UNIVERSIDAD DE QUINTANA ROO

División de Ciencias Sociales y Económico Administrativas

EL DERECHO DE LA INFORMÁTICA EN MÉXICO

TRABAJO MONOGRÁFICO
Para obtener el Grado de
Licenciado en Derecho

PRESENTA

JOSÉ ALFREDO LÓPEZ HERNÁNDEZ

SUPERVISORES:
LIC. IGNACIO ZARAGOZA ÁNGELES
LIC. THALÍA HERNÁNDEZ ROBLEDO
LIC. ELIZABETH MORENO REJÓN

Chetumal, Quintana Roo 2004

UNIVERSIDAD DE QUINTANA ROO

Trabajo monográfico elaborada bajo la supervisión del comité de asesoría y aprobado como requisito parcial, para obtener el grado de:

LICENCIADO EN DERECHO

COMITÉ:

SUPERVISOR: _____
LIC. IGNACIO ZARAGOZA ÁNGELES

SUPERVISOR: _____
LIC. THALÍA HERNÁNDEZ ROBLEDO

SUPERVISOR: _____
LIC. ELIZABETH MORENO REJÓN

Chetumal Quintana Roo, Octubre de 2004.

AGRADECIMIENTOS

A DIOS... POR SU ETERNA E INFINITA BONDAD

A MI MADRE... POR SU AMOR Y APOYO INCONDICIONAL

A MI MAMACITA LUISA... POR SU MARAVILLOSO RECUERO

A EDUARDO... POR ESTAR PRESENTE EN MI VIDA

A MI FAMILIA MATERNA... POR SER UNA GRAN FAMILIA

A THALIA, LIZ Y LALO... POR SER VERDADEROS AMIGOS

A DOÑA GODE... POR SU CARIÑO Y BUENOS CONSEJOS

A ALAIN... POR SU CONFIANZA Y BUEN EJEMPLO

Y EN GENERAL A TODAS LAS PERSONAS QUE EN EL PASADO, EN EL PRESENTE Y EN EL FUTURO, HAN ESTADO Y ESTARAN LIGADAS ESTRECHAMENTE A MI VIDA.

EL DERECHO DE LA INFORMATICA EN MEXICO

INDICE

INTRODUCCIÓN

Es por todos conocido, que Internet, hoy en día, se ha convertido en un instrumento de comunicación, obtención de recursos, intercambios electrónicos, lo que conlleva importantes repercusiones en los distintos sectores sociales, económicos, jurídicos y culturales.

Internet hace posible la interconexión, en el ámbito mundial, de todo aquel que esté dispuesto a sumergirse en un océano que, hoy por hoy, no conoce límites, siendo para ello necesario un equipo terminal de computadora, un mediador electrónico entre la línea telefónica y el equipo terminal (módem). Al mismo tiempo, Internet es el gran escaparate mundial, un escaparate virtual, donde poder ofrecer nuestros productos, nuestros servicios, y por tanto es un gran centro comercial, abierto ininterrumpidamente 24 horas al día, 7 días a la semana, sin limitación de horario alguno.

El ciberespacio, es un mundo virtual en el que los defectos y malos hábitos del ser humano se reproducen rápidamente a la misma velocidad que permiten nuestras computadoras, así como en todo el planeta, ampara la rápida transmisión de mensajes y permite el acceso a toda la información introducida en Internet. Al igual que las ventajas que acarrea esto, se asocian las deformaciones y el mal trato que se le da a esta herramienta en cualquier sistema y que ratifica nuevamente que el mal no está en los medios sino en las personas que lo utilizan. La necesidad de prevenir y sancionar estos malos usos en Internet que es la cuna de la delincuencia, por lo que se hace necesario determinar las alteraciones mas

frecuentes que se producen para cortar de raíz esta modalidad delictiva

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En algunas de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

Dar un concepto sobre delitos informáticos no es una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión "delitos informáticos", este consignada en los códigos penales, lo cual en nuestro país, al igual que en muchos otros, no ha sido objeto de tipificación aún; solo con excepción del estado de Sinaloa que ya incluyó esta modalidad, como lo narraré más adelante.

Actualmente se está produciendo un intenso debate respecto a la necesidad de prevenir y sancionar estos malos usos en la red de redes que es el Internet y el objetivo de este trabajo de investigación es sugerir la inclusión dentro del código penal del estado una legislación que tipifique y penalice el mal uso de la red, porque cada día aparecen nuevos métodos de vulneración de los sistemas, aparte de los fraudes y todo el mal uso que se está dando al Internet y pienso que

nosotros nos hemos de mover con los tiempos, y estar actualizados, porque tanto en el campo de la informática como en el derecho todo cambia continuamente.

En definitiva, con la ayuda de las nuevas tecnologías, aparecen nuevos delitos y nuevas formas de comisión de delitos. Ante esto el legislador no se puede quedar de brazos cruzados y no regular este aspecto de la informática.

Por lo anterior, es que en la elaboración de este trabajo de investigación, se ensayará la utilización de la computadora y del Internet para la comisión de conductas ilegales, de igual manera analizaremos las legislaciones de algunos países en los cuales ya contemplan dichas figuras delictivas, analizaremos en su momento oportuno los argumentos que existen para que se regule la práctica y uso del Internet, y de forma personal porqué discurro que se deben de agregar los Delitos Informáticos en el Código Penal del Estado.

CAPITULO PRIMERO

DESCRIPCIÓN DEL DELITO

Concepto de derecho penal.

Derecho Penal es: "El conjunto de normas jurídicas de derecho público interno, que define los delitos y señala las penas y medidas de seguridad para lograr la permanencia del orden social".[1]

"El criminalista español Eugenio Cuello Calón lo define como el conjunto de normas que determinan los delitos, las penas que el Estado impone a los delincuentes y a las medidas de seguridad que el mismo establece para la prevención de la criminalidad".[2]

El Derecho Penal en sentido objetivo, dice Cuello Calón, "es el conjunto de normas jurídicas establecidas por el Estado que determinan los delitos, las penas y las medidas de seguridad con que aquellos son sancionados". [3]

En México Raúl Carrancá y Trujillo estima que el derecho objetivamente considerado, "es el conjunto de leyes mediante las cuales el Estado define los delitos, determina las penas impunibles a los delincuentes y regula la aplicación concreta de las mismas a los casos de incriminación".[4]

Ignacio Villalobos, en su obra "Derecho Penal Mexicano", define al Derecho Penal como "aquella rama del Derecho Público Interno, cuyas disposiciones tienden a mantener el orden político-social de una comunidad, combatiendo por medio de penas y otras medidas adecuadas a aquellas conductas que le dañan o ponen en peligro".[5]

El Derecho Penal en sentido subjetivo, consiste en la facultad del Estado para

[1] Gonzalez de la vega, francisco. Derecho Penal Mexicano. Porrúa. México, 1996, 473 p.
[2] Idem
[3] Idem
[4] Idem
[5] Villalobos, ignacio. Derecho Penal Mexicano. Op. Cit. 650 p.

determinar los casos en que deben de imponerse las penas y las medidas de seguridad. Es por esto que para Cuello Calón es el derecho del Estado a determinar, imponer y ejecutar las penas y demás medidas de lucha contra la criminalidad; es el atributo de la soberanía por el cual a todo Estado corresponde reprimir los delitos por medio de las penas; en tanto que objetivamente se forma por el conjunto de normas y de disposiciones que reglamentan el ejercicio de ese atributo: el Estado, como organización política de la Sociedad, tiene como fines primordiales la creación y el mantenimiento del orden jurídico; por tanto, su esencia misma supone el uso de los medios adecuados para tal fin".[6]

Definición de delito.

"La palabra delito proviene del verbo latino delinquere, que significa abandonar, apartarse del buen camino, apartarse del sendero señalado por la ley."[7]

Para González Quintanilla, el Delito "es un comportamiento típico, antijurídico y culpable".[8]

Para Ignacio Villalobos, el Delito "es un acto humano típicamente antijurídico y culpable".[9]

Para Rafael de Pina Vara, el Delito "es un acto u omisión constitutivo de una infracción de la ley penal"[10]

"El delito representa generalmente un ataque directo a los derechos del individuo

---

[6] Gonzalez de la vega, francisco. Derecho Penal Mexicano. Porrúa. México, 1996, 473 p.

[7] Betancourt lópez, eduardo. Teoria del delito. Op. Cit., 304 p.

[8] Gonzalez Quintanilla, jose arturo. Derecho penal mexicano (parte general). Op. Cit., 504 p

[9] Villalobos, ignacio. Derecho Penal Mexicano. Op. Cit., 650 p.

[10] Idem

(integridad física, honor, propiedad, etc.), pero atenta siempre, en forma mediata e inmediata, contra los derechos del cuerpo social. Por eso es que la aplicación de las leyes penales no se deja librada a la iniciativa o a la potestad de los particulares, salvo contadísimas excepciones: aunque la víctima de un delito perdone a su ofensor, corresponde al Poder Público perseguir y juzgar al delincuente, de ahí que el Derecho Penal sea considerado, como una de las ramas del derecho público."[11]

La definición jurídica del delito debe de ser, naturalmente, formulada desde el punto de vista del derecho, sin incluir ingredientes causales explicativos.

Aunque muchos de los autores han tratado de dar una definición que sea de carácter universal para todos los pueblos y tiempos. Esto no ha sido posible dado las circunstancias de que se necesita para dar una definición acertada de delito para todas las épocas y lugares, ya que cada una es diferente y por la tanto la definición de delito se debe de adecuar a estos lugares y tiempos.

Clasificación de los delitos.

A continuación se describen los delitos según sus diferentes características.

En función de su gravedad.

Tomando en cuenta la gravedad de las infracciones penales, se han hecho varias clasificaciones. Según una división bipartita se distinguen los delitos de las faltas; la clasificación tripartita habla de crímenes, delitos y faltas o contravenciones. En esta división se considera crímenes los atentados contra la

[11] Gonzalez Quintanilla, jose arturo. Derecho penal mexicano (parte general). Op. Cit., 504 p

vida y los derechos naturales del hombre; delitos, las conductas contrarias a los derechos nacidos del contrato social, como el derecho de propiedad; por faltas o contravenciones, las infracciones a los reglamentos de policía y buen gobierno.

En México carecen de importancia estas distinciones, porque los Códigos Penales sólo se ocupan de los delitos en general, en donde se subsumen también los que otras legislaciones se denominan crímenes; la represión de las faltas se abandona a disposiciones administrativas aplicadas por autoridades de ese carácter".[12]

Según la forma de la conducta del agente.

Por la conducta del agente, o como dicen algunos autores, según la manifestación de la voluntad, los delitos pueden ser de acción y de omisión.

Los de acción se cometen mediante un comportamiento positivo; en ellos se viola una ley prohibitiva. Eusebio Gómez afirma que "son aquellos en que las condiciones de donde deriva su resultado, reconocen como causa determinante un hecho positivo del sujeto. En los delitos de omisión el objeto prohibido es una abstención del agente, consisten en la no ejecución de algo ordenado por la ley. Para el mismo Eusebio Gómez, en los delitos de omisión, las condiciones de que deriva su resultado reconocen, como causa determinante, la falta de observancia por parte del sujeto de un precepto obligatorio"[13]. Debe agregarse que los delitos de omisión violan una ley dispositiva, en tanto los de acción infringen una prohibitiva.

---

[12] Betancourt lópez, eduardo. Teoria del delito. Op. Cit., 304 p.

[13] Idem

Los delitos de omisión suelen dividirse en delitos de simple omisión y de comisión por omisión, también llamados delitos de omisión impropia.

Los delitos de simple omisión, o de omisión propiamente dicho, consisten en la falta de una actividad jurídicamente ordenada, con independencia del resultado material que produzcan; es decir, se sancionan por la omisión misma, tal es el caso que se impone a todos la obligación positiva de auxiliar a las autoridades para la averiguación de los delitos y para la persecución de los delincuentes.

Los delitos de comisión por omisión, o impropios delitos de omisión, son aquellos en los que el agente decide no actuar y por esa inacción se produce el resultado material. Para Cuello Calón, consisten los falsos delitos de omisión en "la aparición de un resultado delictivo de carácter positivo, por inactividad, fórmula que se concretiza en la producción de un cambio en el mundo exterior mediante la omisión de algo que el derecho ordenaba hacer".[14]

Como ejemplo del delito de comisión por omisión, se cita el de la madre que, con deliberado propósito de dar muerte a su hijo recién nacido, no lo amamanta, produciéndose el resultado letal. La madre no ejecuta acto alguno, antes bien, deja de realizar lo debido.

En los delitos de simple omisión, hay una violación jurídica y un resultado puramente formal, mientras en los de comisión por omisión, además de la violación jurídica se produce un resultado material. En los primeros se viola una ley dispositiva; en los de comisión por omisión se infringe una dispositiva y una prohibitiva.

---

[14] Gonzalez de la vega, francisco. Derecho Penal Mexicano. Op. Cit., 473 p.

Por el resultado.

Según el resultado que producen, los delitos se clasifican en formales y materiales. A los primeros también se les denomina delitos de simple actividad o de acción; a los segundos se les llama delitos de resultado o de resultado material.

Los delitos formales son aquellos en los que se agota el tipo penal en el movimiento corporal o en la omisión del agente, no siendo necesaria para su integración que se produzca alguna alteración en la estructura o funcionamiento del objeto material. Son delitos de mera conducta; se sanciona la acción (u omisión) en sí misma. Como están, el delito formal con el falso testimonio, la portación de arma prohibida y la portación ilícita de enervantes.

Los delitos materiales son aquellos en los cuales para su integración se requiere la destrucción o alteración de la estructura o del funcionamiento del objeto material (homicidio, daño en propiedad ajena).

Por la lesión que causan.

Con relación al efecto resentido por la víctima, o sea en razón del bien jurídico, los delitos se dividen en delitos de daño y de peligro. Los primeros, consumados causan daño directo y efectivo en intereses jurídicamente protegidos por la pena violada, como el homicidio, el fraude, etc.; los segundos no causan daño directo a tales intereses, pero los ponen en peligro, como el abandono de personas o la omisión de auxilio. El peligro es la situación en que se colocan los bienes jurídicos, de la cual deriva la posibilidad de casación de un daño.

Por su duración.

Los delitos se dividen en instantáneos, instantáneos con efectos permanentes, continuados y permanentes.

Nuestro Código Penal Federal reformado (según Decreto publicado el 13 de enero de 1984), en su artículo 7° solo alude a tres especies de delitos en función de su duración: instantáneo, permanente o continuo y continuado". [15]

Instantáneo.

La acción que lo consuma se perfecciona en un solo momento. "El carácter de instantáneo, no se lo dan a un delito de efectos que él causa sino la naturaleza de la acción a la que la ley acuerda el carácter de consumatoria".[16] El delito instantáneo puede realizarse mediante una acción compuesta de varios actos o movimientos. Para la calificación se atiende a la unidad de acción, si con ella se consuma el delito no importando que a su vez, esa acción se descomponga en actividades; el momento consumativo expresado en la ley da la nota al delito instantáneo. Existe una acción y una lesión jurídica. El evento consumativo típico se produce en un solo instante, como el homicidio y el robo.

Actualmente la fracción I del artículo 7° del Código Penal Federal lo define así: "instantáneo, cuando la consumación se agota en el mismo momento en que se han realizado todos los elementos constitutivos."[17]

[15] Betancourt lópez, eduardo. Teoria del delito. Op. Cit., 304 p.

[16] Idem

[17] Idem

Instantáneo con efectos permanentes.

"Es aquel cuya conducta destruye o disminuye el bien jurídico tutelado, en forma instantánea, en un solo momento, pero permanecen las consecuencias nocivas del mismo".[18] El homicidio, por ejemplo, se destruye el bien jurídico de la vida y la supresión del mismo, consecuencia de la conducta, perdura para siempre; en las lesiones, el bien jurídico protegido (la salud o la integridad corporal), disminuye instantáneamente como resultado de la actividad humana, pero la alteración en la salud permanece por un determinado tiempo.

Continuado.

En este delito se dan varias acciones y una sola lesión jurídica. Es continuado en la conciencia y descontando en la ejecución. Con razón para Carrára, "la continuidad en este delito debe buscarse en la discontinuidad de la acción".[19] Se dice que el delito continuado consiste:

1° Unidad de resolución;

2° Pluralidad de acciones (discontinuidad en la ejecución);

3° Unidad de lesión jurídica;

4° Unidad de sujeto pasivo. Como ejemplo puede citarse el caso del sujeto que decide robarse veinte botellas de vino, más para no ser descubierto, diariamente se apodera de una, hasta completar la cantidad propuesta.

"Según Alimena, en el delito continuado las varias y diversas consumaciones no

[18] Idem
[19] Beccaria. Tratado de los delitos y las penas. Op. Cit., 408 p.

son más que varias partes de una consumación sola"[20] , mientras para Soler este delito se comete cuando una sola resolución delictiva se ejecuta por medio de varias acciones, cada una de las cuales importa una forma análoga de violar la ley".[21]

Nuestro Código Penal Federal no hacía referencia al delito continuado; con las reformas de 1984 lo definió en la fracción III del articulo 7º: "Cuando con una unidad de propósito delictivo y pluralidad de conductas se viola el mismo precepto legal". Con la reforma del 13 de mayo de 1996 la fracción se adicionó con la exigencia de que se trate del mismo sujeto pasivo".[22]

Permanente.

Sebastián Soler lo define en los términos siguientes: "Puede hablarse de delito permanente sólo cuando la acción delictiva misma permite, por sus características, que se le pueda prolongar voluntariamente en el tiempo, de modo que sea idénticamente violatoria del Derecho en cada uno de sus momentos"[23] Para Alimena existe el delito permanente cuando "todos los momentos de su duración pueden imputarse como consumación".[24] Permanece no el mero efecto del delito, sino el estado mismo de la consumación, a diferencia de lo que ocurre en los delitos instantáneos de efectos permanentes. En el delito permanente puede concebirse la acción como prolongada en el tiempo; hay continuidad en la conciencia y en la ejecución; tal es el caso de los delitos privativos de la libertad

[20] Idem
[21] Idem
[22] Ibid p. Ibiden p.
[23] Betancourt lópez, eduardo. Teoria del delito. Op. Cit., 304 p.

[24] Idem

como el plagio, el robo de infante, etc.

Alimena con fines exclusivamente didácticos, expresa que el delito instantáneo, es instantáneo en la conciencia e instantáneo en la ejecución; el continuado es continuado en la conciencia y discontinuo en la ejecución y, el permanente, es continuado en la conciencia y continuado en la ejecución. El mismo Alimena, expresa que el delito instantáneo puede representarse gráficamente con un punto (.); el continuado con una sucesión de puntos (...); y, el permanente, con una raya horizontal (-).[25] Para Soler el elemento acción puede presentar tres aspectos diversos con relación al tiempo:

a. "Desarrollarse y perfeccionarse en un momento relativamente corto, y entonces se está en presencia del delito instantáneo, como en el homicidio;
b. Desenvolverse sin solución de continuidad en una forma idénticamente antijurídica, dándose en ello el delito permanente, como el plagio y, finalmente,
c. consistir en una serie discontinua de acciones parciales que mutuamente se integran, formando entre todas una sola agresión de conjunto al Derecho, y eso sucede en el continuado."[26]

Porte Petit enumera como elementos del delito permanente:

"a) Una conducta o un hecho; y,

b) Una consumación más menos duradera".[27] A su vez el segundo elemento comprende tres momentos a saber:

---

[25] Idem
[26] Ibid p. Ibiden p.
[27] Beccaria. Tratado de los delitos y de las penas. Op. Cit. 408 p

1. "Un momento inicial identificado con la comprensión del bien jurídico protegido por la ley;
2. Un momento intermedio, que va desde la comprensión del bien jurídico hasta antes de la cesación del estado antijurídico; y,
3. Un momento final, coincidente con la cesación del estado comprensivo del bien jurídico".[28]

En el delito permanente se encuentran dos fases: la primera, de naturaleza activa, consiste en la realización del hecho previsto por la ley; la segunda, de naturaleza omisiva, es el no hacer del agente, con lo que impide la cesación de la compresión del bien jurídico. Contra este criterio se pronuncia Antolisei "al negar la existencia de tales fases. Para él de esos dos momentos sólo uno de ellos es trascendente, o sea precisamente aquel que va de acuerdo con la conducta por el tipo descrita".[29]

Para nosotros es de especial interés subrayar que el delito permanente requiere, esencialmente, la facultad por parte del agente activo, de remover o hacer cesar el estado antijurídico creado con su conducta.

Por el elemento interno o culpabilidad.

Teniendo como base la culpabilidad, los delitos se clasifican en dolosos y culposos. También se agregan los llamados preterintencionales.

De conformidad con el Código Penal del Distrito Federal, las acciones y omisiones delictivas solamente pueden realizarse dolosa o culposamente (artículo

[28] Idem
[29] Betancourt lópez, eduardo. Teoria del delito. Op. Cit., 304 p.

8°)."[30]

El delito es doloso cuando se dirige la voluntad consciente a la realización del hecho típico y antijurídico, como en el robo, en donde el sujeto decide apoderarse y se apodera, sin derecho, del bien mueble ajeno. En la culpa no se requiere el resultado penalmente tipificado, mas surge por obrar sin las cautelas y precauciones exigidas por el Estado para asegurar la vida en común, como en el caso del manejador de un vehículo que, con manifiesta falta de precaución o cuidado, corre a excesiva velocidad y mata o lesiona a un transeúnte. Es preterintencional cuando el resultado sobrepasa a la intención; si el agente, proponiéndose golpear a otro sujeto, lo hace caer debido al empleo de violencia y se produce la muerte; solo hubo dolo respecto a los golpes, pero no se quiso el resultado letal.

Simples y complejos.

En función de su estructura o composición, los delitos se clasifican en simples y complejos. "Llámense simples aquellos en los cuales la lesión jurídica es única, como el homicidio. De ellos la acción determina una lesión jurídica inescindible. Delitos complejos son aquellos en los cuales la figura jurídica consta de unificación de dos infracciones, cuya fusión da nacimiento a una figura delictiva nueva, superior en gravedad a las que la componen, tomadas aisladamente."[31] Edmundo Mezger, por su parte, estima que el delito complejo se forma de la

[30] Codigo penal del distrito federal. Op. Cit. 420 p.
[31] Beccaria. Tratado de los delitos y de las penas. Op. Cit. 408 p

fusión de dos o más".[32]

No es lo mismo delito complejo que concurso de delitos. En el delito complejo la misma ley en un tipo crea el compuesto como delito único, pero en el tipo intervienen dos o más delitos que pueden figurar por separado; en cambio, en el concurso las infracciones no existen como una sola, sino separadamente, pero es un mismo sujeto quien las ejecuta.

El delito de robo puede revestir las dos formas, es decir, es dable considerarlo como delito simple, cuando consiste en mero apoderamiento de bienes muebles ajenos, sin derecho y sin consentimiento de la persona autorizada para disponer de los mismos con arreglo a la ley; pero el Código Penal Federal vigente erige el artículo 381 bis, una calificativa (agravadora de la penalidad del robo simple) para el robo cometido en casa habitación; formase así un tipo circunstanciado que subsume el robo y el allanamiento de morada, delitos que poseen vida independiente; mas si el ilícito patrimonial de referencia se realiza en lugares habitados o destinados para habitación, no es dable aplicar las penas de allanamiento de morada, sino precisamente las correspondientes a la figura compleja".[33]

Delitos unisubsistentes y plurisubsistentes.

Por el número de actos integrantes de la acción típica, los delitos se denominan unisubsistentes y plurisubsistentes; los primeros se forman por un solo acto, mientras los segundos constan de varios actos. Expresa Soler "que el delito

[32] Idem
[33] Ibid p. Ibiden p.

plurisubsistente, a diferencia del complejo, cada uno de los actos integrantes de una sola figura no constituye, a su vez, un delito autónomo. Así, sigue diciendo, para imputar el ejercicio ilegal de la medicina es preciso que la actividad imputada conste de varios hechos homogéneos, pues para la existencia del delito es requerida la habitualidad. El delito plurisubsistente es el resultado de la unificación de varios actos, naturalmente separados, bajo una sola figura; el complejo, en cambio, es el producto de la fusión de dos hechos en sí mismos delictuosos. El delito plurisubsistente es fusión de actos; el complejo, fusión de figuras delictivas".[34]

El delito plurisubsistente se identifica con el llamado "de varios actos", sean estos idénticos o no; en tales condiciones, un mismo delito se da unas veces mediante actos y otras como uno solo, como ocurre en el homicidio, cuyo elemento objetivo puede manifestarse en movimiento único o por varios y el conjunto acarrea el resultado letal. Siguiendo a Soler, solo consideramos plurisubsistente el delito que comporta en su elemento objetivo una repetición de conductas similares que aisladamente no devienen delictuosas, por que el tipo se colma del concurso de ellas. De acuerdo con este punto de vista, el homicidio siempre es unisubsistente, mientras el contemplado por la fracción II del articulo 403 es plurisubsistente, el cual dice: "Se impondrán.... a quienes voten mas de una vez en una sola elección"[35], porque cuando esa conducta ocurre una sola ocasión, no se integra el tipo y, en consecuencia, no se conforma el delito.

[34] Betancourt lópez, eduardo. Teoria del delito. Op. Cit., 304 p.

[35] Beccaria. Tratado de los delitos y de las penas. Op. Cit. 408 p

Delitos unisubjetivos y plurisubjetivos.

Esta clasificación atiende a la unidad o pluralidad de sujetos que intervienen para ejecutar el hecho descrito en el tipo. El peculado, por ejemplo, es delito unisubjetivo, por ser suficiente, para colmar el tipo, la actuación de un solo sujeto que tenga el carácter de encargado de un servicio público y sólo él concurre con su conducta a conformar la descripción de la ley, pero es posible su realización por dos o más; también son unisubjetivos el homicidio, el robo, la violación, etc. El adulterio, al contrario, es un delito plurisubjetivo, por requerir, necesariamente, en virtud de la descripción típica, la concurrencia de dos sujetos para integrar el tipo (a menos que opere en favor de uno de ellos, por ejemplo, una causa de inculpabilidad por error de hecho esencial e insuperable); igualmente la asociación delictuosa, en donde se exige típicamente el concurso de tres o más individuos.

Por la forma de su persecución.

Como una reminiscencia del periodo de la venganza privada, existe en las legislaciones un grupo de delitos que solo pueden perseguirse si así lo manifiesta el ofendido o sus legítimos representantes. Estos delitos son llamados privados o de querella necesaria, cuya persecución únicamente es posible si se llena el requisito previo de la querella de la parte ofendida; mas una vez formulada la querella, la autoridad está obligada a perseguir. Manuel Rivera Silva opina que "no deben de existir delitos perseguibles según el criterio de los ofendidos: el Derecho Penal tan solo debe tomar en cuenta intereses sociales y, por lo mismo,

no abrazar situaciones que importen intereses de carácter exclusivamente particular. Si el acto quebranta la armonía social, debe perseguirse independientemente de que lo quiera o no la parte ofendida y si por cualquier razón vulnera únicamente intereses particulares, ese acto debe desaparecer del catálogo de los delitos para ir a hospedarse a otra rama del derecho".[36]

La razón por la cual se mantienen en las legislaciones estos delitos perseguibles por querella de la parte ofendida, se basa en la consideración de que, en ocasiones la persecución oficiosa acarrearía mayores daños que la misma impunidad del delincuente.

Los delitos perseguibles previa denuncia (conocidos como "perseguibles de oficio") que puede ser formulada por cualquier persona, son todos aquellos en los que la autoridad está obligada a actuar, por mandato legal, persiguiendo y castigando a los responsables, con independencia de la voluntad de los ofendidos. Consecuentemente, en los delitos perseguibles por denuncia no surte efecto alguno el perdón del ofendido, a la inversa de lo que ocurre en los de querella necesaria.

La mayor parte de los delitos se persiguen de oficio y sólo un reducido número a petición de la parte agraviada. Entre éstos pueden citarse el adulterio, el estupro, el abuso de confianza y otros delitos patrimoniales. Actualmente se observa la tendencia a aumentar el número de los delitos perseguidos por querella y que antes requerían denuncia.

---

[36] Villalobos, ignacio. Derecho Penal Mexicano. Op. Cit., 650 p.

Delitos comunes, federales, oficiales, militares y políticos.

Esta clasificación es en función de la materia.

Los delitos comunes constituyen la regla general; son aquellos que se formulan en las leyes dictadas por las legislaturas locales; en cambio, los federales se establecen en leyes expedidas por el Congreso de la Unión."[37]

Los delitos oficiales son los que comete un empleado o funcionario público en el ejercicio de sus funciones (mejor dicho en abuso de ellas).

Los delitos del orden militar afectan la disciplina del Ejército. La Constitución General de la República, en el artículo 13, prohíbe a los tribunales militares extender su jurisdicción sobre personas ajenas al Instituto Armado.

"Los delitos políticos no han sido definidos de manera satisfactoria. Generalmente se incluyen todos los hechos que lesionan la organización del Estado, en sí misma o en sus órganos o representantes. El articulo 144 reformado del Código Penal Federal vigente, considera delitos de carácter político los de rebelión, sedición, motín y el de conspiración para cometerlos".[38] El anteproyecto de 1949 los define así: "Para todos los efectos legales se consideran como de carácter político los delitos contra la seguridad del Estado, el funcionamiento de sus órganos o los derechos políticos reconocidos por la Constitución."[39]

Para el profesor Fernando Martínez Inclan, lo que caracteriza al delito político es el dolo específico, o sea el propósito, por parte del agente, de alterar la estructura

[37] Beccaria. Tratado de los delitos y de las penas. Op. Cit. 408 p

[38] Beccaria. Tratado de los delitos y de las penas. Op. Cit. 408 p

[39] Idem

o las funciones fundamentales del Estado."[40]

Clasificación legal.

El Código Penal Federal de 1931, en el libro Segundo, reparte los delitos en veinticuatro Títulos, a saber: "Delitos contra la seguridad de la Nación; Delitos contra el Derecho Internacional; Delitos contra la humanidad; Delitos contra le seguridad pública; Delitos en materia de vías de comunicación y de correspondencia; Delitos contra la autoridad; delitos contra la salud; Delitos contra la moral pública y las buenas costumbres; Revelación de secretos y acceso ilícito a sistemas o equipos de informática; Delitos cometidos por servidores públicos; Delitos cometidos contra la administración de justicia; Responsabilidad profesional; Falsedad; Delitos contra la economía pública; Delitos sexuales, (ahora llamados delitos contra la libertad y el normal desarrollo psicosexual); Delitos contra el estado civil y bigamia; Delitos en materia de inhumaciones y exhumaciones; Delitos contra la paz y seguridad de las personas; Delitos contra la vida y la integridad corporal; Delitos contra el honor; Privación de la libertad y de otras garantías; Delitos en contra de las personas en su patrimonio; Encubrimiento y operaciones con recursos de procedencia ilícita; Delitos electorales y en materia de Registro Nacional de Ciudadanos; Delitos ambientales; y, Delitos en materia de Derechos de autor".[41]

El legislador de 1931 pretendió, en términos generales, hacer la división de los delitos teniendo en cuenta el bien o el interés protegido. Con acierto sostiene

[40] Idem
[41] Código penal federal. Op. Cit. 386 p.

Fernández Doblado que "el Código Penal Federal vigente, a veces se aparta del criterio científico de clasificación de los delitos en orden al bien o interés jurídico tutelado, como tratándose de los "Delitos cometidos por servidores públicos", en donde se atiende al sujeto activo de la infracción; por lo que respecta al Título Decimotercero "Falsedad", se toma en cuenta la característica de la acción delictiva. Para Fernández Doblado, el delito de abandono de hogar debería albergarse entre la bigamia y demás infracciones contra el estado civil, en un epígrafe que se denominara "Delitos contra la familia".[42]

[42] Ibid p. Ibiden p.

CAPITULO SEGUNDO

ANTECEDENTES DE LA INTERNET Y DIAGNÓSTICO DE LOS PRINCIPALES DELITOS INFORMÁTICOS

Concepto de Internet

Los autores consultados, nos señalan que el Protocolo de Internet (IP) y el Protocolo de Control de Transmisión (TCP) fueron desarrollados inicialmente solo como una idea en 1969, posteriormente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero estadounidense Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de Defensa. Internet comenzó siendo una red informática de ARPA (llamada ARPANET) que conectaba redes de ordenadores de varias universidades y laboratorios de investigación en Estados Unidos. La World Wide Web fue desarrollada en 1989 por el informático británico Timothy Berners-Lee para la Organización Europea para la Investigación Nuclear, más conocida como CERN."[43]

A principios de 1980, las redes más coordinadas, como CSNET (red de ciencias de cómputo), y BITNET, empezaron a proveer redes de alcance nacional, a las entidades académicas y de investigación, las cuales hicieron conexiones especiales que permitieron intercambiar información entre las diferentes comunidades. En 1986, se creó la NSFNET (red de la Fundación Nacional de Ciencias), la cual unió en cinco macro centros de cómputo a investigadores de diferentes Estados de Norte América, de este modo, esta red se expandió con gran rapidez, conectando redes académicas a más centros de investigación, remplazando así a ARPANET en el trabajo de redes de investigación. ARPANET se da de baja en marzo de 1990 y CSNET deja de existir en 1991,

[43] Tellez vargas, irma. Manual de Internet. Enciclopedia Encarta, 2002.

cediendo su lugar a INTERNET.

Esta red se diseñó para una serie descentralizada y autónoma de uniones de redes de computo, con la capacidad de transmitir comunicaciones rápidamente sin el control de persona o empresa comercial alguna y con la habilidad automática de renrutar datos si una o más uniones individuales se dañan o están por alguna razón inaccesibles.

México, fue el primer país latinoamericano en conectarse a Internet, lo cual ocurrió a finales de la década pasada, en febrero de 1989, a través de los medios de acceso e interconexión de teléfonos de México, compañía mexicana que había constituido el monopolio telefónico del país hasta el once de agosto de 1996. Los primeros enlaces de Internet en el país, que tuvieron fines exclusivamente académicos, se establecieron en el Instituto Tecnológico de Estudios Superiores de Monterrey, el Instituto Politécnico Nacional, la Universidad de Guadalajara y la Universidad de las Américas en Puebla.

Cabe señalar que entre otros objetivos, el sistema redundante de la unión de computadoras se diseñó para permitir la continuación de investigaciones vitales y comunicación cuando algunas partes de ésta red se dañaran por cualquier causa. Gracias al diseño de Internet, y a los protocolos de comunicación en los que se basan un mensaje enviado por éste medio puede viajar por cualquiera de diversas rutas, hasta llegar a su destino, y en caso de no encontrarlo, será renrutado a su punto de origen en segundos.

Una de las razones del éxito de Internet, es su interoperatividad, es decir, su capacidad para hacer que diversos sistemas trabajen conjuntamente para

comunicarse, siempre y cuando los equipos se adhieran a determinados estándares o protocolos, que no son sino reglas aceptadas para transmitir y recibir información.

Actualmente, cualquier persona puede ofrecer su propia página, un lugar virtual en el WWW (World Wide Web) o abrir su propio foro de discusión, de los que hoy en día existen alrededor de veinte mil y que abordan desde temas muy interesantes hasta muy deleznables, incluyendo comportamientos criminales. Ahora como ya vimos anteriormente podríamos definir Internet como la interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales. También existen sistemas de redes más pequeños llamados intranet, generalmente para el uso de una única organización.

Cómo funciona Internet

Internet es un conjunto de redes locales conectadas entre sí a través de una computadora especial por cada red, conocida como gateway. Las interconexiones entre gateways se efectúan a través de diversas vías de comunicación, entre las que figuran líneas telefónicas, fibras ópticas y enlaces por radio. Pueden añadirse redes adicionales conectando nuevas puertas. La información que debe enviarse a una máquina remota se etiqueta con la dirección computarizada de dicha máquina.

Los distintos tipos de servicio proporcionados por Internet utilizan diferentes formatos de dirección (Dirección de Internet). Uno de los formatos se conoce como decimal con puntos, por ejemplo 123.45.67.89. Otro formato describe el nombre del ordenador de destino y otras informaciones para el encaminamiento, por ejemplo "mayor.dia.fi.upm.es". Las redes situadas fuera de Estados Unidos utilizan sufijos que indican el país, por ejemplo (.es) para España o (.ar) para Argentina. Dentro de Estados Unidos, el sufijo anterior especifica el tipo de organización a que pertenece la red informática en cuestión, que por ejemplo puede ser una institución educativa (.edu), un centro militar (.mil), una oficina del Gobierno (.gov) o una organización sin ánimo de lucro (.org).

Una vez direccionada, la información sale de su red de origen a través de la puerta. De allí es encaminada de puerta en puerta hasta que llega a la red local que contiene la máquina de destino. Internet no tiene un control central, es decir, ningún ordenador individual que dirija el flujo de información. Esto diferencía a Internet y a los sistemas de redes semejantes de otros tipos de servicios informáticos de red como CompuServe, America Online o Microsoft Network.

Topología de Internet: Varias computadoras individuales conectadas entre sí forman una red de área local (LAN). Internet consiste en una serie de redes (LAN) interconectadas. Las computadoras personales y las estaciones de trabajo pueden estar conectadas a una red de área local mediante un módem a través de una conexión RDSI o RTC, o directamente a la LAN. También hay otras formas de conexión a redes, como la conexión T1 y la línea dedicada. Los puentes y los hubs vinculan múltiples redes entre sí. Un enrutador transmite los datos a través

de las redes y determina la mejor ruta de transmisión.

Concepto de cibernética

Si atendemos a la etimología de dicha palabra, proviene del vocablo "cibernética" que toma su origen de la voz griega "Kybernetes piloto", y kybernes", concepto referido al arte de gobernar. Esta palabra alude a la fusión del cerebro con respecto a las máquinas.

La cibernética es la ciencia de la comunicación y el control. Los aspectos aplicados de ésta ciencia, están relacionados con cualquier campo de estudio. Sus aspectos formales estudian una teoría general del control, extractada de los campos de aplicación y adecuada para todos ellos.

Concepto de informática

Es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en el año de 1962.

En sentido general, la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones."[44]

Mora y Molino, la definen como un estudio que delimita las relaciones entre los medios es decir equipo, y los datos y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado."[45]

---

[44] Barragán, julia. Informática y decisión jurídica. Fontamara, S.A. México, 1994, 184 p.
[45] Idem

La necesidad de crear una policía especializada en delitos informáticos

El día 1 de noviembre de 1988 Internet fue "infectada" con un virus de tipo "gusano". Hasta el 10% de todos los servidores conectados fueron afectados. El acontecimiento subrayó la falta de adecuados mecanismos de seguridad en Internet, por lo cual DARPA formó el Computer Emergency Reponse Team (CERT), un equipo de reacción rápida que mantiene datos sobre todas las incidencias en red y sobre las principales amenazas; esta fue la primera vez que apareció un virus dentro de los sistemas de enlace computacionales.

La investigación policial es una tarea que exige la intervención de diversos agentes especializados, unos equipos que se dedicarán a obtener y estudiar las pruebas delictivas para elaborar los informes periciales que se entregan al juez. Estos equipos estudiarían los hechos desde el punto de vista científico o técnico. Estas unidades considero en lo personal, que deberían estar formadas por especialistas en diversas áreas, todos ellos pertenecientes a las diferentes Direcciones de Servicios Periciales de las Procuradurías Generales de Justicia de los diversos Estados en donde ya hay expertos en la búsqueda y estudio de huellas dactilares, documentos o billetes falsificados, técnicas analíticas, balística y fotografía, entre otras; porque de esta manera con personal especializado en materia de internet, sería contundente y con resultados favorables la búsqueda de delitos y delincuentes en la red. Lo que ocurre es que los métodos de trabajo de los delincuentes cambian, y se demuestra actualmente que los delitos informáticos están a la orden del día; entonces ¿por que no crear una unidad pericial o policíaca especializada en detectar desde donde se hacen todo tipo de

fraudes electrónicos u otros delitos que se comenten utilizando la Web para ello?

El objetivo general, es el de realizar una metodología técnica en el ámbito de la informática para el desarrollo de un Servicio Criminalistico Informático Forense, la investigación y resolución de hechos que revistan de caracteres de delitos informáticos, acorde a la nueva legislación aquí planteada, ya que estos, alteran el orden social, pues causan graves perjuicios económicos a las empresas que actualmente tienen su sistema computacional conectado al Web, así como también causan grave problemática en las relaciones sociales, económicas y morales, es aquí en donde debemos ver la necesidad de crear esta fuerza.

La labor de esta fuerza Policíaca informática seria la de encontrar y determinar la culpabilidad del, o de los responsables, conocer su perfil y modus operandi, claro está que se necesitará de la ayuda de los administradores locales de servicio de Internet (que hasta el momento las empresa prestadoras de este servicio en nuestro país son TELMEX, ALESTRA, Y AVANTEL), pues las demás compañías se encuentran sujetas como proveedores solo del servicio, pues no cuentan con infraestructura propia para brindar el sistema; de esta manera se hace mas fácil la colaboración de estas empresas con las autoridades correspondientes.

Debemos pensar que este tipo de fuerza propuesta, fuera un grupo perfectamente bien capacitado, como licenciados en informática, pues su labor seria predominantemente enfrente de una computadora conectada al Internet; y que tuvieran capacitación periódica, pues cada vez el mundo de la computación se va renovando y los anteriores sistemas se vuelven obsoletos.

La idea sería contar con una agencia de Ministerio Publico especializada en este

tipo de delitos contando siempre con dos fuerzas, una de peritos y otra de Policía Ministerial y a la vez existiendo una coordinación de ambas, para evitar que los policías ministeriales y los peritos sean ocupados para realizar otras labores diversas para los que fueron contratados.

Esto es frecuente debido a la falta de personal dentro de nuestro sistema de Procuración de Justicia, propiamente dicho, dentro de la Procuraduría de Justicia de nuestro Estado.

Imagen 2: Organigrama propositivo para la integración de una fuerza especializada en delitos informáticos dependiente de 3 direcciones: Servicios Periciales, Averiguaciones Previas y Policía Ministerial, creando una coordinación de Delitos Informáticos y a la vez, una nueva agencia especializada con la ayuda de peritos en informática así como policías ministeriales.

Hay que agregar que en otros países, existen actualmente policías, o unidades especializadas que se encargan de detectar estas anomalías informáticas; Tanto NSA, FIRST Forum of Incident Response and Security Teams y CERT Computer Emergency Response Team, tienen equipos de especialistas dedicados a la localización de hackers, estos los encontramos en España, y la mayoría de los países que integran la comunidad Europea; mismos que hacen un tipo de defensa frente a sabotajes e intervención en caso de siniestros informáticos. Por otra parte, algunas policías como el FBI en los Estados Unidos y Scotland Yard en Inglaterra, disponen de unidades especiales para investigar la comisión de delitos a través de la red, actualmente se escucha de una división de la PGR en nuestro país, mas no es un dato confiable pues nunca se ha dicho nada al

respecto.

Conceptos de delitos informáticos.

En Internet se pueden producir ataques, y esos ataques van contra algo medular que es la información la que puede sufrir distintos tipos de intromisión para agredirla en su confidencialidad o integridad.

Definitivamente es indispensable el uso de la computadora y del manejo del Internet para la comisión de conductas delictivas denominadas "Delitos Informáticos", pero en la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe un concepto adecuado para así nombrar a los delitos informáticos. A lo que respecta a nuestro país, Julio Téllez Valdez, dice que hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, requiere que la expresión "delitos informáticos" esté consignada en los Códigos Penales, lo cual en México, al igual que en otros muchos países no ha sido objeto de tipificación aún, a excepción como ya lo hemos mencionado del Estado de Sinaloa.

Para Hilda Callegari, el delito informático es "aquel que se da con la ayuda de la informática o de técnicas anexas".[46]

Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".[47]

Rafael Fernández Calvo, define al delito informático como "la realización de una

[46] Tellez valdés, julio. Derecho informático. Mc graw hill. México, 1996, 283 p.
[47] Idem

acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título I de la Constitución Española".[48]

María de la Luz Lima, dice que el "delito informático en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea con método, medio o fin".[49]

El Dr. Julio Téllez Valdez, menciona dos clasificaciones del Delito Informático para efectos de conceptualización, que parte de lo típico y lo atípico. En el cual en el concepto típico de Delitos Informáticos nos dice que "son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin". En el concepto atípico menciona que "son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin".[50]

El Departamento de Investigación de la Universidad de México, señala como delitos informáticos a "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático".[51]

Así pues, y realizando una definición personal sobre los delitos informáticos,

---

[48] Tellez valdés, julio. Derecho informático. Mc graw hill. México, 1996, 283 p.

[49] Idem

[50] Idem

[51] Idem

diremos que: son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal y que en su realización se valen de las computadoras como medio o fin para su comisión.

Características y clasificación de los delitos informáticos.

Para la comisión de dicha conducta antisocial, hallaremos a uno o varios sujetos activos como también pasivos, los cuales tienen características propias: El Sujeto Activo, posee ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos, es decir, el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional, pues son personas listas, decididas y motivadas, dispuestas a aceptar un reto tecnológico.

El Sujeto Pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera, que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito es sumamente importante, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos. Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otras más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada: "cifra oculta o cifra negra".

En forma general, las principales características que revisten los Delitos informáticos son:

a) Conductas criminógenas de cuello blanco.

b) Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.

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

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" demás de cinco cifras a aquellos que los realizan.

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

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

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i)En su mayoría son imprudenciales y no necesariamente se cometen con intención.

j) Ofrecen facilidades para su comisión a los menores de edad.

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

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

Por lo anterior, se puede apreciar que los que cometen este tipo de ilícitos, son personas con conocimientos sobre la informática y cibernética, los cuales, se encuentran en lugares estratégicos o con facilidad para poder acceder a información de carácter delicado, como puede ser a instituciones crediticias o del gobierno, empresas o personas en lo particular, dañando en la mayoría de los casos el patrimonio de la víctima, la cual, por la falta de una ley aplicable al caso concreto, no es denunciada quedando impune estos tipos de conductas

antisociales; siendo esto alarmante, pues como se mencionó en líneas precedentes este tipo de acciones tienden a proliferar y ser más comunes, por lo que se pretende en la presente investigación, es crear una conciencia sobre la necesidad urgente de regular estas conductas, ya que debe ser legislado de una manera seria y honesta, recurriendo a las diferentes personalidades del conocimiento, tanto técnico en materia de computación, como en lo legal, ya que si no se conoce de la materia, difícilmente se podrán aplicar sanciones justas a las personas que realizan este tipo de actividades de manera regular.

Principales delitos informáticos

Incluye los cometidos contra el sistema y los cometidos por medio de sistemas informáticos ligados con Telemática, o a los bienes jurídicos que se han relacionado con la información: datos, documentos electrónicos, dinero electrónico, etc. Predominan:

Acceso no autorizado: El uso ilegítimo de contraseñas y el ingreso a un sistema informático sin la autorización del propietario está tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

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

Infracción de los derechos de autor: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de

ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line o de un sysop respecto a las copias ilegales introducidas en el sistema. Mientras un tribunal condenó a un sysop porque en su BBS había imágenes scaneadas de la revista Playboy, en el caso LaMacchia, el administrador del sistema fue hallado no responsable de las copias de programas que albergaba su BBS. El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a un "upload" de un programa o fichero que infrinja los derechos de autor de terceros.

Cabe Señalar que los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997 de esto hablaré posteriormente.

Distribución de música por Internet (mp3): Sabido es que con relación a la música existe el conocido MP3, un formato digital de audio que permite comprimir el tamaño de una canción digitalizada en una relación de 10 a 1, es decir que 10 MB de sonido digitalizado ocuparía solo un MB esto es lo que ha permitido un intenso tráfico de música dentro de la red que ha derivado inclusive en la venta ilegal de compactos sin intervención de las discográficas dando lugar a todo un movimiento al respecto que ha sido motivo de numerosas medidas para tratar de evitarlo.

Tan es así que existe una protección en España a cargo de la Sociedad Digital de

Autores y escritores SDAE que ha puesto al servicio de la detección de esta actividad. Nuevas tecnologías tratan de una especie de robot que da vueltas por Internet y se dedica a descubrir aquellos que distribuyen música sin pagar derechos como una forma de tratar de controlarlo y evitarlo. El caso del grupo Metallica es un ejemplo, pues nunca estuvo dispuesto a la distribución de su música en este formato.

Intercepción de E-mail: la violación de correspondencia, y la Intercepción de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno reviste la misma gravedad.

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

Estafas electrónicas: las compras electrónicas son un atractivo mas para que aumente los casos de estafa, existiría un engaño a la persona que compra al distribuidor, al banco y/o al equipo principal encargado de la operación. La proliferación de las compras telemáticas permite que aumenten también los casos de estafa.

Una de las cosas que proporciona la informática es poder realizar muchas tareas sin moverse de casa o la oficina. Esto supone que ya no existe un contacto directo entre las personas para acometer determinadas faenas. Como consecuencia de ello se ha producido un gran cambio en el mundo empresarial y de negocios, y, entre otras cosas, se han abierto nuevas perspectivas de consumo mediante el uso de Internet. Todos los que navegamos por Internet, conocemos

que se venden cientos de productos, de diferentes marcas y modelos a través de la red, el ciberespacio se ha convertido en un nuevo sector a tener en cuenta para las empresas; lo cual es muy lógico, pues se ahorran muchos costos y amplían su potencial de mercado. Lógicamente todo depende del tipo de empresa de que se trate y del producto o servicio que venda, nos podemos encontrar con que la supuesta empresa nos manda productos que no son, no podemos reclamar directamente porque no sabemos dónde se ubica la empresa, o simplemente hemos hecho un pago con la tarjeta de crédito y no nos han dado el servicio o producto; todo esto afecta al consumidor, pero las empresas también pueden ser objeto en este comercio de una estafa, piénsese en dar número de tarjetas de crédito falsas pero que el robot acepta como válidas (conocido en el mundo de Internet como "carding"), etc. Con todo esto vemos que tanto empresas como consumidores pueden ser estafados usando medios informáticos.

Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en países como el nuestro en el que nuestra legislación no prevea los casos en los que la operación se hace engañando al ordenador.

Con todo lo anterior podemos definir la estafa informática como la "manipulación o alteración del proceso de elaboración electrónica de cualquier clase y en cualquier momento de éste, realizada con ánimo de lucro y causando

un perjuicio económico a un tercero"[52]

Transferencias de fondos: este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático ya sea por el mal uso de passwords, tarjetas electrónicas falsificadas, llaves falsas o adulterando el contenido de la información externamente calificando dicha conducta como robo; debería calificarse dicha conducta como robo, existe todavía una falta de uniformidad en la materia. **Delitos Convencionales** Todos los delitos que se dan sin el empleo de medios informáticos y que con la aparición de las rutas virtuales se están reproduciendo también en el ciberespacio. También los actos que no son propiamente delitos sino infracciones administrativas o ilícitos civiles: Predominan:

Espionaje: Se están presentando casos de acceso no autorizado a sistemas informáticos e intercepción de correo electrónico de entidades gubernamentales, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera, evidenciándose una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales por personas especializadas. Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles.

Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

---

[52] Vives Antón T.S. - González Cussac J.L., derecho penal, parte especial 3ªedic. Valencia, 1999.

Espionaje Industrial: También aparecen casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales y fórmulas que posteriormente las utilizan otras empresas de la competencia o las divulgan sin autorización

Terrorismo: La presencia de equipos que encubren la identidad del remitente, convirtiendo el mensaje en anónimo, los servidores que ofrecen servicio de correos gratis permitiendo ingresar datos personales y direcciones ficticias para crear cuentas de correo que posteriormente aprovecharon personas o grupos terroristas para enviar amenazas, remitir consignas y planes de actuación ilícitos.

Después del atentado de Oklahoma, el gobierno norteamericano ha empezado a estudiar formas de investigación y prevención antiterrorista. Ante la sospecha de que en la organización del atentado se utilizara la red Internet para el envío de mensajes encriptados, la propuesta de ley antiterrorista de los senadores Dole y Hatch incluyen la ampliación de las facultades del FBI en materia de vigilancia electrónica y rastreo de la red.

Otro proyecto de la Casa Blanca modifica las leyes que regulan la intimidad y la intervención de las telecomunicaciones (Privacy Act y Wiretap Act) para poder interceptar y desencriptar mensajes electrónicos enviados o recibidos por sospechosos o presuntos terroristas, con plena eficacia procesal como prueba documental incluso cuando dichas evidencias hayan sido obtenidas sin el correspondiente mandamiento judicial.

Narcotráfico: Utilizando mensajes encriptados para ponerse en contacto se ha detectado el uso de la red para la transmisión de formulas para la fabricación de

estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

Tanto el FBI como el Fiscal General de los EE.UU. han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles. También se ha detectado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas. El notable avance de las técnicas de encriptación permite el envío de mensajes que, a pesar de ser interceptados, pueden resultar indescifrables para los investigadores policiales. Debe tenerse en cuenta que sólo en 1994 los jueces americanos concedieron 1.154 órdenes de vigilancia electrónica, de las cuales un importante número tuvieron resultado negativo a causa de la utilización de técnicas de encriptación avanzadas. Por ello, tanto el FBI como los fiscales americanos reclaman que todos los programas de encriptación generen puertas traseras que permitan a los investigadores acceder al contenido del mensaje.

Otros delitos: Al igual que los narcotraficantes, se presentan los traficantes de armas, las sectas satánicas, entre otros, obteniendo las mismas ventajas que encuentran en Internet aprovechadas para la planificación de los respectivos ilícitos que se están trasladando de lo convencional al ciberespacio o viceversa.

Difusión de pornografía: En la mayoría de países así como en nuestro país es ilegal la comercialización de pornografía infantil o cualquier acto de pederastia. Un ejemplo de conducta activa sería remitir una recopilación de imágenes

pornográficas scaneadas a los mailbox de un país en donde estuvieran también prohibidos los actos de difusión o comercialización de las mismas .

Manipulación de los datos: Este fraude conocido también como sustracción de datos, representa el delito informático mas representativo ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos. De acuerdo a la información entregada por entidades de seguridad a nivel mundial, el 75% de los casos de sustracción de datos lo realiza personal interno de la organización o que pertenecieron a ella.

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

Manipulación informática: es una alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos nuevos y falsos, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración, etc.

Se diferencia en las estafas informáticas de las cometidas dentro del sistema y las

cometidas fuera del sistema. Las primeras son las manipulaciones realizadas directamente sobre el sistema operativo, y no existe ningún engaño ni error sobre un ser humano. Las estafas cometidas fuera del sistema, son las manipulaciones de datos hechas antes, durante o después de la elaboración de los programas, siendo éstas las causantes del engaño que determina de disposición patrimonial.

Falsificaciones informáticas

Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada, ya sea que por necesidades se comparten directorios y con esto se permite que usuarios remotos tengan este acceso abriendo una ventana para que ingresen en forma fraudulenta personal ajeno a esta información. Para contrarrestar este acceso se necesita que los usuarios tengan conocimiento tanto de las ventajas (acceso a recursos siempre con claves) como desventajas (intrusión) de esta herramienta, además la adquisición inmediata de equipos muros para autenticar usuarios y ubicar las partes vulnerables de la red.

Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial, con la ayuda de Escáner y de impresoras de alta calidad para modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original donde solo un experto puede diferenciarlos de los documentos auténticos.

Sabotaje informático

Realizado por medio de cualquiera de estos métodos:

Virus. Los virus son un grave problema, ya que a pesar de ser programas muy pequeños pueden hacer mucho, y más si se utiliza Internet como vía de infección.

Un virus informático es un programa diseñado para que vaya de sistema en sistema, haciendo una copia de sí mismo en un fichero. Los virus se adhieren a cierta clase de archivos, normalmente EXE y COM, cuando estos ficheros infectados se transmiten a otro sistema éste también queda infectado, y así sucesivamente. Los virus entran en acción cuando se realiza una determinada actividad, como puede ser el que se ejecute un determinado fichero. Como hemos dicho los virus son programas, y para crearlos los programadores de virus utilizan kits de desarrollo de virus que se distribuyen por Internet, entre las que podemos destacar las siguientes: Virus Creation Laboratories, Virus Factory, Virus Creation 2000, Virus C destruction Est, o The Windows virus Entine. Por ello cualquiera que se haga con alguno de estos kits y sepa programación pueda crear sus propios virus, en este contexto no es raro que la estimación de los virus que existen en la actualidad sea de más de 7.000. Pueden ingresar en un sistema por la copia de un archivo infectado o por Internet que infectan algunos archivos de su sistema y lo pueden transmitir a otros equipos; En 1983 ya hablamos de las primeras referencias del virus.

Gusanos. Se fabrican de forma similar al virus con el objetivo de infiltrarlo en programas originales o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. Podría decirse que es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus, es decir, un programa gusano que posteriormente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera

continuamente dinero a una cuenta ilícita y luego destruirse.

Bomba ilícita o cronológica. Exige conocimientos especializados ya que requiere programar la destrucción o modificación de datos en el futuro. Lo contrario de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso entre todos los dispositivos informáticos criminales, la bombas lógicas son las que poseen el máximo potencial de daño. Su activación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. Puede utilizarse como material de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

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

Esto se debe a varios motivos como lo son desde la simple curiosidad, como en el caso de muchos jóvenes o niños, piratas informáticos (hackers) hasta el sabotaje o espionaje informático (crackers)

Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, recurriendo a uno de los diversos medios como son:

Aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.

Los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

En todos estos casos se producen pérdidas dinerarias provocadas por las conductas involucradas

Sujetos del delito

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

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

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos, el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y

Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

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

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

Efectivamente, este criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros".[53]

Asimismo, dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el

[53] Rojas amandi, victor manuel. El uso de internet en el derecho. Oxford, México, 1998, 348 p.

sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

Conductas ilegales más comunes

HACKER: Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en ordenadores pertenecientes a entidades públicas o privadas. El término de hacker en castellano significa "cortador". Las incursiones de los piratas son muy diferentes y responden a motivaciones dispares, desde el lucro económico a la simple diversión. Los "Hackers", son fanáticos de la informática, generalmente jóvenes, que tan sólo con un ordenador personal, un modem, gran paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, saltándose todas las medidas de seguridad, y leer información, copiarla,

modificarla, preparando las condiciones idóneas para realizar un fraude, o bien destruirla. Se pueden considerar que hay dos tipos; 1) los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad; 2) los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables.

Un hacker es un Apasionado de la tecnología, de todo tipo, quiere investigar cuanta cosa sale en el mercado. Experto en SO, sistemas de seguridad, programación avanzada, criptologia, conocimiento de phreaking.

El hacker puede actuar solo o en grupo, pero generalmente si se reúnen es para intercambiar información, no para que los demás miembros le enseñen a hackear. La rutina para ellos es bajar todo lo que puedan de Internet sobre vulnerabilidad, sistemas operativos, ingeniería social, phreaking, programación), inventan un nick (sobrenombre), para que los demás los reconozcan, y generalmente no transmiten desde su casa.

CRACKER: Para las acciones nocivas existe la más contundente expresión, "Cracker" o "rompedor", sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender; es decir, presenta dos vertientes, el que se infiltra en un sistema informático y roba información o produce destrozos en el mismo, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia. El cracker tiene como intención destruir. El

cracker comete fraudes con tarjetas de crédito, por ejemplo, una persona posee una empresa que vende productos, esos productos pueden ser adquiridos vía web con el uso de una tarjeta de crédito, supongamos que entra un cracker y se apodera de los números de tarjetas de todas las personas que han comprado en ese sitio, el cracker usa la valiosa información que encontró en ese sitio, y piensa en cuanto puede vender esos números.

PHREAKER: Es el que hace una actividad parecida a la anterior, aunque ésta se realiza mediante líneas telefónicas y con y/o sin el auxilio de un equipo de cómputo. Es el especialista en telefonía, empleando sus conocimientos para poder utilizar las telecomunicaciones gratuitamente.

VIRUCKER: Consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o inutilizar la información contenida. Existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

PIRATA INFORMÁTICO: Es quien reproduce, vende o utiliza en forma ilegítima un software que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor.; hay que considerar también la piratería como descargar música de internet y grabarla en un CD para escucharla; resulta pues que estamos inmersos entre una juventud de "corsarios negros" y cada día

hay programas donde se puede descargar gratuitamente el software para descargar la música gratuitamente

Las armas de los hackers

Cazadores de contraseñas: Un cazador de contraseñas es un programa que desencripta las contraseñas o elimina su protección. Aunque estos programas no han de desencriptar nada, y además con determinados sistemas de encriptación es imposible invertir el proceso, si no es de forma autorizada. El funcionamiento es el siguiente: cogemos una palabra de una lista, la encriptamos con el protocolo que han sido encriptadas las claves, y el programa compara las claves encriptadas con la palabra encriptada que le hemos dado, si no coincide pasa a otra clave encriptada, si coincide la palabra en texto legible se almacena en un registro para su posterior visualización. Los cazadores de contraseñas que podemos encontrar son: Crack, CrackerJack, PaceCrak95, Qcrack, Pcrack, Hades, Star Cracker, etc. Hay cazadores de contraseñas para todos los sistemas operativos.

Caballos de troya o troyanos: Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto, p. ej. Formatear el disco duro, modificar un fichero, sacar un mensaje, obtener información privilegiada del sistema, etc. Los troyanos los crean los programadores, ya sea creando ellos un programa original, e introduciendo el código maligno, o cogiendo el código fuente de otro programa e introduciendo el código maligno, y luego distribuirlo como el original.

Superzapping: Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador. El nombre proviene de una utilidad llamada SUPERZAP diseñada para Mainframes y que permite acceder a cualquier parte del ordenador y modificarlo, su equivalente en un PC serian las Pctools o el Norton Disk Editor.

Puertas falsas: Es una práctica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc. con objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas.

Herramientas de destrucción: Este suele ser el procedimiento de sabotaje más utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificara la información, o provocará el cuelgue del sistema. Podemos distinguir cuatro métodos de destrucción: mailbombing, flash bombs, aplicaciones especiales de negación de servicio, y virus.

Mailbombing: Este método se basa en enviar muchos mensajes de correo electrónico, al mismo usuario, lo cual provoca una gran molestia a dicho usuario. Las herramientas que existen para estos ataques son: Up Yours, KaBoom, Avalanche, Unabomber, extreme mail, Homicide, Bombtrack, etc. La mayoría de

estas aplicaciones suelen ser gratuitas, y las hay para todas las plataformas.

Flash bombs: Son herramientas que se utilizan en el IRC. Cuando nos conectamos a un IRC, hay varios canales o chats, y cada chat tiene su operador que es la autoridad en ese chat, y decide la persona que ha de marcharse del chat. Las personas expulsadas del chat toman represalias, y apareció el flash bombs. Las aplicaciones de flahs bombs que existen atacan en el IRC de una forma diferente, pero básicamente lo que hacen puede ser es expulsar a otros usuarios del chat, dejar colgado el chat, o llenar de basura (flooding) un canal. Las herramientas que tenemos a nuestra disposición son: crash.irc, botkill2.irc, ACME, Saga, THUGS, o The 7th Sphere.

Aplicaciones de negación de servicio: Este tipo de ataques trata de dejar colgado o desactivar un servicio de la red saturándolo de información y dejándolo bloqueado, e incluso se obligará a reiniciar la máquina. Las utilidades que podemos encontrar para realizar este tipo de ataques son: Syn_floder, DNSKiller, arnudp100.c, cbcb.c, o win95ping.c.

Ataques asincrónicos: Este es quizá el procedimiento más complicado y del que menos casos se ha tenido conocimiento. Se basa en las características de los grandes sistemas informáticos para recuperarse de las caídas, para ello periódicamente se graban los datos como volcado de memoria, valor de los registros, etc. de una forma periódica. Si alguien consiguiera hacer caer el sistema y modificar dichos ficheros en el momento en que se ponga de nuevo en funcionamiento el sistema, éste continuará con la información facilitada y por tanto la información podría ser modificada o cuando menos provocar errores.

Ingeniera social: Básicamente es convencer a la gente de que haga lo que en realidad no debería, por ejemplo, llamar a un usuario haciéndose pasar por administrador del sistema y requerirle el password con alguna excusa convincente.

Recogida de basura: Este procedimiento consiste en aprovechar la información abandonada en forma de residuo. Existen dos tipos: el físico y el electrónico. El físico se basa principalmente en los papeles abandonados en papeleras y que posteriormente van a la basura, p ej. el papel donde un operario apuntó su password y que tiró al memorizarla, listados de pruebas de programas, listados de errores que se desechan una vez corregidos, etc. El electrónico, se basa en la exploración de zonas de memoria o disco en las que queda información residual que no fue realmente borrada, p. ej. ficheros de swapping, ficheros borrados recuperables (por ejemplo, undelete), ficheros de spooling de impresora, etc.

Simulación de identidad: Básicamente es usar un terminal de un sistema en nombre de otro usuario, bien porque se conoce su clave, o bien porque abandonó el terminal pero no lo desconectó y ocupamos su lugar. El término también es aplicable al uso de tarjetas de crédito o documentos falsos a nombre de otra persona.

Spoofing: Mediante este sistema se utiliza una máquina con la identidad de otra persona, es decir, se puede acceder a un servidor remoto sin utilizar ninguna contraseña. ¿Cómo se hace esto? Pues utilizando la dirección IP de otro usuario, y así hacemos creer al servidor que somos un usuario autorizado. En máquinas

UNIX se suelen utilizar para estos ataques los servicios "r", es decir, el rlogin y rsh; el primero facilita el procedimiento de registro en un ordenador remoto, y el segundo permite iniciar un shell en el ordenador remoto.

Sniffer: Un sniffer es un dispositivo que captura la información que viaja a través de una red, y su objetivo es comprometer la seguridad de dicha red y capturar todo su tráfico. Este tráfico se compone de paquetes de datos, que se intercambian entre ordenadores, y estos paquetes a veces contienen información muy importante, y el sniffer está diseñado para capturar y guardar esos datos, y poder analizarlos con posterioridad. Un ataque mediante un sniffer se considera un riesgo muy alto, ¿por qué?, pues porque se pueden utilizar los sniffers para algo más que para capturar contraseñas, también pueden obtener números de tarjetas de crédito, información confidencial y privada, etc. Actualmente existen sniffers para todas las plataformas, ya que los sniffers se dedican a capturar datos, no computadoras, y por ello es igual la plataforma que se utilice. Algunos sniffers son los siguientes: Gobbler, ETHLOAD, Netman, Esniff.c (se distribuye en código fuente), Sunsniff, linux_sniffer.c, etc.

No se si algún día llegaremos a decir "será penado.... con... el que hackea...? ¿Cuándo un hacker llega a configurar una acción delictiva del verbo hackear?..... Hasta ahora no creo que nadie de la respuesta, ya que al momento de elaboración del presente, la Real Academia aún no lo había incorporado.

CAPITULO TERCERO

TENTATIVAS JURÍDICAS EN NUESTRO PAÍS

Para el desarrollo de este capítulo se analizará la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos, en este entendido, consideramos pertinente recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte en virtud de que el artículo 133 Constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión."[54]

TRATADO DE LIBRE COMERCIO DE AMÉRICA DEL NORTE (TLC)

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la 6ª parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución."[55]

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

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de

[54] Barrios garrido, gabriela. Internet y derecho en méxico. Mc graw hill. México, 1998, 180 p.
[55] Idem

defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capitulo específico del tratado.

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse el contenido del párrafo 1 del artículo 1717 titulado procedimientos y sanciones penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial."[56]

Por lo que se refiere a los anexos de este capítulo, anexo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC."[57]

Asimismo, debe mencionarse que en el artículo 1711, relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos, sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información.

Llama la atención que en su párrafo 2 habla sobre las condiciones requeridas para otorgar la protección de los secretos industriales y de negocios y una de ellas es que éstos consten en medios electrónicos o magnéticos.

---

[56] Ibid p. Ibiden p.
[57] Idem

ACUERDO SOBRE LOS ASPECTOS DE LOS DERECHOS DE PROPIEDAD INTELECTUAL RELACIONADOS CON EL COMERCIO, INCLUSO EL COMERCIO DE MERCANCÍAS FALSIFICADAS.

Al inicializar el contenido de este apartado, debemos aclarar que si bien la institución del GATT se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), todos los acuerdos que se suscribieron en el marco del GATT siguen siendo vigentes.

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

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

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

Asimismo, en la sección 5, denominada procedimientos penales, en particular el

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

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

Como se observa, el tratamiento que los dos instrumentos internacionales que se han comentado otorgan a las conductas ilícitas relacionadas con las computadoras es en el marco del derecho de autor.

En este entendido, cabe destacar que el mismo tratamiento que le han conferido esos acuerdos internacionales a las conductas antijurídicas antes mencionadas, es otorgado por la Ley Federal del Derecho de Autor que a continuación se analiza.

Ley federal del derecho de autor y código penal para el distrito federal en materia de fuero común y para toda la republica en materia de fuero federal.

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

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

De esta forma, cuando se inició la iniciativa correspondiente, se dijo que la importancia de pronunciarse al respecto era que con dicha iniciativa se atendía la complejidad que el tema de los derechos autorales había presentado en los últimos tiempos lo cual exigía una reforma con objeto de aclarar las conductas que podían tipificarse como delitos y determinar las sanciones que resultaran más efectivas para evitar su comisión.

Además, se consideró que debido a que en la iniciativa no se trataban tipos penales de delito se presentaba también una iniciativa de Decreto de Reforma al Código Penal para el Distrito Federal en materia de Fuero Federal, proponiendo la adición de un título Vigésimo Sexto denominado "De los delitos en materia de derechos de autor".

Al respecto, se consideró conveniente la inclusión de la materia en el ordenamiento materialmente punitivo, lo que por un lado habría de traducirse en un factor de impacto superior para inhibir las conductas delictivas y por otro en un instrumento más adecuado para la procuración y la administración de justicia, al poderse disponer en la investigación de los delitos y en su resolución, del instrumento general que orienta ambas funciones públicas.

En este orden, como se mencionó anteriormente, esta Ley regula todo lo relativo

a la protección de los programas de computación, a las bases de datos y a los derechos autorales relacionados con ambos. Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.

En este sentido, consideramos importante detenernos en los artículos 102 y 231. El primero de ellos, regula la protección de los programas de computación y señala además que los programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos, lógicamente no serán protegidos. El segundo en su fracción V sanciona el comercio de programas de dispositivos o sistemas cuya finalidad sea desactivar dispositivos electrónicos de protección de un programa de cómputo."[58]

Apreciamos que aún cuando la infracción se circunscribe al área del comercio, permite la regulación administrativa de este tipo de conductas ilícitas, como una posibilidad de agotar la vía administrativa antes de acudir a la penal.

Por su parte, esta ley en su artículo 215 hace una remisión al Título Vigésimo Sexto, Artículo 424, fracción IV del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal

[58] Tellez valdés, julio. Derecho informático. Op. Cit. 283 p.

del que se infiere la sanción al uso de programas de virus."[59]

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

Por su parte, el artículo 231, fracciones II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias ilícitas de obras protegidas por esta Ley" y "usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular".[60]

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

Además, la regulación de esta conducta se encuentra reforzada por la remisión que hace la Ley de Derecho de Autor en su artículo 215 al Título Vigésimo Sexto del Código Penal citado, donde se sanciona con multa de 300 a 3 mil días o pena de prisión de seis meses hasta seis años al que incurra en este tipo de delitos."[61]

Sin embargo, la regulación existente no ha llegado a contemplar el delito informático como tal, sino que se ha concretado a la protección de los derechos autorales y de propiedad industrial, principalmente.

Tal y como hemos sostenido, México no está exento de formar parte de los países

---

[59] Ibid p. Ibiden p.
[60] Idem
[61] Idem

que se enfrentan a la proliferación de estas conductas ilícitas. Recientemente, la prensa publicó una nota en la que informaba sobre las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que se remontaban a un valor de mil millones de dólares por concepto de piratería de estos programas.

Esto, a la larga podría traer implicaciones muy desventajosas para México, entre las que podemos citar: la pérdida de prestigio a nivel internacional por el actuar ilícito de empresas cuyo radio de acción no está reducido al ámbito nacional y la pérdida de credibilidad por parte de las compañías proveedoras de programas informáticos, lo que se traduciría en un mercado poco atractivo para ellas que pondrían al país en una situación marginada del desarrollo tecnológico.

En este entendido, consideramos que por la gravedad de la conducta ilícita en sí, y las implicaciones que traería aparejadas, justifica su regulación penal.

En otro orden, el Artículo 109, se refiere a la protección de las bases de datos personales, lo que reviste gran importancia debido a la manipulación indiscriminada que individuos inescrupulosos pueden hacer con esta información. Así, el acceso no autorizado a una base de datos de carácter personal de un Hospital de enfermos de SIDA puede ser utilizado contra estas personas quienes a causa de su enfermedad, se encuentran marginados socialmente, en la mayoría de los casos.

Por lo anterior, el análisis de este artículo corrobora la posición que hemos sostenido respecto a que en las conductas ilícitas relacionadas con la informática, el bien jurídico a tutelar no es únicamente la propiedad intelectual sino la

intimidad por lo que este artículo no debería formar parte de una Ley de derechos de autor sino de una legislación especial tal y como se ha hecho en otros países.

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

Por otra parte, debe mencionarse que en abril de 1997 se presentó una reforma a la fracción III del artículo 231 de la Ley Federal del Derecho de Autor así como a la fracción III del artículo 424 del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal.

De esta forma, las modificaciones a la ley autoral permitieron incluir en su enunciado la expresión " fonogramas, videogramas o libros", además del verbo "reproducir", quedando:

Art.231 fracción III Producir, reproducir, almacenar, distribuir, transportar o comercializar copias de obras, fonogramas, videogramas o libros protegidos por los derechos de autor o por los derechos conexos, sin la autorización de los respectivos titulares en los términos de esta Ley".. [62]

Con las reformas al Código Penal Federal se especifica que:

"Art.424 bis fracción.- I A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende, copias de obras, fonogramas,

[62] Tellez valdés, julio. Derecho informático. Op. Cit. 283 p.

viedogramas o libros protegidas por la Ley Federal del Derecho de Autor en forma dolosa, a escala comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos".[63]

Sobre el particular, debe mencionarse que durante la modificación a la Ley en diciembre de 1996 se contempló parcialmente lo que se había acordado en el **TLC** y que por tal razón fue necesaria una segunda modificación, en abril del año en curso para incluir la acción de "reproducción".

De igual forma el artículo 424 que había sufrido una modificación en diciembre de 1996, fue reformado en su fracción tercera en abril pasado para incluir la reproducción y su comisión en una forma dolosa.

Ejemplos de inclusión de los delitos informáticos en otros estados

CÓDIGO PENAL Y PROCEDIMIENTOS PENALES DE SINALOA

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos, consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo

"Delitos contra el patrimonio"

Capítulo V

Delito Informático.

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

---

[63] Tellez valdés, julio. Derecho informático. Op. Cit. 283 p.

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

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.

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

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

CONCLUSIONES

Es indiscutible la importancia social, económica, política y cultural del fenómeno informático.

Las nuevas tecnologías cada vez se van implantando más en nuestra sociedad, hasta el punto de que se ha hecho indispensable para determinadas tareas de vital importancia el uso de la informática y las telecomunicaciones, y además proporcionan un gran servicio a toda la sociedad. Por todo ello, el legislador ha de regular una realidad social, y penar determinadas conductas lesivas de ciertos bienes fundamentales de la persona.

El derecho de la informática, considerado como la regulación jurídica del fenómeno informático, implica a la legislación y a la doctrina judicial, así como a la doctrina jurídica, la docencia y la investigación, de manera adyacente.

Las redes de telecomunicaciones como Internet han generado un submundo en el que los delitos son difíciles de perseguir debido a la propia naturaleza del entorno y a la falta de tipificación de las modalidades de comisión y de los medios empleados. Entre los delitos, infracciones administrativas y malos usos que se pueden llevar a cabo en la llamada infraestructura de la información.

Entiendo personalmente que es casi imposible en este momento y tal como están dadas las cosas, llegar a una descripción cerrada de estas conductas delictivas, por cuanto Internet es algo absolutamente dinámico, (es uno de los hechos más importantes de los últimos tiempos), en que su progreso debe contarse por horas ya que sufre cada segundo una modificación continua que el avance tecnológico

le imprime a sus mecanismos, no es fácil formular un catálogo de conductas, por cuanto las mismas continuamente se van perfeccionado, por decirlo de a lguna forma, o se van modificando surgiendo otras nuevas. Por eso en Internet, las técnicas para llegar a realizar este tipo de conductas son prácticamente inagotables.

Básicamente lo primordial es que en la red se tenga una garantía de seguridad.

Tal como se dijo Internet revoluciona la naturaleza de los procesos, modifica el sentido de conceptos tradicionales, por ejemplo desaparece en la diferencia entre publicación y difusión porque colocar un dato en la red, es difundirlo inmediatamente, arrasa con la censura a través de los foros que se pueden organizar en los que se emiten opiniones con absoluta libertad de expresión. En ese contexto, es que deben reunirse los datos empíricos necesarios para propiciar la intervención ultima ratio del derecho penal.

Así el único hacedor de la ley penal federal, entiéndase el legislador, conforme con nuestro principio de legalidad, podría llegar a expresar concreta, concisa y lo más claramente posible conductas que sean penalizadas.

La persecución al buen término aplicando las sanciones prescriptas.

Esto, es lo que requiere un arduo esfuerzo que para emprenderlo es necesaria una previa y exhaustiva investigación de los hechos que componen la mayoría de casos, donde ya se habla de millonarios perjuicios de orden económicos y de delitos de "guante virtual" terminología que se ha barajado en Seminarios de España y destaco que Europa está mucho más adelantado respecto de este tema que América y por ende nuestro país.

Cabe mencionar que en México, actualmente el Instituto Mexicano de la propiedad Industrial (IMPI.) conjuntamente con la Procuraduría General de la Republica, apoyándose básicamente en la ley de la propiedad Industrial y en el Código Penal Federal; ha organizado auditorias a diversas empresas detectando que 4 de cada 10 computadoras funciona con software ilegal; esto es un avance y un ejemplo de lo necesario que es regular los delitos informáticos para que no se tengan que estar apoyando en instituciones alternas.

Una vez delimitados estos conceptos y no estoy entrando acá en las ciencias penales, o sea delimitados fácticamente con comprensión de su realidad, con estadísticas bien logradas, y respuestas a preguntas del porqué, para qué y cómo se podría hablar de delito, se estará en condiciones de concretar, sobre la base de la Constitución, cuál será el bien jurídico tutelado, estas como etapas indispensables a seguir para decir, cuál es el delito informático en nuestro derecho penal.

El dinamismo, que comprende el tráfico en la red torna sumamente difícil aunque casi imposible delimitar conductas penales para lo cual, se requeriría de crear una policía o una fuerza altamente especializada en la detección de este tipo de conductas criminales.

Así las cosas, cómo debe ser aquello que provea al legislador de un criterio material obligatorio que le proporcione también las pautas directrices y de igual carácter para interpretar y criticar las normas penales existentes proporcionándole decisiones valorativas, previas y obligatorias, para encarar la ley penal federal y, que sólo pueden desprenderse de la Constitución.

Solo a partir de ella se puede construir este concepto de bien jurídico pues ésta es quien contiene esas decisiones valorativas fundamentales para elaborarlo (con el citado carácter de previas y obligatorias) para cualquier ley penal.

Debo señalar que el estudio que ha de realizar el legislador requiere una determinación precisa de la sociedad estatal, en el ámbito de la constitución y de las "condiciones y funciones en las que se basa nuestra vida social" dentro de ese marco constitucional y que deben ser protegidas.

BIBLIOGRAFÍA

González de la vega, francisco. Derecho penal mexicano. Porrúa. México 1996. 473 p.

Betancourt López, Eduardo. Teoría del delito. Porrúa. México 1994. 304 p.

Beccaria. Tratado de los delitos y de las penas. Porrúa. México 1995. 408 p.

González quintanilla, José Arturo. Derecho penal mexicano. (Parte general). Porrúa. México 1993. 504 p

Villalobos, Ignacio. Derecho penal mexicano. Porrúa. México 1975. 650 p.

Barrios garrido Gabriela, Muñoz de Alba Marcia, Pérez Bustillos Camilo. Internet y derecho en México. Mc Graw Hill. México 1998. 180 p.

Barragán, julia. Informática y decisión jurídica. Distribuciones fontamara. Primera edición 1994, México. 184 p.

Diccionario de la micro computación t. Ii. 632 p.

Téllez Valdez Julio. Derecho informático. Mc Graw Hill. México, Segunda edición 1996. 283 p.

Constitución Política de los Estados Unidos Mexicanos.

Código Penal Federal.

Código de Procedimientos Penales Federal.

Carnelutti, Francesco. Derecho procesal civil y penal. Colección Clásicos del Derecho. México.

Poder Judicial De La Federación; Apéndice al Semanario Judicial de la Federación (1917-2000), Themis, México

Rojas Amandi, Víctor Manuel; El uso de Internet en el Derecho. Oxford. México.

Tratado De Libre Comercio De América Del Norte (TLC)

Acervo Jurídico, Versión B, CD-ROM, México.

Enciclopedia Encarta 2002

Ley de la Propiedad Industrial