÉS A SU LADO, COMPARTIENDO SU GLORIA.)
("Y POR QUIÉN CREES QUE HACEMOS TODO ESTO, SEAN INTELIGENTES")

A quien prometí terminar la carrera, para que estuviese orgulloso de mí. Este trabajo rinde tributo al cariño y a los años dedicados para poder darme una buena educación. GRACIAS por ser un hombre entero y cabal en toda la extensión de la palabra, por guiar mis pasos y ser mi maestro, por tus sabios consejos como aquel en donde me dijiste "estudia para que tengas un mejor futuro", por enseñarme a trabajar, por tu admirable forma de no depender de nadie para hacer las cosas; por tener un inmenso corazón al dar mucho y esperar muy poco de ciertas personas, al buscar tan solo tantito amor, apoyo y comprensión en aquellos que no saben darlo, ni valorarlo. De ti aprendí muchas cosas importantes entre ellas a ser una persona responsable, tener palabra para un compromiso, ver más allá de una simple amistad, a no estar esperanzado a la ayuda de otra persona y a saber valorar a mi familia.
La riqueza de los felices momentos que en mi mente llevo, ni el tiempo podrán destruir, puesto que los años no podrán borrar el placer y la alegría de tú recuerdo.

"TE QUIERO MUCHO PAPÁ"

A MI MADRE CON CARIÑO Y AMOR.

MARÍA GUADALUPE LUCIO COVARRUBIAS

(CON TODO MI CORAZÓN)

Esperando ser un motivo de orgullo para ti al culminar hoy otro pasó en mí haber. GRACIAS por darme la vida y cuidarme, porque no sólo me soportaste en tú vientre nueve meses, sino todo este tiempo, en el cual te he hecho pasar muchas tristezas. GRACIAS por que junto con mi padre me diste las mejores bases para mi formación profesional y personal. GRACIAS por tus consejos, por tu incansable fuerza de voluntad, entrega, esmero y dedicación para hacer de mí una buena persona, por acompañarme en cada momento de alegría y tristeza de mi vida, por enseñarme que todo cuesta y no es tan fácil obtenerlo ya que es necesario en muchas ocasiones sacrificar algo para obtener o lograr otra satisfacción. GRACIAS por darme ánimos con tus palabras siempre de aliento para la culminación de este trabajo, el cual lleva implícita mi carrera.

"TE ADORO MAMÁ"

A MIS QUERIDOS Y APRECIADOS HERMANOS

HILDA REYNA LUCIO

(A QUIEN ADMIRO Y RESPETO)

Liliana realmente no encuentro palabras para describir todo el agradecimiento que tengo hacia ti, más sin embargo en esta página quiero dejar constancia de tu invaluable apoyo recibido para la culminación de mi carrera y para la realización del presente trabajo, agradeciéndote las horas, días, meses y años dedicados a la familia, por haber sacrificado más que tu tiempo, por tus orientaciones y por tú paciencia a lo largo de mi vida. Tu presencia en mi vida ha sido, es y será indispensable, sin tu apoyo ningún proyecto familiar hubiese sido posible, caminaste al lado de mi padre hasta llegar a ser un pilar en su vida, nunca dudes cuanto te amamos y queremos.

"GRACIAS FLAQUITA"

ADALBERTO REYNA LUCIO

(ERES DUEÑO DE UN GRAN CORAZÓN, CUÍDALO)

Adal sabes que te estimo y que admiro tu fuerza de voluntad y de determinación para hacer las cosas, además de tú diligencia para ello, tal y como nuestro padre era. Eres una persona segura con mucha decisión, eres el más chico de nuestra verdadera familia pero el más maduro en la forma de pensar. GRACIAS por hacerme ver mis debilidades y algunos de mis errores a tiempo, por tolerarme desde mi infancia pues hemos compartido muchas penas y alegrías; y finalmente te agradezco tu gran apoyo para la culminación de este trabajo

"GRACIAS POR SER UNA PERSONA EXTRAORDINARIA"

ARACELI REYNA LUCIO

(CONSERVA LA ALEGRÍA QUE SIEMPRE TE HA CARACTERIZADO)

Eres una persona con grandes cualidades, entre ellas está tu carisma hacia la gente. Gracias por ser mi hermana, por haberme brindado más que palabras de aliento para concluir este trabajo y por apoyarme en muchas cosas mientras estuve en E.U.

A MIS SOBRINOS CESAR Y KELLYN ROSELINE, como testimonio del cariño que les tengo por ser parte de mi familia.

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, AL COLEGIO DE CIENCIAS Y HUMANIDADES AZCAPOTZALCO Y A LA FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN. Por ser mí segunda casa en cuyo seno he podido forjarme profesionalmente, en ellas aprendí el valor de la palabra escrita, gracias por brindarme la oportunidad de progresar en el largo camino de la vida.

A TODOS ELLOS LO QUE NO PUDE O NO SUPE EXPRESAR SE RESUME EN UNA SOLA PALABRA "GRACIAS".

HIMNO DE LA UNAM CAMPUS ARAGÓN

En el horizonte
Se agita majestuoso y esplendente
el emblema hermoso…
de mi Universidad

Universidad Nacional
Autónoma de México
tienes en tu emblema
dos símbolos de libertad.

Máxima ilusión del hombre
es mi Universidad
Crisol del ser humano…
es mi Universidad.
Síntesis de amor y bondad
es mi Universidad
Templo sagrado del saber…
es mi Universidad

Como una flor en el desierto...
Así eres tú Campus Aragón
Como un lucero en la obscuridad...
Así eres tú Campus Aragón
Como un oasis salvador
Así eres tú Campus Aragón
Como un camino a mi libertad…
Así eres tú… Campus Aragón.

Campus Aragón…
Campus Aragón…
Campus Aragón…
de la Universidad Nacional
Autónoma de México

Universidad Nacional
Autónoma de México
te llevo en mi corazón
jamás te podré olvidar

Tú me has permitido
extender mis alas y volar
a través del tiempo
luchando por mi libertad

Campus Aragón…
Campus Aragón…
Campus Aragón…
de la Universidad Nacional
Autónoma de México

Máxima ilusión del hombre
es mi Universidad
crisol del ser humano
es mi Universidad.
síntesis de amor y bondad
es mi Universidad
Templo sagrado del saber…
es mi Universidad

Campus Aragón…
Campus Aragón…
Campus Aragón…
de la Universidad Nacional
Autónoma de México…

LIC. GAUDELIO GARCÍA ESTRADA.

DECÁLOGO DEL ABOGADO

***1º ESTUDIA:** El derecho se transforma constantemente, si no sigues sus pasos, serás cada día un poco menos abogado.*

***2º PIENSA:** El derecho se aprende estudiando pero se ejerce pensando.*

***3º LUCHA:** Tu Deber es luchar por el derecho, pero el día en que encuentres en conflicto el derecho con la justicia, lucha por la justicia.*

***4º TRABAJA:** La abogacía es una fatiga puesta al servicio de la justicia.*

***5º SE LEAL:** Leal para con tu cliente, al que no debes abandonar hasta que comprendas que es indigno de ti. Leal para con el adversario, aún cuando él sea desleal contigo. Leal para con el Juez que ignora los hechos y debe confiar en lo que tú dices; y que, en cuento al derecho alguna que otra vez debe confiar en el que tú le invocas.*

***6º TOLERA:** Tolera la verdad ajena en la misma medida en que quieres que sea tolerada la tuya.*

***7º TEN PACIENCIA:** En el derecho, el tiempo se venga de las cosas que se hacen sin su colaboración.*

***8º TEN FE:** Ten fe en el derecho, como el mejor instrumento para la convivencia humana; en la justicia, como destino normal del derecho; en la paz como sustituto bondadoso de la justicia; y sobre todo ten fe en la libertad, sin la cual no hay derecho, ni justicia, ni paz.*

***9º OLVIDA:** La abogacía es una lucha de pasiones; si en cada batalla fueres cargando tu alma de rencor, llegará un día en que la vida será imposible para ti. Concluido el combate, olvida tan pronto tu victoria como tu derrota.*

***10º AMA TU PROFESIÓN:** Trata de considerar la abogacía de tal manera, que el día en que tu hijo te pida consejo sobre su destino, consideres un honor proponerle que sea abogado.*

ÍNDICE

“LOS MEDIOS INFORMÁTICOS COMO AGRAVANTE DEL DELITO DE FRAUDE”

INTRODUCCIÓN. I

Capítulo 1.- Generalidades. 1

1. 1.- La informática y los medios informáticos. 1

1. 2.- El fraude como un delito informático (Fraude Informático). 8

1. 3.- Sujeto activo y sujeto pasivo en el fraude informático. 13

1. 4.- Programas, métodos y técnicas por medio de los cuales se puede llevar cabo el fraude informático. 16

1. 5.- Situación internacional del fraude informático. 24

Capítulo 2.- El fraude informático en México. 29

2. 1.- Protección jurídica que brinda el derecho mexicano contra el fraude informático. 29

2. 2.- El principio de legalidad, la garantía de seguridad jurídica y el fraude informático. 35

2. 3.- Las tres principales formas como se ha manifestado el fraude informático en México. 37

2. 3. 1.- El fraude informático en el sistema bancario y en las tarjetas de crédito o débito. 37

2. 3. 2.- El fraude informático en la obtención de datos personales y su problemática. 40

2. 3. 3.- El fraude informático en las subastas electrónicas. 42

Conclusiones. 44

Glosario. 46

Fuentes consultadas. 51

INTRODUCCIÓN

En el presente trabajo haremos un estudio sobre el delito de Fraude, estudiando específicamente la forma en que se realiza, mediante el empleo de medios electrónicos y maniobras informáticas (fraude informático). Teniendo como fin primordial de nuestra investigación, precisar si es necesario que la descripción típica siga en los mismos términos en que ha sido plasmada por el legislador, si es necesario efectuar algunas modificaciones al texto legal, o si existe la necesidad de tipificarlo como un nuevo delito.

El desarrollo de la tecnología informática ha abierto las puertas a nuevas formas o conductas para delinquir, tales como la manipulación fraudulenta de los ordenadores, la destrucción de programas, y el acceso o la utilización indebida de la información que puede afectar la esfera de la privacidad; dichas conductas a la vez forman parte del procesamiento electrónico de datos, mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales y morales. Se trata de una delincuencia realizada muchas veces por especialistas capaces de efectuar el delito y de borrar toda huella de los hechos. Por lo tanto la informática puede ser el medio idóneo para la comisión de distintos delitos, en especial de carácter patrimonial, ya que reúne una gran cantidad de datos y proporciona la facilidad de acceso y manipulación de los mismos mediante el empleo de medios o técnicas informáticas

Al inicio de la presente investigación analizáremos cómo los medios informáticos responden a las nuevas necesidades de la comunicación humana, toda vez que proporcionan nuevas formas de transmitir y recibir información, es decir veremos como el progreso de la tecnología permite en la actualidad procesar todo tipo de información (ya sea en el ámbito científico, el técnico, el profesional o personal), y además ponerla a disposición de la sociedad, tomando en cuenta que las computadoras forman parte de los medios informáticos y son un medio eficaz para obtener y dar a conocer mucha información, ese enorme caudal de información puede obtenerse en segundos o minutos, transmitirse incluso documentalmente, gracias a la informática (tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos). Más adelante observaremos como la

informática está hoy presente en casi todos los campos de la vida moderna y como ha provocado un cambio tanto en nuestra forma de pensar como de hacer las cosas. Correlacionando todo lo anterior con la definición de delito informático trataremos de explicar a la vez, porque en el desarrollo del presente trabajo se emplea la expresión de Fraude Informático para referirnos a las conductas anteriormente señaladas, mismas que se originan al utilizar con malicia los medios informáticos. Indicaremos algunas de las denominaciones que se le han dado a los sujetos que usan dicha tecnología para delinquir; además apreciaremos los programas, métodos y técnicas por medio de los cuales se puede llevar a cabo el fraude informático. Posteriormente veremos como La Organización de Naciones Unidas (ONU) ha reconocido al fraude informático como un delito y al mismo tiempo puntualizáremos como el crecimiento de la tecnología ha llevado, en un nivel internacional, a los juzgadores a revalorar los tipos penales ya existentes, a efecto de determinar en cuál tipo penal encuadra determinada conducta, siempre relacionada con los avances informáticos, o bien a formular un nuevo tipo penal para ésta clase de delito.

En el capítulo II se pretende establecer si existe un bien jurídico tutelado específico o si se trata simplemente de una nueva forma de comisión de conductas delictivas, ya tipificadas por los ordenamientos penales existentes. Principalmente con un enfoque en nuestro país, conoceremos los perjuicios ocasionados por no tomar en cuenta jurídicamente las manipulaciones efectuadas a los sistemas informatizados, las cuales son empleadas para cometer el delito de Fraude mediante el uso de medios informáticos; además analizaremos la protección jurídica que el derecho mexicano nos brinda ante la figura del fraude informático, observando el principio de legalidad y la garantía de seguridad jurídica. Continuaremos con las principales formas en las que se ha manifestado dicho fraude en nuestro país, observando en este punto, como el fraude realizado a través de los medios informáticos es capaz de producir grandes perjuicios económicos en el patrimonio de las personas, al ejecutarse de una manera muy sofisticada en todo el sistema bancario, incluyendo los mecanismos de pago más comunes, es decir las tarjetas de crédito o débito; conoceremos las técnicas empleadas para poder obtener los datos personales, los cuales pueden utilizarse para cometer aún más fraudes, y para finalizar estudiaremos al fraude informático en las subastas electrónicas.

CAPÍTULO 1. GENERALIDADES

En este capítulo apreciaremos el motivo por el cual se añade el término de informático al delito de fraude, con el fin de explicar porqué en el desarrollo del presente trabajo se emplea la expresión de Fraude Informático, para señalar a las conductas que hacen uso de los medios informáticos para realizar o llevar a cabo el delito de fraude; al manipular la información en cualquier etapa de su procesamiento. Al mismo tiempo se incluirá la importancia que tienen dichos medios en la expansión de la información y el conocimiento.

1. 1 LA INFORMÁTICA Y LOS MEDIOS INFORMÁTICOS

El hombre siempre ha tenido la necesidad de comunicarse con los demás para expresar sus pensamientos, ideas y emociones, lo cual ha implicado al mismo tiempo la necesidad de buscar, de saber y de obtener información creada y transmitida por otros. Por lo tanto podemos definir a la comunicación como la transferencia de información de un lugar a otro, y a la información la podríamos considerar como todo mensaje que logra disminuir la incertidumbre y que permite adquirir cualquier tipo de conocimiento.

La búsqueda constante del hombre para satisfacer dicha necesidad de comunicación ha sido el motivo para la creación de instrumentos cada día más sofisticados y veloces, traduciéndose éstos en nuevas y mejores tecnologías para comunicarse entre sí; en otras palabras dicha búsqueda ha dado lugar a la creación de la Informática, la cual combina los aspectos teóricos y prácticos de la ingeniería en electrónica, de la teoría de la información, de las matemáticas, de la lógica y del comportamiento humano.

La palabra informática proviene del francés informatique, término sugerido por el ingeniero Philippe Dreyfus en 1962, formado por la conjunción de las palabras information (información) y automatique (automatización). En sentido general se define a la informática como el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores. En esta disciplina se estudia el tratamiento automático (creación, procesamiento, almacenamiento y transmisión), de la información (datos), utilizando ordenadores electrónicos, es

decir estudia lo que los programas son capaces de hacer (teoría de la computabilidad), la eficiencia de los algoritmos que se emplean (complejidad y algorítmica), la organización y el almacenamiento de datos (la estructura y las bases de datos) y la comunicación entre programas, humanos y máquinas (interfaces de usuario, lenguajes de programación, procesadores de lenguajes, etcétera). Nava Garcés nos dice que "Su campo cubre los sistemas de información, la forma en que ésta se elabora, transmite y utiliza." [1] En resumidas palabras la informática abarca desde la programación hasta la inteligencia artificial y la robótica.

Esta disciplina hoy en día está presente en casi todas las ramas del conocimiento humano, la podemos apreciar en: transacciones comerciales, en las comunicaciones masivas, en los procesos industriales, en la investigación científica, en la seguridad, en la educación e incluso en el ocio, de ahí la importancia que tiene la misma para el desarrollo y progreso de un país en todos sus aspectos. Tan solo para podernos darnos cuenta de la presencia e importancia que tiene la informática en la vida humana mencionaremos algunos ejemplos:

1.- Supongamos que estamos en la calle y tenemos que hacer una llamada telefónica urgente, y nuestro teléfono celular no tiene suficiente corriente o crédito. Todo parece ser muy fácil: localizamos un teléfono público, sacamos una tarjeta telefónica, la introducimos en él, marcamos y listo. Lo que en realidad sucede es que ponemos a trabajar y a comunicarse entre sí a un buen número de microchips (dispositivo informático integrado por millones de circuitos microscópicos), tanto el que lleva el registro de tu dinero en la tarjeta, como el que procesa el número telefónico al que marcas y que va descontando el dinero de tu tarjeta, el de la central telefónica que enruta la llamada y, finalmente, el del teléfono de la persona que estamos llamando. Sin darnos cuenta, consultamos el reloj para ver si llegaremos a tiempo al supermercado; nos subimos al coche (en uno de modelo reciente al menos dos computadoras se ponen en acción: una que controla al motor y otra al sistema eléctrico; son ellas las que nos avisan a través del tablero que hace falta gasolina, líquido de frenos, aceite, o los desperfectos en el sistema eléctrico); en la ruta al supermercado nos encontramos con un semáforo que cambia a luz verde, esto

[1] NAVA GARCÉS, Alberto Enrique. Análisis de los Delitos Informáticos, Porrúa, México, 2005, p. 15.

es porque seguramente cuentan con un sistema automatizado que controla la duración de las luces; Por fin llegamos en diez minutos al supermercado, pero no es solamente una tienda de autoservicio, es también una jungla de informática. Tomamos una caja de cereal y, vemos en ella un código de barras (que es algo así como el alfabeto que pueden leer las computadoras) que sirve para que cuando vayamos a pagar, la caja registradora sepa cuál es el precio correcto; llegó la hora de pagar el cereal, sacamos la tarjeta de crédito o débito, la cual en su parte de atrás tiene una banda magnética en la que se almacenan nuestros datos de identificación, misma que la cajera pasa por un lector que los lleva hasta la institución bancaria por medio de telecomunicaciones, en donde el pago es aprobado; y con la aprobación de nuestra compra empiezan otros procesos informáticos; como por ejemplo al haber utilizado nuestra tarjeta para pagar se genera una transacción económica en donde se descontará de nuestra cuenta bancaria el monto de nuestra compra, esa caja de cereal que adquirimos se reporta en el inventario de la tienda como artículo vendido que necesita ser repuesto y se agrega en la base de órdenes de compras, la cual más adelante es enviada por medios informáticos al distribuidor para que surta otra caja de cereal. Tanto en el reloj como en las tarjetas (telefónicas, de crédito o de débito), en las computadoras del automóvil, en los semáforos y en las modernas cajas registradoras, está presente de manera silenciosa la informática ya que contienen cientos de circuitos impresos en un chip que hacen que funcionen para desempeñar un fin determinado, al efectuar la actividad para la cual fueron creados y programados.

2.- La televisión y videocasetera pueden programarse para grabar un programa o apagarse a determinada hora gracias a que contienen aditamentos informáticos. Un aparato de sonido puede grabar la ubicación de varias estaciones de radio en su memoria o recordar el orden para escuchar las canciones de un disco compacto, también porque cuentan con chips. Los mismos discos compactos no son otra cosa que medios informáticos en los que se encuentran grabadas las canciones en forma de archivos digitales. Los videojuegos que conectamos a la televisión como el Nintendo, el Play Station, o el XBOX, son verdaderas computadoras disfrazadas de electrodoméstico, capaces de interpretar millones de instrucciones por segundo para que podamos ganar ese juego virtual.

3.- La Informática jurídica, la cual es una técnica interdisciplinaria que estudia e investiga el tratamiento lógico y automático de la información legal, y la utilización de aparatos o elementos físicos electrónicos en el Derecho; en otras palabras, es el conjunto de medios e instrumentos informáticos que ayudan al derecho para su mejor aplicación, entre ellos podemos encontrar a los programas que utilizamos como abogados para poder ser más eficientes en nuestro trabajo, en síntesis es el uso de la informática en el derecho.

4.- En el manejo de grandes volúmenes de datos, como al tratar de encontrar el historial de un paciente en un fichero con otros 600.000 pacientes, manipular la información sobre los fondos bibliográficos de una biblioteca (miles de libros), guardar el registro de habitantes de una gran ciudad, guardar el registro de los criminales de un país, y poder disponer de la información sobre uno de ellos en cuestión de segundos sería muy difícil, puesto que la cantidad de información que se debe gestionar diariamente es abismal; Las bases de datos junto con las altas capacidades de procesar la información que nos proporciona esta disciplina nos permiten afrontar el reto

Como podemos apreciar, la informática está presente en muchas actividades del hombre, y no sólo en aquéllas directamente relacionadas a una computadora. De esta manera queda claro que el uso de la informática es en ocasiones indispensable y hasta conveniente, sin embargo, junto a las incuestionables ventajas que ésta representa, han comenzado a surgir algunos inconvenientes negativos que han dado lugar a una nueva forma de delincuencia, debido a que esta tecnología pone a disposición del delincuente los medios informáticos necesarios para alcanzar sus propósitos criminales.

Los medios informáticos incluyen a todos los aparatos, máquinas, artefactos, dispositivos, herramientas, programas, circuitos integrados (chips o microchips) y sistemas, asociados al tratamiento automático de la información; La palabra medio se emplea para referirnos a aquella cosa que puede servir para un determinado fin, en este caso a la informática, por lo tanto podemos decir que un medio informático es todo aquello que sirve para que la informática cumpla con sus fines. De tal manera que los medios informáticos se relacionan directamente con los equipos de cómputo y todos sus aditamentos o accesorios.

Cuando hablamos de los accesorios ó aditamentos nos referimos a los dispositivos complementarios de un ordenador o computadora, como una impresora, un módem, un escáner, un teléfono o una cámara web. El accesorio ofrece una funcionalidad que no está disponible en la máquina original y que no es necesaria para el funcionamiento de la misma, no obstante, el accesorio puede resultar imprescindible para determinadas tareas; por ejemplo, un módem en la actualidad es indispensable para conectarse a Internet.

Como ya hemos mencionado la Informática combina los aspectos teóricos y prácticos de la ingeniería y de la electrónica, es por ello que consideramos pertinente dar la siguiente definición; La electrónica es el campo de la ingeniería y de la física aplicada tanto al diseño como al uso de dispositivos, por lo general circuitos electrónicos, cuyo funcionamiento depende del flujo de electrones para la generación, transmisión, recepción y almacenamiento de información. Esta información puede consistir en:

1.- Señales de audio: Voz o música en un receptor de radio o en el teléfono.
2.- Señales de video: Una imagen en una pantalla de televisión o un monitor.
3.- Números, letras, signos u otros datos en un ordenador o computadora.

Para la finalidad de nuestro trabajo nos avocaremos a aquellos medios informáticos en los cuales el avance de la tecnología en electrónica se ha implementado aun más; a continuación pasaremos a una sencilla descripción de algunos de estos medios:

El teléfono es un instrumento de comunicación, diseñado principalmente para la transmisión de voz y demás sonidos hasta lugares remotos mediante la electricidad. El teléfono contiene un micrófono (transmisor) que recibe el impacto de las ondas de sonido (vibraciones) transformándolas en impulsos eléctricos, la corriente eléctrica así generada se transmite a distancia, y un altavoz (receptor) vuelve a convertir la señal eléctrica en sonido; en la actualidad el teléfono permite enviar no sólo señales de audio, sino también datos de imágenes o cualquier otro tipo de información que pueda codificarse y convertirse en señal, la cual puede transmitirse inclusive por microondas (ondas de radio), fibra óptica o vía satélite utilizando una señal digital que viaja entre los distintos puntos conectados a la red de interconexión (en este lapso es

donde puede ser interceptada), permitiendo así el acceso directo a múltiples servicios, como el videoteléfono, mensajes de texto y. el correo de voz.

Un módem es un equipo utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de voz o datos; permite entre otros servicios, acceder a una base de datos, transferir ficheros y enviar o recibir un correo electrónico. El módem convierte las señales digitales moduladas del emisor en otras analógicas (señales demoduladas), susceptibles de ser enviadas por la línea de teléfono, a la cual deben estar conectados el emisor y el receptor. Cuando la señal llega a su destino, otro módem se encarga de reconstruir la señal demodulada a digital, de cuyo proceso se encarga la computadora receptora. En la actualidad los módems son capaces de trabajar con diversas velocidades de emisión y recepción de datos. Los módems pueden ser externos (estos tiene que estar conectados al dispositivo emisor mediante un cable), o internos (tarjeta módem).

El ordenador o computadora puede ser definido como un dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otro tipo de información. Indiscutiblemente, las computadoras han invadido ya todos y cada uno de los campos de la actividad humana: ciencia, tecnología, arte, educación, recreación, administración, economía y de acuerdo a la tendencia actual, nuestra civilización y las venideras dependerán cada vez más de estos cerebros electrónicos. La computadora es la herramienta informática más versátil que hay: un mismo equipo puede servir tanto para escuchar un disco compacto como para controlar las funciones de un satélite o clasificar a los componentes del genoma humano. Esa es su fortaleza, pero también es su debilidad, porque para soportar tan amplia versatilidad, las computadoras deben incluir sistemas operativos, (conjunto básico de programas sin el cual nada en ella funcionaría), y contar con muchos aditamentos, como la tarjeta de sonido, las bocinas, la tarjeta de vídeo, la impresora, el escáner, etcétera; lo cual da como resultado una máquina costosa y más difícil de usar para la mayoría de las personas. En la actualidad son innumerables los beneficios que brindan las computadoras, entre ellos podemos mencionar la rapidez en la obtención de resultados, el almacenamiento de grandes volúmenes de información, las facilidades para obtener información

adecuada y actualizada por parte de científicos, investigadores, profesionales, o estudiantes; Las computadoras tienen un sinfín de aplicaciones, lo que las ubica como una técnica idónea para la comunicación, han introducido una nueva cultura en nuestro tiempo, incluso ha llegado a considerárseles como el primer motor de desarrollo económico del mundo; forman parte de las nuevas tecnologías que se están introduciendo continuamente a la vida moderna, reemplazando a otras del mismo tipo en muy poco tiempo; y de manera muy especial se debe destacar que el desarrollo de las computadoras está condicionado a la informática.

La utilización de los medios informáticos trae inconvenientes en relación con la identidad y la autenticidad de las personas que los emplean, además si a esto le sumamos que aun no existe un programa del todo seguro para proteger la información contenida en ellos y que para emplear cualquier medio de este tipo, es necesario contar con conocimientos mínimos del medio a utilizar, es por ello que los medios informáticos han causado una sensación de desconfianza por parte de los usuarios, quienes en definitiva, acaban asumiendo estas nuevas herramientas como una carga, más que una ventaja.

En síntesis podemos decir que la informática proporciona los medios informáticos necesarios para realizar un gran número de fraudes, tales como; hacerse ilícitamente del patrimonio ajeno a través de la información contenida en las tarjetas bancarias, la vulneración y alteración de los sistemas de cómputo para recibir servicios, las transferencias electrónicas de fondos mediante la manipulación de programas y la interceptación de las comunicaciones para obtener datos personales. En este punto es prudente enfatizar que aún cuando el espacio en el que se efectúa la operación es virtual tanto la conducta de los delincuentes como los daños, desilusiones, perjuicios y otras consecuencias que se pueden generar son reales y pueden representar incuantificables pérdidas económicas para quienes sean defraudados, afectando de esta forma el patrimonio de la víctima.

Con todo lo anterior nos podemos dar cuenta de la importancia y prioridad que amerita regular mediante normas vigentes las conductas delictivas que nacen por el mal uso de los medios informáticos, ya que estamos hablando de la protección jurídica para las presentes y futuras generaciones.

1. 2 EL FRAUDE COMO UN DELITO INFORMÁTICO (FRAUDE INFORMÁTICO)

En el presente tema se dará la noción de lo que se entiende por un delito de carácter informático, y su relación con el fraude. A continuación proporcionaremos los conceptos de delito y delito informático:

Para Moto Salazar: “El delito en *Latu Sensu* se produce dentro de la sociedad; mirándolo objetivamente se presenta como un hecho social dañoso, puesto que destruye la convivencia pacífica de los individuos; la convivencia está protegida y ordenada por la ley en consecuencia el delito, al afectar y atacar los vínculos de solidaridad, implica una violación a la propia ley, de ahí que sea un hecho ilícito. En *Strictu Sensu* es el acto culpable, antisocial e ilícito, sancionado por la ley penal.” [2] Y de acuerdo al artículo séptimo del Código Penal Federal el delito es el acto u omisión que sancionan las leyes penales. Por lo tanto al expresarnos en términos jurídicos, para que exista delito es necesario que el acto u omisión sea sancionado por las leyes penales, ya que una de las características indispensables del delito es la tipicidad, es decir, que la conducta esté descrita en un tipo penal, en una ley penal, además de ser antijurídica, culpable, y punible.

En cuanto a los delitos informáticos, el autor mexicano Julio Téllez Valdés señala que dar un concepto sobre ellos no es una labor fácil, toda vez que su misma denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas o tipificadas, es decir, contemplados en textos jurídicos penales, se requiere que la expresión delitos informáticos este consignada en los códigos penales, lo cual en la mayoría de los países no ha sucedido aún. Es por ello que para efectos de una conceptuación hace la siguiente distinción: “los delitos informáticos son actitudes contrarias a los intereses de las personas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico).” [3]

---

[2] MOTO SALAZAR, Efraín. Elementos del Derecho, 44ª Edición, Porrúa, México, 1998, p. 308.

[3] TÉLLEZ VALDÉS, Julio. Derecho Informático, 3ª Edición, Mc Graw Hill, México, 2005, p. 163.

Por lo tanto podríamos decir que los delitos informáticos comprenden cualquier comportamiento criminal, en el cual la computadora ha estado involucrada de alguna de las siguientes maneras: 1.- Como **instrumento**, donde se valen de las computadoras como un medio para la comisión del delito, tal y como lo es el uso no autorizado del *software*, la apropiación ó modificación indebida de datos, las intercepciones de transferencias electrónicas, el robo de tiempo de computadora, la alteración en el funcionamiento de los sistemas, el método del caballo de Troya, la técnica del Salami, etc.; 2.- Como **fin**, es decir como objetivo, aquí las conductas criminológicas van dirigidas en contra de las computadoras, sus accesorios o programas como entidad física, por ejemplo causar daños físicos a la memoria.

El Código Penal Para el Estado de Sinaloa, nos proporciona un adelanto en materia informática, al tipificar en su Título Décimo (Delitos Contra El Patrimonio), Capítulo V, al Delito Informático, de la siguiente forma;

> Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:
> I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o
> II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.
> Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

No está por demás señalar, que este artículo es un excelente punto de partida para la futura y posible reglamentación informática a nivel federal, ya que aunque no lo expresa literalmente se sobreentiende que para poder ejecutar las conductas aquí señaladas, se debe hacer uso de algún medio informático. Además debemos enfatizar que mejor un grupo de legisladores a

nivel estatal se ha preocupado por regular los delitos en comento, en lugar de que fuese una propuesta por parte de los legisladores a nivel federal, a pesar del gran riesgo que se corre con este tipo de delitos.

Ahora bien la palabra **fraude** "proviene del latín *fraus*, *udis, fraudis*, que significa engañar, usurpar, despojar, burlar; *fraudulentus*, equivalente a fraudulento, engañoso, fingido, falaz, malicioso. Gramaticalmente es engaño o acción contraria a la verdad o rectitud".[4]

De tal forma que podríamos entender al fraude como una de las maneras más antiguas de conseguir beneficios mediante la utilización de la inteligencia y creatividad del ser humano.

Moto Salazar en su libro Elementos del Derecho define al fraude como: "El engaño que se hace a una persona aprovechándose del error en que ésta se halla para apoderarse ilícitamente de una cosa u obtener un lucro indebido."[5]

En el ámbito del derecho penal es donde tiene mayor cabida este vocablo, toda vez que es considerado como un delito, como lo podemos observar en el artículo 386 del Código Penal Federal, el cual expresa lo siguiente:

> Artículo 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…

Al comparar el tipo penal federal del delito de fraude, con el concepto proporcionado por el autor Moto Salazar, apreciamos la similitud indiscutible de ambos, al señalar que se hace ilícitamente de alguna cosa, se hace alusión no solamente a una prestación económica, sino también a toda información (datos) o la prestación de algún servicio como lo es el servicio telefónico, el de paquetería, etc.; ahora bien en el Código Penal Para El Distrito Federal, se

---

[4] BIBLIOTECA DE CONSULTA MICROSOFT. Encarta 2004, Edición 1993-2003, disco compacto, Microsoft Corporation, México, 2004.

[5] MOTO SALAZAR, Efraín. *op. cit*. p. 333.

denota a diferencia de los anteriores que el beneficio puede ser propio o para un tercero, tal y como lo expresa el Título Décimo Quinto (Delitos Contra El Patrimonio), Capítulo III (Fraude), en el siguiente artículo:

> Artículo 230 del Código Penal Para El Distrito Federal.- Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, se le impondrán…

La doctrina considera que tanto el engaño como el aprovechamiento de error (características primordiales de la conducta del sujeto activo del Delito de Fraude) no pueden dirigirse contra las máquinas, al carecer éstas de discernimiento (juicio y criterio de decisión), y toda vez que se limitan a ejecutar las conductas para las que fueron pre programadas. En este punto debe hacerse notar lo siguiente:

- Si bien es cierto que no puede existir engaño sobre una máquina, pero ésta sí puede ser objeto de manipulación en los programas y provocar así un mal hacia el usuario y su patrimonio.
- En realidad la máquina solo está siendo el medio para transmitir y recibir la conducta o voluntad del usuario, en este caso del sujeto activo.
- Los medios informáticos deben provocar el error o aprovechar el error ya existente mediante la actividad fraudulenta.
- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.

Con lo anterior podemos observar que la humanidad no está frente al peligro de la informática, sino mas bien frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa tener el conocimiento; ya que estos individuos aprovechan el avance de la tecnología y su conocimiento personal para poder delinquir, mediante el uso de los medios informáticos (Incorporando de esta forma a la informática como herramienta de comisión), provocando con ello un perjuicio en el patrimonio de las personas.

Al reunir el concepto de delito informático y el concepto legal del delito de fraude anteriormente señalados, podemos definir al fraude informático como la acción de manipular la información de un sistema informático, en cualquier etapa de su procesamiento, empleando algún medio informático para engañar u aprovechar así un error del propietario o usuario y con el fin de obtener ilícitamente cualquier tipo de beneficio, en provecho propio o para un tercero.

Romeo Casabona define al fraude informático de la siguiente manera; "es la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de un tercero." [6] Con esta definición podemos reafirmar que la conducta del sujeto activo va encaminada a la modificación de la información en cualquier etapa de su procesamiento.

Los perjuicios ocasionados mediante este fraude pueden acumular grandes sumas de dinero, afectando de esta manera el patrimonio de las personas físicas o morales. Por lo tanto es de suma importancia que se penalice este tipo de acciones, podríamos argumentar que mientras no haya un claro panorama sobre los delitos informáticos de acuerdo con los avances tecnológicos que hoy en día tenemos en el mundo y que involucran a la sociedad mexicana, no habrá una buena regulación de los mismos, provocando que México sea blanco fácil de cualquier ataque de esta índole, de tal modo que la criminalidad informática constituye un reto considerable para los legisladores y para las autoridades policiales encargadas de su investigación.

En síntesis en el presente trabajo utilizamos la denominación de Fraude Informático para referirnos a aquellas conductas ilícitas que hacen uso de los medios informáticos para llevar a cabo el delito de fraude, al manipular la información en cualquier etapa de su procesamiento, es decir tanto en la entrada (generación, creación), como en el almacenamiento (archivada en la memoria del ordenador) y en la salida (transmisión) de la información (datos).

---

[6] ROMEO CASABONA, Carlos María. El Poder Informático y Seguridad Jurídica, Fundesco, Madrid España, 2002, p. 89.

1. 3 SUJETO ACTIVO Y SUJETO PASIVO EN EL FRAUDE INFORMÁTICO

SUJETO ACTIVO

En resumidas palabras podemos decir que es aquella persona que realiza o lleva a cabo el Fraude Informático, la cual posee ciertas características, entre ellas podemos mencionar las siguientes:

1.- Poseen importantes conocimientos de informática, este tipo de personas tienen habilidades para el manejo de los sistemas informáticos.

2.- Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible y cuentan con el acceso al sistema que posee dicha información, o bien no necesariamente desarrollan actividades laborales, pero poseen gran destreza para sobrepasar la protección de dicha información.

3.- Se les ha considerado personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico, además de que se piensa que poseen un cierto status socioeconómico. Por lo tanto no es fácil descubrirlos ni sancionarlos, en razón del poder económico que ostentan.

4.- Poseen el síndrome de *Robín Hood*, porque consideran que hacen justicia al defraudar las grandes organizaciones financieras y por ello no consideran inmoral sus actos delictivos, pues creen que no les han hecho daño a las demás personas, de esta forma algunos obtienen cierta simpatía por parte de la opinión pública.

Al sujeto que comete este tipo de conducta no se le considera un delincuente ordinario, ya que no se le relega, desprecia o desvaloriza; por el contrario, es considerado y se considera a sí mismo, como una persona respetable. Se trata de personas que se conectan a las máquinas mediante programas, tomando el control de los mismos o interceptan sus procesos de comunicación, permitiendo así una actuación transnacional, y generando al mismo tiempo conflictos de jurisdicción y de legislación que ello implica. Con el paso del tiempo se ha podido comprobar que los autores son muy diversos, debido al modus operandi de cada uno.

Podemos encontrarnos con diferentes calificativos para definir a estas personas, los cuales dependerán tanto de los métodos empleados para atacar a los sistemas como de los efectos causados por dichos ataques, por ejemplo:

Hacker.- Este término se utiliza para identificar a la persona que se introduce en un sistema protegido sin tener autorización, como si se tratara de un reto personal, sin intentar causar daños; no son conscientes de la gravedad y el peligro de sus actos puesto que consideran sus acciones como un juego.

Cracker.- Tiene como principal objetivo al introducirse a un sistema, producir daños que en muchos casos suponen un problema de extrema gravedad para el administrador del sistema, claramente cuentan con conocimientos informáticos para robar información sensible o difundir programas indeseables, en provecho propio, es decir para lograr sus objetivos

Phreaker.- Poseen conocimientos profundos de los sistemas de telefonía, buscan burlar la obligatoriedad del pago por servicio, mediante la construcción de equipos electrónicos artesanales que incluso pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares, sin que el titular se percate de ello debido a que en la actualidad casi todas las redes de telefonía son soportadas y administradas desde sistemas computarizados.

El sujeto activo modifica, sustrae, o destruye la información contenida en los equipos informáticos, e incluso daña los sistemas informáticos de programación con diferentes fines, como por ejemplo para vengarse de un despido con la esperanza de que una vez probada su pericia tecnológica sea contratado en la empresa víctima del ataque; porque la empresa rival le ha pagado para infiltrar un virus y tirar la página Web del competidor (denegación del servicio) u obtener sus secretos industriales; y otros muchos, incluso la pura amenaza de soltar un virus puede ser una forma de extorsión muy lucrativa.

Todos estos sujetos son un grave problema público, puesto que utilizan inadecuadamente las grandes posibilidades que nos ofrece una tecnología como la informática; además las posibilidades tecnológicas son muchas y cambian frecuentemente, lo cual trae como consecuencia que las modalidades del fraude y el calificativo de sus autores aumenten día a día.

SUJETO PASIVO

Es el ente sobre el cual recae la conducta que realiza el sujeto activo, puede ser cualquier persona en particular, instituciones financieras y sus clientes, instituciones militares, órganos de gobierno, etc.; que usen de cualquier forma sistemas automatizados de información, generalmente conectados a otros. Tratándose de Instituciones Financieras, deberían ser éstas las que sufran el perjuicio patrimonial, toda vez que en su calidad de depositaria, debería restituir el importe de lo defraudado a sus clientes, lo cual en realidad no sucede, siendo estos últimos los que asumen dicho perjuicio. Resultando el sujeto pasivo el titular de los bienes, valores o derechos.

Aquellas personas que no poseen los conocimientos informáticos básicos (por lo general personas de escasos recursos económicos, por escases de tiempo o por falta de interés en el tema.), son más vulnerables a ser víctimas de este delito; ya que pueden ser engañadas, si en un momento dado tienen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de dichas tecnologías como el Internet, el correo electrónico, etc.

De acuerdo con Gabriel Andrés Cámpoli, “este tipo de delitos genera un nuevo grupo de víctimas: aquellas que no son consientes de los ataques a su privacidad o intimidad” [7], al citar como ejemplo la reciente venta de la base de datos del Instituto Federal Electoral que recoge como víctimas al menos a 58 millones de mexicanos que han visto vulnerada su privacidad.

Por medio de la víctima (sujeto pasivo) podemos conocer las diferentes causas que favorecen la ejecución del fraude informático, como el error de no proteger sus equipos de cómputo e información con un programa adecuado, ya sea por la falta de conocimiento sobre ello, o por olvidar instalar dicho programa. Para concluir este tema debemos enfatizar que el fraude informático es uno de los fenómenos más importantes dentro de la delincuencia informática, ya que es una de las zonas más inexploradas y la de mayor problema en cuanto a su prevención, detección y represión.

[7] CÁMPOLI, Gabriel Andrés. Delitos Informáticos en la Legislación Mexicana, Instituto Nacional de Ciencias Penales, México, 2005, p. 70.

1. 4 PROGRAMAS, MÉTODOS Y TÉCNICAS POR MEDIO DE LOS CUALES SE PUEDE LLEVAR CABO EL FRAUDE INFORMÁTICO

El manejo electrónico fraudulento por parte del sujeto activo puede llevarse a cabo de muy variadas formas, de tal modo que pueda desde modificar las instrucciones con las que originalmente se habían configurado los programas hasta inducir el error al sistema o bien aprovechar los errores de seguridad y protección existentes en ellos mismos, para obtener de esta manera una percepción económica o algún servicio, es decir, conseguir un aprovechamiento ilícito. A continuación daremos los programas, métodos y técnicas por medio de los cuales se puede llevar a cabo el fraude informático:

Ataque Remoto o **Intercepción de Comunicación en una Red Local o Inalámbrica de Internet**: Este ataque consiste en que el delincuente se coloque entre el sitio web y la computadora del usuario, de manera que la información que viaja de ida y vuelta puede ser vista y modificada por la computadora del atacante, es por ello que también se le ha llegado a denominar como el Hombre en Medio (*man in the middle*). Aquí se emplea el término de Redes Hostiles para indicarnos que entre más pública sea la red a la que se conecte, más probabilidades hay de que su comunicación pueda ser interceptada, dentro de esta expresión se incluyen las redes inalámbricas de universidades y de restaurantes. Un ejemplo claro para este tipo de ataque, podría ser cuando el delincuente intercepta una transacción bancaria y pone su propio número de cuenta, antes de que la información llegue al Banco.

Ataques Sincrónicos o *Asíncronos (Asyncronous Attacks)*.- Es un método de ataque basado en la forma de cómo funcionan los sistemas operativos y sus conexiones con los programas de aplicación a los que sirven y soportan en su ejecución. Es una táctica de alto conocimiento técnico, muy difícil de detectar. Este ataque aprovecha la posibilidad que tiene el sistema operativo de volver a inicializar el sistema en condiciones diferentes a las autorizadas, como sucede en ciertos puntos de recuperación del sistema. Un ejemplo de un ataque asíncrono sería un programa que reproduzca la pantalla de entrada en un sistema, cuando el usuario proporciona su clave, se almacena esta información en un archivo de la persona que está realizando el fraude, de esta manera logra el acceso que le estaba prohibido.

Bombas Lógicas o Cronológicas (*Logic Bombs)*.- Consiste en la introducción de un programa con un conjunto de instrucciones que se ocultan en la memoria del sistema, en los discos, o en los archivos de programas ejecutables con tipo COM o EXE, en espera de una determinada fecha, hora, o circunstancia para explotar; se activan cuando se ejecuta el programa que las contiene, provocando que el funcionamiento del sistema se detenga en el momento decidido por el autor del hecho, destruyendo los datos o los programas de los mismos. Algunos de estos virus no son destructivos y solo exhiben mensajes en las pantallas al llegar el momento de la explosión. Se emplean para cometer el delito y alejarse sin dejar rastro, ya que destruyen datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo, cuando el delincuente ya se encuentra lejos. Las bombas lógicas, son difíciles de detectar antes de que exploten, por ello puede utilizarse también como instrumento de extorsión para pedir un rescate a cambio de dar a conocer el lugar en donde se encuentra.

Caballo de Troya (*Trojan Horse)*.- Generalmente lo conocemos como *troyano* o *códigos troyanos*. Son programas aparentemente útiles e inofensivos que en realidad contienen un código oculto diseñado para dañar o beneficiarse del sistema en el que se ejecuta; permanecen en el sistema, no ocasionando inmediatamente acciones destructivas, sino todo lo contrario suele capturar datos, generalmente *password* enviándolos a otro sitio; o dejar indefenso el ordenador donde se ejecuta, abriendo agujeros en la seguridad del sistema, con la siguiente profanación de nuestros datos. Consiste en introducir una serie de instrucciones no autorizadas en un programa para que actúe en forma distinta a como estaba previsto, evidentemente, en beneficio del autor. Se envían normalmente a través de mensajes de correo electrónico que falsean el objetivo y la función del programa. El *troyano* deja una *carga* o realiza una tarea malintencionada cuando se ejecuta. No se consideran *virus* informáticos ni *gusanos* porque no se pueden propagar por sí mismos; no obstante, se puede utilizar un virus o un gusano para copiar y dejar un *troyano* en el sistema que se desea atacar (este proceso se denomina colocación). Normalmente, los troyanos tienen como objetivo interrumpir el trabajo del usuario o el funcionamiento normal del sistema, por ejemplo, los *troyanos* pueden crear una *puerta trasera* (*Backdoor*) en el sistema para que los atacantes puedan robar datos o cambiar la configuración.

Data Leakage.- Es un método utilizado para sustraer información confidencial de una empresa. También incluye la divulgación no autorizada de información secreta (datos reservados), obteniendo los datos de información que estaban destinados para otra finalidad, como por ejemplo del censo electoral, información médica, etcétera. También es conocido como filtración de datos. Para su realización se emplean múltiples programas.

Gusano (*Worm*).- Son programas que se copian a sí mismos hasta ocupar toda la memoria de la computadora. Suelen llegar a través de los correos electrónicos en forma de archivo adjunto. Tratan de reproducirse a sí mismos con el fin de colapsar el sistema o ancho de banda. El mayor efecto de los gusanos es su capacidad para saturar e incluso bloquear por exceso de tráfico a los sitios web. Los *gusanos* pueden realizar acciones dañinas, como consumir los recursos de la red o del sistema local, dando lugar probablemente a un ataque de denegación de servicio. Se propagan por sí mismos sin modificar u ocultarse bajo otros programas. No destruyen información de forma directa, pero algunos pueden contener las propiedades de un *virus* que si puede hacerlo. Determinados tipos de *gusanos* se pueden ejecutar y propagar sin la intervención del usuario, mientras que otros requieren que éste ejecute directamente el código para su propagación.

***Hacking* (*Hackear*)**.- Consiste en entrar de forma ilegal en un sistema, para obtener información. No conlleva la destrucción de datos ni la instalación de *virus*, pero pueden instalarse troyanos que proporcionen *passwords* nuevos. Hay quien opina que lo que en realidad significa es una búsqueda de información a la que se debería tener acceso legalmente. Es decir, los sujetos que actúan de esta forma (Los *Hacker*) lo hacen en forma de protesta contra el acceso denegado e infundado al uso de la información, ya que se dice que pelean contra un sistema injusto utilizando como arma al propio sistema, a algunos *hackers* los intriga el desafío, mientras que a otros les atrae substraer datos delicados para algún beneficio propio. Los *hackers* son capaces de acceder a redes de transmisión de datos, con un modem, saltándose las medidas de seguridad y obtener el acceso a la información confidencial.

Hoax.- Este método básicamente consiste en mensajes con historias inventadas, es decir mentiras solapadas en narraciones, cuya finalidad es atraer

el interés del lector o destinatario para conseguir dinero o propagar un *virus*. Por lo general concluyen la historia con una frase semejante a la siguiente; no dude en aportar su imprescindible ayuda, envié un mensaje de apoyo o bien su aportación económica al número de cuenta que se adjunta.

Ingeniería Social (*Piggybacking and Impersonation*).- Es el Arte de convencer a la gente de hacer algo que en realidad no debería, permitiendo obtener información con engaños y simulación de personas. Este método se puede manifestar de tres formas, mediante el:

1.- **Engaño Telefónico**.- Donde el delincuente realiza una llamada telefónica al usuario haciéndose pasar por administrador del sistema, un ejecutivo u otra persona y requerirle información confidencial (como el número de tarjeta o un *password)*, con alguna excusa convincente.

2.- **Engaño para ejecutar un programa oculto**.- Es muy común que el atacante envíe un archivo por correo electrónico o por mensajería instantánea, que parezca ser otra cosa (como podría ser una foto, un documento, un video), para engañar al usuario, e inducirlo a que accese a él. Al abrir dicho archivo se ejecuta un instalador que introduce un *troyano* o *puerta trasera* a la computadora de la víctima, posteriormente manda un mensaje de error ficticio, desde ese momento el atacante tendrá acceso total a la computadora remota como si estuviera sentado frente a ella, consiguiendo ver toda la información del disco duro, ejecutar programas, espiar al usuario e incluso conectarse a un banco para hacer transacciones.

3.- ***Spoofing***.- *E*s el término que se emplea para designar el hecho de usurpar la identidad de otra persona en internet y de utilizarla con fines mal intencionados.

Pharming.- Consiste en la actividad de desviar el tráfico de Internet de un sitio web hacia otro sitio falso de apariencia similar, con la finalidad de engañar a los usuarios para obtener sus nombres y contraseñas de acceso. Con frecuencia, los sitios de banca en línea y otros similares se convierten en los principales objetivos de estos ataques, en los que los delincuentes intentan adquirir datos personales con el fin de obtener acceso a cuentas bancarias,

robar datos identificativos o cometer más delitos suplantando a usuarios. En este método se puede desviar al usuario sin que tenga conocimiento de ello, mediante un proceso denominado "envenenamiento de DNS", donde el atacante obtiene acceso a alguna de las enormes bases de datos que utilizan los proveedores de Internet para dar una nueva ruta y desviar a los usuarios hacia el sitio falso antes de que éstos tengan acceso a la página deseada.

Phishing.- Se pronuncia igual que *fishing* (pesca, en inglés), también se conoce como suplantación de marca o *carding.* Es una técnica de captación ilícita de datos personales, principalmente relacionados con claves para el acceso a servicios bancarios y financieros (*login y password*), a través de correos electrónicos y páginas web que imitan exactamente la imagen o apariencia idéntica de una entidad bancaria o financiera, e incluso de cualquier otro tipo de empresa de reconocido prestigio. Estas acciones fraudulentas *online,* usualmente se llevan a cabo cuando el correo electrónico falso remite al usuario a una página web también fraudulenta, donde siempre se incluyen una petición final en la que solicita a los usuarios por ejemplo actualizar claves bancarias o información financiera confidencial, como la confirmación de datos personales alegando distintos motivos (problemas técnicos, cambio de política de seguridad, posible fraude, etc.); dada la confianza que los usuarios tienen depositada en las entidades de las que son clientes, y por el desconocimiento o simplemente ante la incertidumbre o temor provocado, acceden a dichas páginas web piratas, donde el delincuente, obtiene los datos personales o claves de acceso personales, y finalmente con esos datos obtenidos realizan operaciones no autorizadas, en nombre de la víctima.

***Phreaking* (*Wiretapping) ó* Pinchado de Líneas Telefónicas**.- Esta técnica consiste en apoderarse, redirigir o en manipular los datos que circulan a través de la línea telefónica, por medio de equipos electrónicos construidos artesanalmente, entre los cuales podemos citar los siguientes:

- *Blackbox*: Dispositivo que engaña a la central telefónica haciéndole creer que no se levantó el teléfono cuando en realidad se está produciendo una comunicación.
- *Bluebox*: Aparato que emite tonos de *multifrecuencias* para controlar las centrales telefónicas. Generalmente se utiliza para lograr comunicaciones

gratuitas, es decir para llamar gratis, entre otras cosas.

- *Redbox*: Simula la introducción de monedas en teléfonos públicos.
- Mediante la conexión sofisticada entre un radio, un modem y una impresora se intervienen las líneas.

Pirámides de Valor.- En este método los delincuentes se valen del internet con temas que contienen algo similar a la leyenda “Consiga aumentar sus ganancias en poco tiempo” o “Hágase rico con tan solo”. El objetivo de tan suculento mensaje es captar la atención del usuario, con la única finalidad de que lean el cuerpo del mensaje y se crea que pueden conseguir grandes comisiones por no hacer nada, una vez que han engatusado a sus próximas víctimas suelen remitirles un correo electrónico o bien un enlace para que accedan a una determinad página web, a su vez, le solicitan sus datos de carácter personal y un número de cuenta en la que los estafadores depositarán los ingresos de las futuras comisiones, lo único que deben hacer es pagar una determinada cantidad de dinero e incluirse en la cadena ya nacida, posteriormente, deben remitir miles y miles de correos electrónicos a usuarios para que éstos repitan el procedimiento. En teoría según vaya escalando en la cadena, irá aumentando el porcentaje de la comisión.

Puerta Falsa, Puerta Trampa *(Trapdoor)* ó puerta trasera (Backdoor).- Método que consiste en introducir interrupciones en la lógica de los programas con objeto de checar en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin, o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante. En otras palabras es hacer agujeros o espacios y provocar defectos ya sea en la seguridad de los sistemas o en las entradas provisionales, que poseen los programas para hacer más ágil su proceso de prueba y depuración, y permitir que la instalación de la versión definitiva sea exitosa.

Recogida de Información Residual *(Scavenging*).- Técnica también conocida como *To Scavenge* (recoger basura) o *Dumpster Diving*. Consiste en aprovechar todo tipo de información abandonada o desechada (tirados en la papelera o basura *virtual*), sin ninguna protección, ya que no fueron destruidos totalmente y que contienen información sensible. Se efectúa al tomar información residual que ha quedado en la memoria o en soportes magnéticos.

Rootkits.- Son programas que los atacantes utilizan para obtener acceso remoto no autorizado a un equipo y ejecutar ataques adicionales. Pueden utilizar varias técnicas diferentes, entre las que se incluyen el seguimiento de las pulsaciones de teclas, el cambio de los archivos de registro o de las aplicaciones existentes en el sistema, la creación de puertas traseras y el ataque a otros equipos de la red. Por lo general, los *rootkits* se organizan como un conjunto de herramientas que se adaptan específicamente para atacar a un sistema operativo determinado. Los primeros aparecieron a principios de los 90, siendo sus principales objetivos los sistemas operativos *Sun* y *Linux*. Actualmente son muchos los sistemas operativos objetivo, entre ellos la plataforma Microsoft Windows.

Scam.- Esta técnica consta de tres partes en las cuales se hace uso de otros medios de defraudación. La primera se realiza mediante mensajes de ofertas de empleo o de trabajo en casa con una gran rentabilidad o disposición de dinero (*Hoax*), en el caso de que caigan en la trampa, deben rellenar determinados campos, tales como; datos personales y número de cuenta bancaria. Una vez recabados estos datos, se pasa al segundo de los escalafones, mediante la cual se remiten millones de correos electrónicos, bajo la apariencia de entidades bancarias, solicitando las claves de la cuenta bancaria (*Phishing*). El tercer escalafón consiste en que los delincuentes comienzan a retirar sumas importantes de dinero, las cuales son transmitidas a las cuentas de los intermediarios, quienes posteriormente deben dar traspaso a las cuentas de los delincuentes, llevándose éstos las cantidades de dinero y aquellos intermediarios un porcentaje de la transacción como comisión.

Spam.- Este método trata del envió masivo de correos electrónicos no deseados, es decir, sin que los usuarios los hubieran solicitado, se genera para hacer publicidad de un servicio o producto; mediante el empleo de estos correos se puede sustraer la información que contenga el sistema donde se introdujo. Los mensajes de este tipo constituyen un problema para la infraestructura de Internet y para la productividad de las empresas, consiste

***Spyware* (Programa espía)**- Es un programa que abarca otros tipos de programas hostiles, los cuales tienen como funcionalidad recopilar información del usuario y enviarla al creador. El tipo de información que recopilan depende

mucho del *spyware* instalado, pero puede ir desde hábitos de navegación en Internet, hasta todos lo que haya escrito el usuario (incluyendo contraseñas). El *spyware* más sofisticado tiene la funcionalidad de un *Troyano*.

Técnica del *Salamí (Salamí Techniques o Rouding Down)*.- Esta técnica consiste en alterar un programa que maneja transacciones financieras de las cuentas bancarias o de nóminas, logrando que sumas, casi imperceptibles, de algunas de las cuentas (generalmente centavos), se acrediten en otra cuenta manejada por el delincuente; al sumar estas pequeñas manipulaciones o substracciones se provoca un gran fraude y un perjuicio a la sociedad. Dicha técnica se ejecuta al aprovechar las repeticiones automáticas de los procesos de cómputo y sin grandes dificultades. Uno de los casos más ingeniosos es el redondeo hacia abajo, que consiste en una instrucción que se da al sistema informático para que transfiera a una determinada cuenta, los centavos que se descuenten por el redondeo. Se considera que el término *Salamí*, empleado por esta técnica, fue extraído de la palabra *Salamín*, la cual se emplea para designar a una persona tonta o de escaso entendimiento.

Uso no Autorizado de un Programa Especial (*Superzapping)*.- Es una llave no autorizada que abre cualquier archivo del ordenador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar los datos almacenados en el ordenador. El nombre en inglés deriva de un conocido programa de servicio creado para ciertos sistemas de IBM "*superzap*".

Virus.- Es un código informático que se adjunta a sí mismo a un programa o archivo para propagarse de un equipo a otro. Infecta a medida que se transmite. Al igual que los virus humanos tienen una gravedad variable, los virus informáticos van desde molestias moderadas hasta llegar a ser destructivos, ya que pueden dañar, alterar o destruir tanto al *Software*, como el *Hardware* y los archivos de datos de un ordenador.

Con todo lo expuesto anteriormente, es fácil observar que la cantidad de métodos y técnicas aumentan con el tiempo, así como el ingenio, que nunca falta, de los interesados en cometer un fraude. Por ello los métodos aquí mencionados son una tipología limitada, como de hecho, lo será cualquier otra tipología más reciente o futura, debido al dinamismo de la informática.

1. 5 SITUACIÓN INTERNACIONAL DEL FRAUDE INFORMÁTICO

En los últimos años, se ha perfilado un cierto cambio internacional en lo concerniente a lo jurídico y a los problemas derivados del mal uso que se hace de los medios informáticos. Cuando se habla de fraude y delincuencia informática, habitualmente se hace de una manera muy genérica, ya que es muy difícil concretar el delito informático como tal, puesto que la legislación sobre delitos informáticos es todavía muy limitada en la mayoría de los países, por tal razón es común que se refieran al fraude informático como aquella conducta realizada mediante un sistema informático con la que se busca conseguir un beneficio ilícito. Los fallos judiciales absolutorios han dado evidencia de que dicha conducta no encuadra en los tipos penales existentes, lo cual ha motivado en otros países, la creación de un tipo penal específico para el fraude informático, para evitar que esta clase de conductas queden impunes. En este sentido:

En **Alemania**: La Ley contra la Criminalidad Económica de 1986 contempla como delitos: a) el fraude informático, b) el sabotaje informático, c) el espionaje de datos, y d) la alteración de datos. Por otro lado el Código Penal Alemán establece en su artículo 263 que quien con el propósito de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que perjudique el patrimonio de otro, por una estructuración incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado de datos, o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso, será castigado con pena privativa de la libertad hasta cinco años.

En **Argentina**: Existe un proyecto de ley sobre delitos informáticos que establece en su artículo 8, una sanción privativa de libertad, de ocho meses a seis años, a la persona que a través de cualquier medio, manipule sistemas o datos informáticos y obtenga para sí o para terceros una ventaja económica.

En **Austria**: La Ley de reforma del Código Penal, promulgada el 22 de diciembre de 1987, en el artículo 148, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de la elaboración automática de datos, a través de la confección del programa, por la

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

En **España**: Este país quizás sea el que mayor experiencia haya obtenido en casos de delitos informáticos. Su actual Ley Orgánica de Protección de datos de Carácter Personal (LOPDCP) aprobada el 15 de diciembre de 1999, reemplaza una veintena de leyes anteriores de la misma índole, y contempla la mayor cantidad de acciones lesivas sobre la información. Así mismo el Nuevo Código Penal de España establece en su artículo 264-2 castigos de prisión de uno a tres años y multas, a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos; y en el segundo párrafo del artículo 248 establece una pena rigurosa a los que con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

En **Estados Unidos de América**: La Ley Federal de Protección de Sistemas de 1985 fue la base para el *Acta de Fraude y Abuso Computacional (Computer Fraud y Abuse Act)* de 1986, la cual se refiere en su mayor parte a delitos de abuso o fraude en contra de casas financieras, registros médicos, u órganos de gobierno. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de *passwords* ajenos o propios en forma inadecuada. En 1994 es sustituida por el Acta Federal de Abuso Computacional, en donde se sanciona con pena de prisión y multa, a la persona que defraude a otro mediante el uso de una computadora o red informática. Esta acta es un adelanto porque prohíbe la transmisión de programas, virus, códigos o comandos que causen daño a la computadora, a los sistemas informáticos, a las redes, información, datos o programas.

En **Francia**: En enero de 1988, se dicta la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multa de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique los datos existentes. Contemplando las siguientes conductas punibles: en su artículo 462-2 se sanciona tanto el acceso al sistema como al

que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema; en el articulo 462-3 se contempla la acción de impedir o alterar el funcionamiento de un sistema; y en su artículo 462-4 se penaliza a quien introduzca datos en un sistema de procesamiento automatizado, o haya suprimido o modificado los datos que éste contiene, o sus modos de tratamiento (procesamiento), o de transmisión.

En **Gran Bretaña**: En 1991 comenzó a regir La Ley de Abusos Informáticos (*Computer Misuse Act*), mediante la cual el intento exitoso o no de alterar o modificar los datos informáticos con intención criminal y sin autorización se castiga hasta con cinco años de prisión o multas sin límite, en ese apartado, se incluyen a los virus en esta categoría, de modo que el hecho de liberar un virus tiene penas que van desde un mes hasta cinco años. El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas. La ley se puede considerar dividida en tres partes: *hackear* (ingresar sin permiso en una computadora), hacer algo con la computadora *hackeada* y realizar alguna modificación no autorizada; y el último apartado se refiere tanto al *hacking, como a* la modificación de un programa para instalar un *backdoor* (el cual es la infección de un programa con un virus que puede llegar a la inhabilitación del funcionamiento de la computadora).

En **Holanda**: El 1º de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos. Esta ley contempla acciones específicas sobre técnicas de *Hacking,* otras acciones de los *Phreackers, y de* la Ingeniería Social*,* comprendiendo también la distribución de virus. El mero hecho de entrar en una computadora en la cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis meses de cárcel. Si además se usó esa computadora *hackeada* para acceder a otra, la pena sube a cuatro años. Copiar archivos de la máquina *hackeada* o procesar datos en ella también conlleva un castigo de cuatro años en la cárcel. El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel, de seis meses a quince años. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos años de prisión pero, si se hizo vía remota aumenta a cuatro. Como ya se ha hecho mención los virus están considerados de una manera muy especial en esta ley,

si estos virus distribuyen datos con la intención de causar problemas, el castigo puede llegar hasta los cuatro años de cárcel, y si se demuestra que estos virus se escaparon por error la pena no superará el mes de prisión. El usar el servicio telefónico mediante un truco técnico (*Phreacking*) o pasando señales falsas con el objetivo de no pagarlo, puede recibir hasta tres años de prisión. La venta de elementos materiales (un radio o un modem especial), que permitan el *Phreacking* se castiga con un año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo aumenta a tres. Falsificar tarjetas de crédito de banca electrónica y usarlas para obtener beneficios o como si fueran las originales está penado con hasta seis años.

El presente análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas puestas en vigor están dirigidas a proteger el empleo abusivo de la información reunida y procesada mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos.

Por otra parte La Organización de Naciones Unidas (**ONU**) ha reconocido los siguientes tipos de fraudes cometidos mediante la manipulación de computadoras (fraudes informáticos):

1.- **Manipulación de los datos de entrada**: Este tipo de fraude informático es fácil de cometer y difícil de descubrir. No requiere de amplios conocimientos técnicos de informática, por lo tanto puede realizarlo cualquier persona que tenga acceso al procesamiento de datos, en la fase de adquisición de los mismos; también es conocido como sustracción de datos.

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

Para poder comprender mejor los dos anteriores puntos es necesario explicar que las etapas del procesamiento de datos comprende tanto la entrada (es decir cuando se generan, adquieren o crean los datos), como el almacenamiento (al reunir, guardar o registrar la información en la memoria de un ordenador), la salida (el modo de visualizarlos o escucharlos), y la transmisión de dichos datos. Estos datos pueden contener información numérica, textual, de audio o vídeo, en fin todo tipo de información codificada.

3.- **La manipulación de programas**: Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Para ejecutar este tipo de fraude el delincuente debe tener conocimientos profundos y concretos de informática (especialmente en programación informática), lo cual provoca que sea muy difícil de descubrir. El método más utilizado es el denominado **Caballo de Troya**, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

4.- **Fraude efectuado por manipulación informática**: En este tipo de fraude informático se aprovecha las repeticiones automáticas de los procesos de cómputo. Para esta organización es la técnica especializada que se denomina **técnica del *salamí*** (la cual ya ha sido explicada con amplitud en el tema anterior).

Como podemos apreciar la conceptualización utilizada por la ONU para este delito, se enfoca de manera primordial, al comportamiento desplegado por el sujeto activo, mediante la manipulación de datos y programas, es decir, se ha optado por definir a la conducta que caracteriza al fraude informático como una manipulación, en el entendido de que dicho término comprende la acción de insertar, ingresar, suprimir, modificar o adulterar la información de un sistema informático, ya sea en programas o en el procesamiento de dicha información (entrada, almacenamiento, salida o transmisión de datos). Cabe decir que la palabra manipulación proviene del latín *manus* (poder), noción que implica la influencia voluntaria en los acontecimientos o en las relaciones personales, con distorsión de la verdad o la justicia, y al servicio de intereses particulares.

CAPÍTULO 2. EL FRAUDE INFORMÁTICO EN MÉXICO

En la actualidad nuestro país carece de una regulación adecuada para este tipo de conductas, en los siguientes temas trataremos de dar una noción de cómo la sociedad se encuentra desprotegida ante la amenaza que trae consigo el mal uso de la innovación tecnológica y medios informáticos, a pesar de que dicha innovación marcara el futuro, tanto de las presentes como de las próximas generaciones.

2. 1 PROTECCIÓN JURÍDICA QUE BRINDA EL DERECHO MEXICANO CONTRA EL FRAUDE INFORMÁTICO

En nuestro sistema legal se han realizado muchos intentos para tipificar conductas relacionadas con el fraude informático, como lo podemos apreciar en los siguientes ordenamientos jurídicos:

En el Código Penal Federal, dentro del Titulo Noveno, Capítulo II (Acceso ilícito a sistemas y equipos de informática), se encuentran los artículos 211 bis 1 al 211 bis 7, donde se tipifican determinados comportamientos ilícitos de los llamados *hackers* o *crackers*, que atentan contra los sistemas o equipos de informática del Estado o de las instituciones que integran el sistema financiero (dichas instituciones están señaladas en el artículo 400 Bis, de este mismo ordenamiento.), protegidos por algún mecanismo de seguridad, en estos artículos se sanciona al sujeto que tenga acceso a los ya mencionados sistemas o equipos, con la debida autorización o sin ella, y altere, modifique, destruya, dañe, conozca indebidamente, copie, o provoque pérdida de información contenida en ellos. Incrementando la pena en una mitad cuando, en el caso particular de que las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. Para una mejor comprensión a continuación se transcriben dichos artículos:

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

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

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

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

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

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

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

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.
Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

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

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

Artículo 400 bis.- Párrafo séptimo ...el sistema financiero se encuentra integrado por las instituciones de crédito, de

> seguros y de fianzas, almacenes generales de depósito, arrendadoras financieras, sociedades de ahorro y préstamo, sociedades financieras de objeto limitado, uniones de crédito, empresas de factoraje financiero, casas de bolsa y otros intermediarios bursátiles, casas de cambio, administradoras de fondos de retiro y cualquier otro intermediario financiero o cambiario.

Al analizar dichos artículos del Código Penal Federal se hacen las siguientes consideraciones:

A) El artículo 211 bis 1, ampara toda información contenida en los sistemas o equipos de informática pertenecientes a una empresa, institución o persona en sentido amplio, que pueda ser objeto de dicha conducta, toda vez que este artículo no especifica a quien pertenece dicho sistema u equipo.

B) Los artículos 211 bis 2 y 211 bis 3, solo protegen la información contenida en sistemas o equipos de informática propiedad del Estado.

C) Los artículos 211 bis 4 y 211 bis 5, únicamente protegen la información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, entendiéndose como tales a las señaladas en el artículo 400 Bis del mismo ordenamiento.

D) Los legisladores incurren en el error de plasmar como requisito en los artículos 211 bis 1, 211 bis 2 y 211 bis 4, que los sistemas o equipos de informática se encuentren protegidos por algún mecanismo de seguridad, cuando en realidad deben contemplarlos se encuentren o no protegidos, puesto que lo más frecuente es que los delincuentes aprovechen el error de las víctimas al no tener instalada una debida protección en sus equipos, ya sea por desconocimiento u olvido. Además se debe tomar en cuenta que en la actualidad cualquier sistema de seguridad puede ser violado.

E) Tanto las penas privativas de libertad como pecuniarias previstas en dichos artículos se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

En la Ley de Instituciones de Crédito, ordenamiento federal, se contemplan tipos penales especiales, mismos que aluden a la clonación de tarjetas de crédito o débito y a la alteración de los cajeros automáticos, como se aprecia de la lectura de los siguientes preceptos:

> Artículo 112 bis.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que:
> I. Produzca, reproduzca, introduzca al país, imprima o comercie tarjetas de crédito, de débito, formatos o esqueletos de cheques, o en general instrumentos de pago utilizados por el sistema bancario, sin consentimiento de quien esté facultado para ello;
> II. Posea, utilice o distribuya tarjetas de crédito, de débito, formatos o esqueletos de cheques, o en general instrumentos de pago utilizados por el sistema bancario, a sabiendas de que son falsos;
> III. Altere el medio de identificación electrónica y acceda a los equipos electromagnéticos del sistema bancario, con el propósito de disponer indebidamente de recursos económicos, u
> IV. Obtenga o use indebidamente la información sobre clientes u operaciones del sistema bancario, y sin contar con la autorización correspondiente…
>
> Artículo 113 bis.- A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de recursos o valores de los clientes de las instituciones de crédito, se le aplicará una sanción de tres a diez años de prisión y multa de quinientos a treinta mil días de salario…

De tal forma que en los anteriores artículos se protege exclusivamente al sistema bancario y a los clientes de sus instituciones, dejando sin protección a los sistemas y programas informáticos que no pertenecen a dicho sistema y a las personas que no tengan relación alguna con las instituciones bancarias.

El Código Penal para el Distrito Federal, nos señala en su Título Décimo Quinto (Delitos contra el patrimonio), Capítulo III (Fraude), lo siguiente:

> Artículo 231. Se impondrán las penas previstas en el artículo anterior, a quien:
> …XIV. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución;…

Podríamos decir que esta fracción aporta algo nuevo al delito de fraude, y aún más en relación a lo informático, toda vez que al señalarnos “por cualquier medio”, de una forma muy generalizada, nos hace suponer que la protección penal que se ofrece abarca el empleo de cualquier medio informático, más sin embargo al igual que en los artículos 211 bis 4 y 211 bis 5, del Código Penal Federal, dicha protección jurídica queda circunscrita a un determinado sistema o programa de informática que pertenezca solo al sistema financiero, ignorando de esta forma la información contenida en los sistemas informáticos de los demás entes sociales.

Por su parte El Código Penal para el Estado de Guanajuato, plasma en su artículo 231, un tipo penal en el que se alude, en forma expresa, a la información contenida en los equipos de cómputo o sus accesorios; dicho tipo penal denominado violación de correspondencia, tutela las vías de comunicación de uso público y la correspondencia, en el se sanciona (en su facción II), la conducta consistente en acceder, destruir o alterar la comunicación o información contenida en equipos de cómputo o sus accesorios u otros análogos; indicando de una manera muy acertada que no se impondrá pena alguna a quienes ejerciendo la patria potestad o la tutela, ejecute la conducta antes descrita, tratándose de sus hijos menores de edad o de quienes se hallen bajo su guarda, además se especifica que se requerirá querella de parte ofendida cuando se trate de ascendientes y descendientes, cónyuges o concubinos, parientes, civiles o hermanos.

2. 2 EL PRINCIPIO DE LEGALIDAD, LA GARANTÍA DE SEGURIDAD JURÍDICA Y EL FRAUDE INFORMÁTICO

El principio de legalidad se identifica en un primer sentido con la reserva relativa de la ley, entendiendo ley en el sentido formal del acto o mandato legislativo y se limita a prescribir la sujeción del juez a las leyes vigentes, en un segundo sentido, se identifica con la reserva absoluta de la ley, proscribiendo que tal contenido esté formado por supuestos típicos de significado preciso.

"El principio de legalidad inherente al Estado Mexicano da sustento a otras cuatro garantías individuales de carácter procesal, dentro de las cuales se encuentra la garantía criminal *nullum crime sine lege*, que establece que una conducta sólo puede considerarse delictiva cuando esté descrita como tal en una ley penal anterior a su comisión". [1]

De este modo podemos decir que el tipo penal cumple una función de garantía, de manera que nadie puede ser sancionado penalmente si la conducta no se encuentra prevista como delictiva en un ordenamiento vigente con anterioridad al hecho.

La Suprema Corte de Justicia de la Nación ha sostenido que "la garantía de seguridad jurídica de exacta aplicación de la ley no se limita a obligar a la autoridad judicial a abstenerse de imponer por analogía o mayoría de razón pena alguna que no esté decretada por una ley aplicable al hecho delictivo, sino que obliga al legislador para que al momento de expedir las normas de carácter penal, señale las conductas típicas y penas aplicables con tal precisión que evite un estado de incertidumbre jurídica al gobernado y una actuación arbitraria del juzgador". [2]

Por lo tanto se asume que la ley penal debe estar creada de tal forma que los términos mediante los cuales especifica los delitos o las penas sean claros, precisos y exactos, evitando que la autoridad aplicadora incurra en confusión y en detrimento de la defensa del procesado.

---

[1] DÍAZ ARANDA, Enrique. Derecho Penal Parte General, Porrúa, México, 2003, p. 57.

[2] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. Las Garantías de Seguridad Jurídica, México, Nuevo Milenio, 2004, p. 67.

Todo lo anterior lo podemos apreciar en el artículo 14 Constitucional:

> Artículo 14.- …Nadie podrá ser privado de la libertad o de sus propiedades, posesiones o derechos, sino mediante juicio seguido ante los tribunales previamente establecidos, en el que se cumplan las formalidades esenciales del procedimiento y conforme a las leyes expedidas con anterioridad al hecho.
>
> 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…

Ahora bien, la incertidumbre de los juzgadores, al tener frente a ellos un caso de la naturaleza del fraude informático, se hace presente cuando la conducta del sujeto activo se realiza con el empleo de los medios informáticos u otro artificio semejante. Por ello es precisamente aquí donde debemos hacer notar y enfatizar que los elementos del tipo penal de fraude informático son iguales a los del tipo genérico tradicional, ya que se requiere el engaño o el aprovechamiento de un error como el acto que provoca el perjuicio para un tercero, y la obtención ilícita de cualquier cosa o un lucro indebido como el menoscabo a su patrimonio; siendo la única variante el modo de ejecutar, manifestar o transmitir la conducta del delincuente mediante el empleo de los medios informáticos. Por lo tanto podemos considerar que no resulta razonable la creación de un nuevo tipo penal para el fraude informático, ya que este nuevo tipo no haría más que confundir y sobreponer el delito ya existente. Lo anterior nos lleva a que nuestra propuesta para regular la comisión del fraude informático, sea la de incluir su forma de ejecución como una agravante de la pena del delito de fraude, lo cual evitaría la incertidumbre de los juzgadores al enjuiciar, ya que la conducta del sujeto activo (el engaño o el aprovechamiento del error), se hace presente al efectuar cualquier manipulación informática (ingresar, insertar, sustraer, suprimir, modificar o alterar la información de un sistema informatizado), ya sea en programas o en cualquier etapa del procesamiento de la información (el cual comprende tanto la entrada, como el almacenamiento, la salida o la transmisión de los datos), mediante el empleo de algún medio informático o un artificio semejante.

2. 3 LAS TRES PRINCIPALES FORMAS COMO SE HA MANIFESTADO EL FRAUDE INFORMÁTICO EN MÉXICO

Evidentemente el motivo que resulta más atractivo para cometer el Fraude informático es la obtención de dinero o algo de valor. Por lo tanto, los sistemas que pueden estar más expuestos a fraude son los que tratan con pagos (como los de nómina, los de ventas y en los de compras.), en ellos es donde es más fácil realizar transacciones fraudulentas de dinero. En segundo término quedaría la obtención de datos personales (tales como su ideología, edad, religión, creencias, salud, origen racial y vida sexual.), para emplearlos posteriormente de alguna forma ilícita y cometer el delito; En tercer lugar tendríamos al fraude cometido en subastas por internet y por último al fraude cometido para la obtención ilegal de alguna prestación de servicios (como el uso del servicio telefónico).

En los siguientes tres puntos, mencionaremos los rasgos principales de los fraudes informáticos, que con mayor frecuencia han afectado a usuarios en nuestro país, mencionando las formas o métodos empleados para poder realizarlos.

2. 3. 1 EL FRAUDE INFORMÁTICO EN EL SISTEMA BANCARIO Y EN LAS TARJETAS DE CRÉDITO O DÉBITO

Con la incursión de la informática en el sistema bancario, se ha reemplazado muchos de los documentos tradicionales, plasmados en papel, por anotaciones en cuenta o registros lógicos realizadas con el empleo de los medios informáticos, este fenómeno permite a los clientes operar con sus bancos con gran agilidad y comodidad, sin la necesidad de presentarse en sus oficinas. Es aquí donde tienen cabida las manipulaciones a los sistemas, que constituyen la forma más frecuente de comisión del fraude informático.

En nuestro país existen ciertos tipos penales en donde las conductas efectuadas mediante el empleo de la informática, para obtener un beneficio económico ilegal, pudieran quedar comprendidas, tal es el caso de la Ley de Instituciones de Crédito, ordenamiento federal, en sus artículos 112 bis y 113 bis; En el Código Penal Federal del artículo 211 bis 4 al 211 bis 6; y por último

el artículo 231, fracción XIV del Código Penal para el Distrito Federal. Tal y como los analizamos anteriormente en el tema II. I Protección Jurídica Que Brinda El Derecho Mexicano contra El Fraude Informático. Tomando en cuenta que el significado del término Financiero, mencionado en dichos artículos, atañe a todo lo relacionado con la Hacienda pública, a los grandes negocios mercantiles, y a las cuestiones bancarias o bursátiles.

En este tipo de fraude informático, el objetivo principal del atacante es tener acceso a las cuentas bancarias, a los números de las tarjetas, y al correcto *password o nip* (contraseñas o claves de acceso personales), de la víctima para poder transferir dinero o hacer cargos de forma ilícita Para ello el delincuente puede actuar mediante el empleo de las siguientes técnicas:

- Ataque Remoto
- *Hacking*
- Ingeniería Social
- *Phishing*
- Técnica del *Salamí*

El esfuerzo de muchos expertos ha estado enfocado en prevenir este tipo de ataques para garantizar la legitimidad y seguridad de las transacciones informáticas. Mas sin embargo los mecanismos de seguridad implantados por la mayoría de bancos no son completamente satisfactorios para una actividad como la que desarrolla la banca, en la que el usuario no sólo consulta saldos y movimientos de sus cuentas y tarjetas, sino que también puede efectuar todo tipo de transferencias electrónicas a través de Internet, como el retirar o depositar a una determinada cuenta bancaria, la compra y venta de acciones, y la compra de artículos realizadas a través del comercio electrónico.

Básicamente existen dos formas de actuación por parte de las personas que se dedican al fraude con tarjeta de crédito (*Carding*) o débito: Por un lado la obtención de la tarjeta física como tal, y por el otro capturar los datos de la banda magnética para su posterior utilización.

En el primero de los casos, en donde los delincuentes se hacen físicamente de la tarjeta, una forma de obtenerla discretamente es por medio de

un cajero automático, colocando en la ranura, donde se debe introducir la tarjeta, un dispositivo que lleva una especie de tope para que la tarjeta al ser introducida quede bloqueada; Posteriormente uno de los delincuentes se acerca al usuario de la tarjeta y le comenta que debe marcar una serie de números y agregar su clave personal, para poder liberar su tarjeta, ignorando que el delincuente estará mirando y memorizando dicha clave. El siguiente paso consiste en esperar que el dueño de la tarjeta se vaya, y una vez que se retire, un segundo delincuente (cómplice del primero) se acerca al cajero y retira la tarjeta, con lo que ya disponen de la tarjeta y de la clave personal.

En cuanto a la segunda forma de actuar consiste en obtener los datos de la tarjeta y posteriormente grabarlos en otra o emplear dichos datos en transacciones vía informática (por internet). En el mercado existen lectoras y grabadoras de bandas magnéticas, que facilitan a los delincuentes esta tarea. Otros dos métodos, aparte de las técnicas ya mencionadas, de conseguir estos datos son las siguientes:

1.- Por medio del dispositivo que permite abrir la puerta del cajero automático, al pasar la tarjeta por el mismo, si bien es cierto que este dispositivo existe en algunas entidades bancarias, en otras son colocados por delincuentes, ya que en el momento de pasar la tarjeta por el lector se están grabando los datos contenidos en la banda magnética, y para poder operar solo tienen que reproducirla y conseguir la clave secreta, lo cual se logra al colocar una cámara que graba como pulsamos los números.

2.- Colocar sobre el cajero automático una fachada falsa, consistente en el *display* con el teclado numérico y la ranura para la tarjeta, de esta manera graban los datos de la tarjeta al introducirla y la clave secreta al momento de teclearla; en este método el dueño de la tarjeta únicamente cree que el cajero esta estropeado y procede a retirar su tarjeta, ya que al pulsar la clave personal le sale un mensaje en el que se le indica que la operación ha sido cancelada.

Por lo tanto queda claro que las tarjetas ya sean de crédito o débito, comienza a ser un mecanismo de pago no del todo seguro, ya que podemos ser víctimas sin enterarnos, percatándonos del fraude solo hasta el momento en el que volvamos a utilizarlas.

2. 3. 2 El FRAUDE INFORMÁTICO EN LA OBTENCIÓN DE DATOS PERSONALES Y SU PROBLEMÁTICA

Este tipo de fraude tiene la finalidad de obtener, mediante el empleo de un medio informático, la información que consideramos de interés personal, es decir tanto a aquella información que contenga cualquier dato que pueda ser identificable a una persona (como las características físicas, su nombre, numero de afiliación al seguro social); como aquella que haga referencia a su domicilio, número de teléfono, patrimonio, ideología, origen étnico y racial, o a aspectos morales, emocionales, de la vida afectiva familia, etcétera. Dicha información está comprendida como Datos Personales, los cuales pueden ser utilizados posteriormente a su obtención para cometer aun más prácticas fraudulentas u otros tipos de delitos.

La utilización masiva de los datos de carácter personal se facilitó con la digitalización de la información, o en otras palabras al emplear a la informática para el tratamiento de dicha información; lo cual ha provocado una gran amenaza, puesto que al introducirse en la esfera privada e íntima de las personas, pone al descubierto sus gustos, preferencias, e incluso actividades que debieran de estar vedadas a los ojos de terceros.

La regulación de los Datos Personales, no son materia del presente análisis, ya que implicaría la desviación de nuestro tema principal. Por ello nos limitaremos a decir que actualmente México no cuenta con un marco jurídico a nivel federal que regule y proteja el manejo adecuado de los datos personales, solo en algunos estados de la república se han tomado algunas medidas en lo particular, tal es el caso de la Ley de Protección de Datos Personales del Estado de Colima.

La falta de regulación en este tema ha provocando que su mal uso se haga de manera indiscriminada; un mal manejo de esos datos personales se da en las transacciones de bienes o servicios en línea, y en la mayoría de las actuales prácticas de mercadotecnia (La Mercadotecnia es el conjunto de principios y conocimientos que buscan el aumento del comercio, especialmente de la demanda.), y al no hacer un uso adecuado de los datos personales se provoca que el titular de los datos resulte afectado con prácticas comerciales

que pueden ser engañosas y fraudulentas tanto a nivel nacional como internacional; es por ello que en la actualidad es urgente la necesidad de proteger legalmente a los individuos, del uso indiscriminado y potencialmente lesivo de sus datos personales, causados por el avance tecnológico en materia de informática y en redes de cómputo.

En cuanto a la forma de obtenerlos, podemos decir que existen una infinidad de técnicas y métodos para ello, especialmente en el proceso de comunicación, ya que la transmisión de estos datos a través de un medio informático representa múltiples oportunidades para que puedan ser interceptados y copiados, o simplemente existe la posibilidad de introducirse directamente en los equipos donde dicha información está físicamente almacenada. Entre las principales prácticas fraudulentas para obtener los datos personales, destacan las siguientes:

- Adquisición de música y juegos
- *Data Leakage*
- Loterías y otros premios virtuales
- Paquetes vacacionales
- *Phishing*
- *Phreaking*
- Pirámides de Valor
- Pornografía
- *Scam* (Ofertas de trabajo o trabajo en casa)
- *Spam*
- Venta de títulos y grados académicos

A manera de conclusión para este tema diremos que la protección de los datos personales debería ser un derecho fundamental, puesto que el individuo tiene derecho a decidir cuándo, cómo y quién va a tener acceso a su información personal. De tal modo que los datos personales deben usarse solo para los fines que fueron obtenidos expresamente y con el consentimiento explícito e inequívoco del dueño; su mala o buena utilización sin dicho consentimiento, viola el derecho a la intimidad y privacidad de las personas, es decir la información solo puede ser conocida por individuos autorizados.

2. 3. 3 EL FRAUDE INFORMÁTICO EN LAS SUBASTAS ELECTRÓNICAS

Una vez más estamos en presencia de la notable vulnerabilidad que tiene nuestra sociedad, por la falta de regulación jurídica informática en la comisión de actos penalmente reprochables, puesto que a través de las denominadas plataformas de comercio (páginas web donde particulares colocan a la venta y al mejor postor, productos de cualquier tipo, desde material informático o electrónico hasta equipos de imagen y sonido, e incluso joyas, mobiliario, ropa, calzado, etc.), se han incrementado los fraudes informáticos. A estas plataformas también se les conoce como casas de subasta en línea, o subastas electrónicas, términos que nos indican que se realizan por internet.

El concepto de la palabra subasta nos remite a la venta pública de bienes que se hace al mejor postor, regularmente por mandato y con intervención de un juez u otra autoridad; y a la adjudicación que en la misma forma se hace de una contrata, generalmente de servicio público; como la ejecución de una obra, el suministro de provisiones, etcétera; dicho vocablo proviene del latín *Sub* (bajo) y *hasta* (Lanza), es decir bajo la lanza. Según la costumbre romana se colocaba una lanza o un asta, sobre alguna cosa, para indicar que se ponía en venta pública y que el acto de la venta estaba bajo la protección de la fuerza pública. Esto último en las subastas electrónicas no sucede, pues los sitios de subastas operan sin ninguna restricción jurídica por parte de los ordenamientos de nuestro país.

El modo de operar de las subastas electrónicas es el siguiente; se comienza por describir el artículo que el vendedor (propietario) pone a disposición del sitio en línea, posteriormente dicho artículo se ofrece, a partir de un precio base, de modo que a quien haga las mejores propuestas económicas en un determinado tiempo, y previo pago, se le cederá la propiedad o la adjudicación de lo ofrecido.

Las casas de subastas *online* (en línea), es decir por internet, generan una imagen de confianza en el consumidor invitándole, con señuelos, a realizar la compra a través de su web, donde ellos cobrará una comisión en función del precio de la venta; dichas casas no son capaces de garantizar los derechos a los usuarios, ya que no proporcionan ningún dato que nos sirva para identificar

a la persona que proporciona el objeto a subastar. Por lo tanto en estos casos las garantías para el usuario son nulas y las reclamaciones muy complejas. El método más usual para invitar a estas páginas web es a través del envió de correos electrónicos, los cuales ofrecen artículos a precios muy bajos, pero en realidad no son más que otro engaño muy bien pensado y perpetrado.

Los fraudes que se producen una vez que ya se ha adjudicado el bien a cierta persona por medio de la subasta y el dinero del precio pactado ya ha sido cobrado, admiten múltiples variantes, de las cuales podemos citar las siguientes:

1.- El usuario no recibe en su domicilio el producto adquirido.
2.- El producto recibido no tiene ningún valor.
3.- Se recibe un producto cuyas características no corresponden con las prometidas, es decir compró un producto y se le mandó otro.
4.- Compra productos nuevos y reciben productos usados o arreglados, sin sus accesorios originales.
5.- El producto que se recibió está defectuoso, es decir no funciona como debería.

La actividad fraudulenta de los sitios de subastas en línea, puede manifestarse de dos formas; ya sea que se utilice el sitio en la web como medio, o bien considerar al sitio mismo como fraudulento. Los sitios no pueden alegar la falta de participación directa en la comisión de los fraudes por los usuarios, pues conocen detalladamente la situación y son plenamente conscientes de que el sistema es propicio para la realización de las citadas maniobras delictivas, las cuales llevan a cabo para su beneficio; por lo tanto no les conviene una reglamentación jurídica en donde todos los casos en que se produzcan fraudes dentro de las subastas en línea, las empresas prestadoras del servicio resulten penalmente responsables como partícipes necesarios del delito, debido a que ponen a disposición el medio específico de comisión del delito. Las empresas que realizan este tipo de subastas sin la autorización respectiva, se amparan en los vacíos legales que se generan en internet. Por ello es necesario que a las empresas que operan con este tipo de servicio, se les obligue a que adecuen su actividad, a lo normado por las leyes vigentes, con el fin de evitar daños potenciales a los usuarios por la falta de control.

CONCLUSIONES

Primera.- El desarrollo de la Informática debe ir acompañado de leyes que protejan al individuo de las conductas criminales que emplean medios informáticos para la comisión de delitos.

Segunda.- La obtención ilícita de dinero o de un servicio, se puede realizar, mediante la manipulación informática de sistemas o máquinas que actúan en forma automática, con el empleo de medios informáticos, al inducir un engaño o al aprovechar un error existente.

Tercera.- Los programas, métodos y técnicas por medio de los cuales se puede realizar el fraude informático, aumentan día a día, junto con el ingenio y perspicacia de los delincuentes para poder efectuarlo.

Cuarta.- El crecimiento de la tecnología ha llevado, en un nivel internacional, a los juzgadores a revalorar los tipos penales existentes, a efecto de determinar en cuál tipo penal encuadra determinada conducta relacionada con los avances tecnológicos e informáticos.

Quinta.- El Derecho Mexicano se ha quedado con mucho rezago en la regulación del fraude informático, el cual requiere una atención inmediata, tal y como lo hemos comentado en el tema 1.5 relativo a la situación internacional del fraude informático.

Sexta.- Los datos personales en la actualidad ameritan una protección jurídica efectiva, ya que su mal uso afecta el derecho a la privacidad e intimidad de cada persona y dan pauta para la comisión de nuevos fraudes informáticos.

Séptima.- El Fraude Informático sigue cumpliendo con los elementos del tipo penal de Fraude, razón por la cual resulta ilógica la creación de un nuevo tipo, por lo tanto la propuesta que se hace en este sentido, es la de añadir como un agravante de la pena, la comisión de este delito mediante el empleo de un medio informático u otro artificio semejante.

La modificación a nivel federal de este artículo podría quedar como sigue:

Artículo 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.

El delito de fraude se castigará con las penas siguientes: I.- Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario; II.- Con prisión de 6 meses a 3 años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario; III.- Con prisión de tres a doce años y multa hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.

Al que realizase esta conducta valiéndose de un medio informático u otro artificio semejante que sea capaz de ingresar, insertar, sustraer, suprimir, modificar o alterar la información de un sistema informatizado, ya sea en programas o en cualquier etapa del procesamiento de la información (entrada, almacenamiento, salida o la transmisión de los datos), se le aumentará hasta en una mitad la pena que corresponda; si el sujeto activo cuenta con conocimientos importantes en el campo de la informática se hará acreedor a tres cuartas partes más de la sanción privativa de libertad y multa de hasta veinte mil días de salario mínimo general vigente; independientemente si tenía permitido el acceso o no al sistema informático.

En este trabajo se ha pretendido proporcionar información para conocer la problemática del fraude Informático, y por otro lado una propuesta que intenta ser un punto de partida para descubrir la mejor manera de regular dicho fraude. El problema es complejo ya que el uso de las nuevas tecnologías trae consigo nuevas tendencias delictivas, que ocasionan simultáneamente un gran daño a la sociedad. Todavía estamos a tiempo de resolver un problema que día a día cobrará mayor importancia, dado al flujo de información y a los actos que se realizan a través de medios informáticos, considerando que la información es uno de los más valiosos tesoros que la especie humana posee, ya que forma parte de la comunicación y de la vida misma (este último junto con la salud física y mental, a mi consideración, conforman el más grande tesoro.).

GLOSARIO

Antivirus: programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido o un disquete. Al mismo tiempo sirve para evitar que cualquier tipo de virus entre a la computadora y se ejecute.

Archivo: Es una colección de textos o datos guardados bajo un nombre que les es propio. La mayoría de la información que contiene la computadora está almacenada en archivos.

Automático (a): Dicho de un mecanismo, equipo, aparato o dispositivo que funciona en todo o en parte por sí solo.

Automatización: Realización de una combinación específica de acciones por una máquina, sin la ayuda de personas. Acción y efecto de automatizar.

Backdoor (puerta trasera) ó Trapdoor (puerta trampa): Sección oculta de un programa de computadora, que sólo se pone en funcionamiento si se dan condiciones o circunstancias muy particulares en el programa. Consiste en introducir interrupciones en la lógica de los programas.

Base de datos: conjunto de datos organizados de modo tal que resulte fácil acceder a ellos, gestionarlos y actualizarlos.

Carding: Uso de tarjetas de crédito de otras personas, generación de nuevas tarjetas de crédito para realizar pagos a sistemas de compra a distancia (principalmente). En general, cualquier actividad fraudulenta que tenga que ver con las tarjetas de crédito.

Chip: Pequeño circuito integrado que realiza numerosas funciones en ordenadores y dispositivos electrónicos. Circuito muy pequeño que está compuesto por miles a millones de transistores impresos sobre una oblea de silicio. Es la abreviatura de **Microchip** (chip miniaturizado).

Circuito electrónico: Conjunto de conductores que recorre una corriente eléctrica, y en el cual hay generalmente intercalados aparatos productores o consumidores de esta corriente.

Circuito integrado: Circuito electrónico miniaturizado formado por componentes extremadamente pequeños (numerosos transistores, diodos, condensadores y resistencias), los cuales se colocan en una única pieza plana de poco espesor de un material conocido como semiconductor. También son conocidos como microchips o chips.

Comando (C*ommand*): Instrucción que un usuario da al sistema operativo de la computadora para realizar determinada tarea.

Correo electrónico (e-mail): Es el medio por el cual se intercambian mensajes los usuarios en Internet a través de programas específicos para su gestión, pueden incluir texto y elementos multimedia.

Cortafuegos (**Firewall**): Programas que impiden el acceso a personas no autorizadas a un ordenador o red. Con estos dispositivos se pretende mantener seguros la información que se encuentran en un sistema.

Dato (Data): Son los hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean manipulados, transmitidos o procesados por los medios automáticos y a los cuales se les asigna un significado. Véase también el concepto de información.

Demodulación: Proceso consistente en recuperar información contenida en una onda transmisora modulada.

Digital: Perteneciente o relativo a los dedos; Referente a los números dígitos. Este vocablo se emplea para referirse a los instrumentos de medida que la expresan con ellos, como el Reloj digital.

Digitar: Incorporar datos a la computadora utilizando el teclado. Es el tratamiento automático de la información por medio de las computadoras

Fibra óptica: Tecnología para transmitir información como pulsos luminosos a través de un conducto de fibra de vidrio. La fibra óptica transporta mucha más información que el cable de cobre convencional. La mayoría de las líneas de larga distancia de las compañías telefónicas utilizan la fibra óptica.

Hardware: Son todos los componentes físicos de la computadora, así como sus periféricos, considerados en forma independiente de su capacidad o función, pueden incluir herramientas, tarjetas, implementos, instrumentos, conexiones, ensamblajes y partes. Componentes electrónicos que conforman un sistema de computación.

Impresora: dispositivo periférico que reproduce textos e imágenes en papel. Los principales tipos son: de matriz de puntos, de chorro de tinta y láser.

Información: Es la agregación de datos que tiene un significado específico más allá de cada uno de éstos. Un ejemplo: 2, 0, 0 y 7 son datos; y 2007 es una información. Es el resultado del procesamiento de datos. Todo aquello que permite adquirir cualquier tipo de conocimiento. E todo mensaje que logra disminuir la incertidumbre

Informática: Es el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de las computadoras. Es la disciplina o ciencia que estudia el tratamiento automático

(creación, procesamiento, almacenamiento y transmisión), de la información (datos), utilizando ordenadores electrónicos.

Inteligencia artificial: simulación de los procesos de la inteligencia humana, por medio de sistemas de computación.

Internet: Es una red pública mundial de computadoras, que ofrece posibilidades para desarrollar aplicaciones internas de una empresa o de interconexión con clientes y/o proveedores. Las redes que son parte de esta red se pueden comunicar entre sí a través de un protocolo denominado, TCP/IP (Transmission Control Protocol/ Internet Protocol). Fue concebida a fines de la década de 1960 por el Departamento de Defensa de los Estados Unidos; más precisamente, por la ARPA. Se la llamó primero Arpanet y fue pensada para cumplir funciones de investigación. Su uso se popularizó a partir de la creación de la World Wide Web (www). Actualmente es un espacio público utilizado por millones de personas en todo el mundo como herramienta de comunicación e información. Generalmente se define como la red de redes mundial o Sistema mundial de redes de computadoras interconectadas.

Login: Acción de conectarse a un sistema ingresando un nombre de usuario y una contraseña, en otras palabras es el procedimiento de identificarse frente a un sistema para acceder a él y luego usarlo. Este identificativo más el password o nip correcto permite acceder a información restringida.

Medios Informáticos: Son todos los aparatos, maquinas, artefactos, dispositivos, herramientas, programas, circuitos integrados (chips o microchips) y sistemas, asociados al tratamiento automático de la información; es decir es todo aquello que sirve para que la informática cumpla con sus fines.

Memoria: Almacenamiento primario de una computadora.

Microprocesador (microprocessor): es el chip más importante de una computadora. Su velocidad se mide en MHz.

Módem (**mo**dulador-**dem**odulador): Aparato que convierte las señales digitales en analógicas y viceversa. Dispositivo periférico que conecta la computadora a la línea telefónica para permitir la comunicación entre dos o más computadoras.

Online: Conectado en línea. Estado en que se encuentra una computadora cuando se conecta directamente con la red a través de un dispositivo, por ejemplo, un módem.

Ordenador, Computador o Computadora: Comúnmente se utilizan estos tres términos como sinónimos. Es la unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas

operaciones aritméticas o lógicas. En otras palabras es el dispositivo capaz de solucionar problemas aceptando datos, realizando operaciones predefinidas sobre ellos y proporcionando los resultados de estas operaciones.

Página web: una de las páginas que componen un sitio de la www. Un sitio web agrupa un conjunto de páginas afines. A la página de inicio se la llama "home page".

Password o nip (Contraseñas): Son las claves de acceso personal utilizadas para ingresar a una red o a un sistema. Técnicamente son las secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder de manera segura a la data o a la información contenidas en un sistema; Se usa como medio de identificación inicial y sirve para verificar que un usuario es realmente quien dice ser. Coloquialmente es una herramienta de seguridad empleada para identificar a los usuarios autorizados de un programa o de una red y para determinar sus privilegios, como el de solo lectura, el de escritura, o el de copiado de archivos.

Periférico (s): Es todo dispositivo que se conecta a la computadora. Por ejemplo: teclado, monitor, mouse, impresora, escáner, teléfono, módem, cámara web (Webcam), bocinas, etcétera.

Procesador (processor): Conjunto de circuitos lógicos que procesa las instrucciones básicas de una computadora.

Procesamiento de información o procesamiento de datos: Realización sistemática de operaciones sobre la información (tales como manejo, fusión, organización), para obtener un resultado deseado.

Proceso. Manipular datos o realizar otras operaciones de acuerdo a un programa.

Programa: Plan, rutina, serie o secuencia de instrucciones utilizados para realizar operaciones específicas (como el programa Word para un trabajo de texto en particular o un programa de cálculo para resolver un problema dado), a través de un computador, para obtener un resultado deseado.

Realidad virtual: Simulación de un medio ambiente real o imaginario que se puede experimentar visualmente en tres dimensiones. La realidad virtual puede además proporcionar una experiencia interactiva de percepción táctil, sonora y de movimiento.

Red: en tecnología de la información, una red es un conjunto de dos o más computadoras interconectadas.

Redirigir: Cambiar el destino de algo. Por ejemplo, redirigir una llamada es hacer que suene en un teléfono distinto del que se intentaba llamar.

Robótica: Técnica que aplica la informática al diseño y empleo de aparatos que, en sustitución de personas, realizan operaciones o trabajos, por lo general en instalaciones industriales.

Sistema: Conjunto de elementos relacionados entre sí, que trabajan juntos de forma ordenada para obtener un resultado deseado. Conjunto estructurado de unidades interrelacionadas que se definen por oposición.

Sistema operativo: Programa o conjunto de programas que efectúan la gestión de los procesos básicos de un sistema informático, y permite la normal ejecución del resto de las operaciones, es decir es el programa que administra los demás programas en una computadora; sin el nada en la computadora funcionaría puesto que este programa de control dirige todo su hardware; entre ellos podemos mencionar a Linux, Macintosh, Unix, Windows 95, Windows 98, Windows 2000, Windows XP, y al más actual el Microsoft Windows Vista.

Software: Término general que designa los diversos tipos de programas usados en computación, es decir son todos los programas del sistema (paquetería o utilería), expresados en un lenguaje que la computadora entiende y puede ejecutar para realizar una tarea específica.

Tratamiento de la información: Aplicación sistemática de uno o varios programas sobre un conjunto de datos para utilizar la información que contienen. Modo de trabajar cierta información para su transformación.

Usuario: Es toda aquella persona que usa un sistema de información.

Videoconferencia: Conversación entre dos o más personas que se encuentran en lugares diferentes pero pueden verse y oírse al utilizar una webcam.

Virtual. Se dice de la representación en una computadora de algo que no existe, o no está presente en ese lugar. Que tiene existencia aparente y no real; que tiene virtud para producir un efecto, aunque no lo produce de presente.

Webcam o cámara web: Es una videocámara que registra imágenes a las cuales se puede acceder desde un sitio web.

World Wide Web (WWW): También conocido como Red mundial o Telaraña mundial. **Es la parte multimedia de Internet**, que implica la introducción de gráficos e hipertextos, es decir, los recursos creados en HTML y sus derivados. Es el sistema de información global desarrollado en 1990 por Robert Cailliau y Tim Berners-Lee en el CERN (Consejo Europeo para la Investigación Nuclear) que fue la base para la explosiva popularización de Internet a partir de 1993.

FUENTES CONSULTADAS

Libros.

CÁMPOLI, Gabriel Andrés. Delitos Informáticos en la Legislación Mexicana, Instituto Nacional de Ciencias Penales, México, 2005.

DÍAZ ARANDA, Enrique. Derecho Penal Parte General, Porrúa, México, 2003.

MOTO SALAZAR, Efraín. Elementos del Derecho, 44ª edición, Porrúa, México, 1998.

NAVA GARCÉS, Alberto Enrique. Análisis de los Delitos Informáticos, Porrúa, México, 2005.

ROMEO CASABONA, Carlos María. Poder Informático Y Seguridad Jurídica, Fundesco, Madrid España, 2002.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. Las Garantías de Seguridad Jurídica, Nuevo Milenio, México, 2004.

TÉLLEZ VALDÉS, Julio. Derecho Informático, 3ª edición, Mc Graw Hill, México, 2005.

Legislativas.

Constitución Política de los Estados Unidos Mexicanos.
Código Penal Federal.
Ley de Instituciones de Crédito.
Código Penal Para El Distrito Federal.
Código Penal para el Estado de Guanajuato.
Código Penal Para el Estado de Sinaloa.

Electrónicas.

www.delitosinformaticos.com,
www.cosnet.sep.gob.mx/ciberseguridad.

Documentos electrónicos.

BIBLIOTECA DE CONSULTA MICROSOFT. Encarta 2004, Edición 1993-2003, disco compacto, Microsoft Corporation, México, 2004.