UNIVERSIDAD NACIONAL AUTÒNOMA DE MÈXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

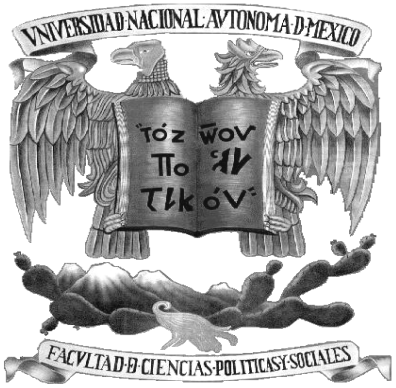
LA REGULACIÓN JURÍDICA INTERNACIONAL DEL CIBERESPACIO. TERRORISMO INFORMÁTICO.

TESIS

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN RELACIONES INTERNACIONALES

P R E S E N T A



MORALES GALVÁN ROXANA FABIOLA

Director: Dr. Juan Carlos Velázquez Elizarrarás

México, DF, 2007

A mi mamá.
Por tu ejemplo de perseverancia y constancia; por apoyarme en todo momento, por tus consejos y valores para salir adelante siempre; por la motivación constante que me ha permitido ser una persona de bien, por haberme educado y soportar mis errores, pero más que nada, por tu amor y paciencia.

A mi papá.
Por tu amor, cariño, comprensión y apoyo que siempre han estado presentes de una u otra manera.

A mis hermanos Ore, Cris y Pon.
Por ser mí ejemplo muchas veces, por dejarme aprender de sus aciertos y momentos difíciles; por contar con ustedes para todo; porque me han enseñado que el trabajo de ser la hermana mayor no es fácil, pero vale la pena.

A mis Familiares.
Por su apoyo y cariño.

A mis maestros.
Gracias a todos los que contribuyeron realmente en mi formación, por todos sus consejos, sus formidables clases y su paciencia, en especial al ***Dr. Juan Carlos Velázquez*** *por su gran apoyo y motivación para la culminación de mis estudios profesionales y para la elaboración de esta tesis; por guiar mi formación no solamente académica, sino como persona; por compartir su conocimiento conmigo e inspirar en mi mucha admiración; al* ***Dr. Alfonso Melo****, por sus consejos y sugerencias para el presente trabajo; por su paciencia y tolerancia al buscar soluciones ante mis dudas; por ayudarme a descubrir esa combinación de complejidad y sencillez que a la vez se presentan en nuestra realidad; al* ***Mtro. Juan Palma*** *por permitirme colaborar con él, por su tiempo compartido, consejos y apoyo; por su enseñanza, confianza y fortaleza en los momentos difíciles y por impulsar el desarrollo de nuestra formación profesional; a la* ***Mtra. Laura Ramírez****, por ayudarme a lo largo de la tesis desinteresadamente y brindarme su apoyo, recomendaciones y propuestas; al* ***Lic. Roberto Tenorio****, por su paciencia y contribuciones al revisar este trabajo.*

A la Universidad Nacional Autónoma de México.
En especial a la ***Facultad de Ciencias Políticas y Sociales*** *y al* ***Centro de Relaciones Internacionales*** *que me dieron la oportunidad de formar parte de ellas y ampliar mis horizontes.*

Por último, quisiera agradecer a todo aquel que de una forma u otra estuvo implicado en el desarrollo de este trabajo, su paciencia y apoyo.

Gracias a todos.

ÍNDICE

INTRODUCCIÓN

A través de la tecnología y la computadora se han tenido, en diferentes campos, innumerables avances: en el científico, en la educación, la medicina, el entretenimiento, y en cualquier área donde el hombre se desenvuelve. No se podría imaginar ahora en el siglo XXI al hombre sin la ayuda de las computadoras.

Nuestra era se caracteriza por un creciente acceso a la tecnología y a una globalización social de la información y de la economía. En los próximos años el desarrollo tecnológico y el mayor uso de redes abiertas,[1] como Internet, proporcionarán oportunidades nuevas e importantes y plantearán nuevos desafíos. La infraestructura de la información se ha convertido en una parte vital del eje de nuestras vidas.

El uso de las nuevas tecnologías digitales y de la telefonía inalámbrica se ha generalizado. Estas tecnologías nos brindan la libertad para poder movernos y permanecer comunicados y conectados con miles de servicios construidos sobre "redes de redes". Nos dan la posibilidad de participar, enseñar y aprender, jugar, trabajar juntos y de intervenir en los procesos políticos.

A medida que las sociedades dependen cada vez más de estas tecnologías, será necesario utilizar medios jurídicos y prácticos eficaces para prevenir los riesgos asociados a su uso.

Al mismo tiempo el desarrollo de Internet, como un nuevo medio de difusión masiva de contenidos, se erige como una realidad indiscutible, con todos los visos de seguir experimentando un crecimiento exponencial en los próximos años.

Este crecimiento no se encuentra exento de fuertes tensiones derivadas de las potencialidades que encierra el uso de la tecnología digital, y de las facilidades intrínsecas del sistema para acceder y transmitir datos de una máquina a otra, sin que las fronteras políticas supongan barrera efectiva para ello ya que, el ciberespacio (ó Internet), es un espacio abierto donde interactúan sujetos públicos y privados, individuales y colectivos de todo el mundo, que constituyen una sociedad virtual fundada en relaciones comerciales, educativas, sociales, culturales e incluso políticas.

Toda esta actividad ha generado inquietudes en diversos ámbitos internacionales en lo que respecta a su regulación, en aspectos tales como impuestos, tratamiento de datos, propiedad intelectual, comercio electrónico, derechos fundamentales, jurisdicción y otros asuntos relativos al ámbito jurídico.

[1] Se usa el término "redes abiertas", a toda aquella información a la que se tiene acceso libre, es decir, todo sujeto puede hacer uso ilimitado de ésta.

La relevancia de este tema para la carrera de Relaciones Internacionales, estriba en que la delincuencia informática se comete en el ciberespacio, y no se detiene en las fronteras nacionales convencionales, por lo tanto, puede perpetrarse desde cualquier lugar y contra cualquier usuario de ordenador del mundo, por ende se necesita una acción eficaz, tanto en el ámbito nacional como internacional, para luchar contra la delincuencia informática, ya que a escala nacional, no hay respuestas globales y con vocación internacional frente a los nuevos retos de la seguridad de la red y la delincuencia informática. En los países, las reacciones frente a la delincuencia informática se centran en el derecho nacional, descuidando medidas alternativas de prevención.

A pesar de los esfuerzos de las organizaciones internacionales y supranacionales, las diversas leyes nacionales de todo el mundo ponen de manifiesto considerables diferencias, especialmente en las disposiciones del derecho penal sobre piratería informática y contenidos ilícitos. También existen considerables diferencias en cuanto al poder coercitivo de los organismos investigadores, la jurisdicción en materia penal, y con respecto a la responsabilidad de los proveedores de servicios intermediarios por una parte y los proveedores de contenidos por otra.

En el cuadro de investigación de las Ciencias Sociales este tema presenta particular importancia debido a que en la escala internacional y supranacional, se ha reconocido ampliamente la necesidad de luchar eficazmente contra la delincuencia informática, y diversas organizaciones han coordinado o han intentado armonizar actividades al respecto, pero todas estas acciones internacionales no han logrado impactar en nuestra realidad ni cambiar la nula percepción de inseguridad que sentimos frente a estos nuevos hechos.

En la doctrina hay algunas propuestas principales de regulación de Internet, que se han desarrollado en los últimos años. Ninguna de ellas se ha impuesto de manera generalizada y por el contrario las soluciones actuales han correspondido a la incorporación parcial de ciertos aspectos de cada una de las propuestas, conformando una regulación mixta, que lo único que ha generado es una discontinuidad de la legislación, una inseguridad jurídica y la inaplicación de muchas de las normas; ya sea por falta de jurisdicción, de medios de coerción o de competencia de quien legisla, o bien por la existencia de los propios medios tecnológicos que permiten la omisión de responsabilidades y de obligaciones acordadas por la comunidad de Internet.

También se puede decir que nadie escapa a la enorme influencia que ha alcanzado la informática y su progreso para el desarrollo. Transacciones comerciales, comunicación, procesos

industriales, investigaciones, seguridad, sanidad, etc., son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática, por citar sólo algunos.

Si nos detenemos ante las maravillas tecnológicas que hoy en día nos amparan y simplifican nuestro trabajo, debemos reconocer que en casi cualquier ámbito nos encontramos con grandes aplicaciones que hacen de la vida de los hombres una tarea mucho más sencilla que hace sólo 60 años atrás cuando estaban apareciendo las primeras computadoras.

Al mirar hacia nuestro alrededor, el término "tecnología digital" se nos hace de lo más común y de hecho identifica las tendencias hacia donde deben ir las nuevas ofertas comerciales a fin de que el mercado reaccione de manera favorable a los nuevos productos. Eso en cuanto a la vida diaria de cada ciudadano (exceptuando aquellos que se encuentren en niveles apreciables de pobreza), de hecho, podemos decir que casi cualquier persona cuenta con al menos uno o dos de estos nuevos implementos digitales, los que incluyen teléfonos celulares, teléfonos fijos, televisores, radios, etc.

Como primera aproximación, se abordan, en el primer capítulo las nociones del delito, su definición, sus elementos y tipos, para poder llegar a una conceptualización de los delitos informáticos (los cuáles deben reconocerse como aquellos que ataquen equipos de informática o sus aplicaciones). En el segundo capítulo, se analiza la relación entre éstos y la piratería informática, así como en su especificidad los principales tipos de delitos informáticos, sus características y clasificación. Finalmente, se detallan las principales teorías usadas por el derecho para la regulación del ciberespacio y el marco jurídico en donde se incluye un panorama general sobre la seguridad, contenidos y propuestas regulatorias en Internet.

Una vez determinadas las técnicas y acciones de los delincuentes más comunes en la red, se interpreta en el tercer capítulo, cómo es que el terrorismo informático tiene la singular característica de cometer delitos de carácter telemático, es decir, el grupo de delitos informáticos que pueden cometerse a distancia, ni siquiera es requisito que el autor material o siquiera el intelectual conozcan la ciudad que se desea atacar, o que alguna vez tengan presencia física en el lugar del atentado.

De aquí que surja una de mis hipótesis al plantear que el Terrorismo Informático, tratará de descargar daño físico y destrucción (posiblemente causando desgracias humanas, también), a través del Ciberespacio. Éste proporcionará, a los terroristas, el placer del gran impacto y la publicidad de las operaciones sin la necesidad de la proximidad física y sus asociados riesgos.

Tales operaciones podrían también reducir las complejidades lógicas del transporte de explosivos y otros equipos.

En un último capítulo, se presenta un estudio comparado de los países que cuentan con estudios avanzados en el tema y sus respectivas legislaciones (sin omitir desde luego, el estudio de nuestro país), a fin de que al analizar las actividades que se realizan para fomentar la cooperación internacional en los campos relativos al Internet, se proyecte cómo es que más allá de regular situaciones específicas que sólo aplican a determinadas circunstancias de espacio, tiempo y sujetos concretos, debe valorarse en un debate internacional cuál es la intención social, política y económica de aplicar un régimen jurídico al mundo virtual, teniendo como base la regulación del ciberespacio y sobre todo de la piratería informática y el terrorismo informático.

En el desarrollo de esta investigación se plantean reflexiones y se trata de conducir a un debate sobre Internet que gire en torno a la dificultad de establecer límites en los contenidos de éste sin vulnerar la libertad de expresión y comprobar si realmente es necesaria o no esta regulación.

Asimismo, se trató de realizar un estudio de los mecanismos y modalidades de ejecución y fomento de la autorregulación de la Internet y los mecanismos de supervisión de los contenidos, por ejemplo, los relativos a la pornografía infantil o aquellos que inciten al odio por motivos de raza, sexo, religión, nacionalidad u origen étnico.

Mediante la evaluación de las medidas de apoyo, las diferentes percepciones y los conceptos hoy utilizados y conocidos por la comunidad internacional, en cuanto al tema de investigación, sostengo, en mi hipótesis central que el desarrollo de un marco normativo y legal que comprenda todo el conjunto de delitos vía Internet, especificando qué se entiende por delito, sus posibles castigos y las diversas estrategias políticas, sociales y económicas que deben ser desarrolladas para aplicar un régimen jurídico al mundo virtual donde se consideren los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional, prevendrá las situaciones tan conflictivas que se han estado originando desde la aparición de la Internet, por lo que, las estrategias que se empleen deben ser concebidas con la participación de toda la estructura del Estado-Nación y sustentadas en Inteligencia, lo cual permitirá proyectar la acción contra los delitos informáticos y el terrorismo con visión de futuro, uniendo las acciones intermedias y permitir atacar el fenómeno desde sus raíces.

A simple vista y sin realizar un análisis detallado de las circunstancias implicadas en éstas temáticas, (piratería informática, delitos informáticos y terrorismo informático), podría parecer

que no hay relación alguna entre ellas, ya que en una primera apreciación los delitos informáticos comprenden un ámbito expresamente privado que nada tendría que ver con actos masivos de terror institucionalizado con fines políticos o ideológicos, tal como se define terrorismo.

Si bien es cierto que muchos ataques realizados por medios informáticos no pueden producir el temor necesario para que sean considerados terrorismo internacional, no es menos cierto que ello no invalida la hipótesis de que ciertos delitos puedan crear situaciones de terror a una población local, nacional o incluso internacional.

La mayoría de los usuarios de computadoras personales conocen el efecto devastador que un virus informático causa en su equipo, y cuánto cuesta limpiar el sistema de tales programas agresivos y furtivos. Imaginemos ahora virus de computadora mucho más sofisticados, actuando en redes de sistemas informáticos complejos, que han sido diseñados para actuar en puntos neurálgicos del sistema agredido.

Redes enteras de computadoras pueden ser desarticuladas, engañadas, destruidas. Estos virus pueden tomar diversas formas y actuar siguiendo diferentes estrategias para llevar a cabo su misión de interferir, confundir y destruir a los programas, datos y al flujo de información. Estos virus inclusos pueden ser diseñados para atacar y trastocar datos muy específicos o instrucciones de un programa informático, para causar acciones bien determinadas en el mundo físico.

En cambio las armas de pulso electromagnético producen la destrucción física del hardware, desarticulando los sistemas informáticos al eliminar los procesadores y/o equipos periféricos. Este efecto de las ondas electromagnéticas de gran energía liberada en tiempos muy breves, fue descubierto durante los ensayos de las armas nucleares, las que eran capaces de destruir equipos electrónicos a gran distancia, sin intervenir los efectos térmicos o mecánicos de la explosión atómica, usando únicamente la energía electromagnética generada en la detonación.

La realización de tareas de inteligencia, necesarias para llevar a cabo atentados tanto en el mundo físico o en el mundo virtual es mucho más simple debido a la masa de información disponible electrónicamente sobre casi todos los aspectos de la civilización contemporánea. La fabricación de elementos ofensivos para llevar a cabo atentados explosivos o biológicos es facilitada por la aparición de manuales electrónicos sobre tecnología de bombas o armas químicas y bacteriológicas.

Sin embargo el uso de las armas de la llamada Infoguerra (proveniente del mal uso de los medios informáticos hacia la sociedad mundial), pueden brindar una capacidad mucho más sutil y efectiva de causar terror a una sociedad. El análisis de los nodos de convergencia entre el mundo

real y el mundo virtual es el primer paso para determinar que tipos de actos terroristas pueden ser realizados.

Pero existen aún más espacios que crean puntos de convergencia entre el mundo virtual o informático y el mundo real que nos rodean: el control de subterráneos y trenes, sistemas de distribución de energía eléctrica y gas, sistemas de comunicación, sistemas bancarios y financieros, todos susceptibles de ser atacados y perturbados por medio de la intrusión a las computadoras del sistema, infectándolas con virus, bombas lógicas o troyanos, o simplemente cambiando información o programas.

Los efectos físicos de estos ataques en el mundo virtual pueden resultar en un alto costo de vidas y bienes, pero fundamentalmente el objetivo del atentado ciberterrorista será minar la confianza de los habitantes en la sociedad en que viven, trasmitir un mensaje claro: nadie esta a salvo, y todo es posible de ser infiltrado, trastocado, corrompido y desestabilizado.

Las estrategias que se empleen para combatir el terrorismo informático deben ser concebidas con la participación de toda la estructura del Estado-Nación y del mismo modo considerar la participación de los diferentes actores del sistema internacional. El combate contra el terrorismo debe estar sustentado en Inteligencia, una inteligencia que permita proyectar la acción contra el terrorismo con visión de futuro, uniendo las acciones intermedias y permitir atacar el fenómeno desde sus raíces, produciendo un conocimiento útil y buscando los consensos para conformar sistemas de inteligencia adecuados en su estructura y en sus fines, por lo que debe ser preocupación no sólo de militares sino también de civiles, profesionales de diferentes áreas, gobernantes y políticos.

La tarea de prevención necesaria es mucha y las necesidades de legislaciones y equipos de trabajo acordes al reto por venir es inmediatamente necesaria, lo que se requiere es sólo la voluntad política de los encargados de dirigir los destinos de las naciones a fin de evitar que algo que nació con fines científicos como lo fue Internet termine convirtiéndose en una nueva y poderosa arma de terrorismo internacional por la simple inacción o falta de visión de los políticos.

CAPÍTULO I

El delito: definición legal y doctrinaria

Dado que el hombre está dotado de una voluntad libre que le permite desarrollar sus facultades naturales, tiene como única limitante a esa libertad su propia naturaleza; pero, en sociedad, esta libertad está forzosamente limitada por el respeto a la libertad de otros hombres; de aquí deriva la necesidad de normas o reglas que garanticen a cada miembro del cuerpo social, con una medida igual, el ejercicio de su actividad y desarrollo. La teoría y existencia de este principio constituye el Derecho, en su acepción más extensa.

Por tanto, el derecho como un conjunto de normas de observancia obligatoria para todos los miembros de la sociedad, que han sido establecidas por el Estado de acuerdo a procedimientos previamente establecidos, permiten la convivencia de todos los miembros de la sociedad entre sí, de las instituciones del Estado y la interrelación de éstas y la sociedad. Desde luego, la manifestación del derecho, en su aspecto práctico y real, es por medio o a través de la ley.

Al cometer una infracción hacia las normas jurídicas ó en su defecto caer en la no observación de las disposiciones de la ley, se comete un delito, en perjuicio de la sociedad y de la obligatoriedad de la misma ley por los hombres.

Esto obedece a muchos y muy diversos factores, sin embargo, esos factores tienen origen en la propia naturaleza del hombre y la convivencia estrecha a la que, hoy en día, se ve sometido, ya que, el ser humano siempre pretenderá tener un mayor número de satisfactores que otros, (incluso más de los que necesita), por el sólo hecho de acumular riquezas y el poder, que en la sociedad actual, representan una posición admirada y envidiada por algunos de sus miembros, aún cuando no las puede conseguir de manera honesta y legal.

La palabra "delito", deriva del verbo *delinquere*, a su vez compuesto por dos palabras: *linquere*, que significa dejar y por el prefijo *de*, en la connotación peyorativa, se toma como *linquere viam* o *rectam viam*: dejar o abandonar el buen camino.[2]

Para González Quintanilla, el delito "es un comportamiento típico, antijurídico y culpable."[3] Para Ignacio Villalobos, el delito "es un acto humano típicamente antijurídico y

[2] Juan Palomar de Miguel, *Diccionario para Juristas*, México, Mayo Ediciones, 1981, p. 196.
[3] José Arturo González Quintanilla, *Derecho Penal Mexicano*, México, Editorial Porrúa, 1993 p. 104.

culpable."[4] Para Rafael de Pina Vara, el delito "es un acto u omisión constitutivo de una infracción de la ley penal."[5]

Así pues, la idea del delito toma su origen en la ley penal. Entre la ley penal y el delito existe un nexo indisoluble, pues el delito es propiamente la violación de la ley penal o, para ser más exactos, la infracción de una orden o prohibición impuesta por la ley; en consecuencia, delito será "todo hecho al cual el ordenamiento jurídico penal le adscribe como consecuencia una pena, impuesta por la autoridad judicial por medio de un proceso."[6]

En el delito, para su existencia, deben de incidir dos sujetos: el sujeto activo y el sujeto pasivo,[7] en ocasiones intervienen otros en conjunción con el activo, ya sea antes o después de la comisión o realización del delito.

El sujeto activo del delito será toda persona que, en términos generales, infrinja la ley, ya sea por su propia voluntad o sin ella; es decir, el delito puede ser cometido, por el sujeto activo, con pleno conocimiento de la acción que va a realizar, esperando el resultado de ése, o, en caso contrario, sin la voluntad de ese sujeto, cuando la acción, que da origen al delito, no es deseada y se comete por imprudencia o sucede por un accidente. Sin embargo, este sujeto será el que realice la acción de la conducta o la omisión de la misma que están previstas y sancionadas por la ley penal.

En el caso del sujeto pasivo del delito, éste será toda persona que resienta el daño que ocasiona la comisión del delito, la consecuencia de la conducta delictiva, ya se trate de su persona, en sus derechos o en sus bienes. La persona a quien se le afecta en su esfera personal de derechos e intereses.

Desde luego, la naturaleza y tipo de delito, de que se trate, influirá en la calidad, tipo y número de los sujetos activos y, las consecuencias de ése, en los pasivos.

Por otra parte, el objeto del delito es muy importante, no solamente en la teoría del mismo, sino para la existencia y vida del mismo, incluyendo su comisión o realización. Es así como el objeto jurídico del delito, es el bien protegido por el derecho y que precisamente por esa razón, se denomina bien jurídico, es decir el *quid* de la norma, que, con la amenaza de la sanción, trata de proteger contra posibles agresiones.[8]

---

[4] Ignacio Villalobos, *Derecho Penal Mexicano,* México, Editorial Porrúa, 1975, p. 158.
[5] Rafael De Pina y Vara, *Derecho Civil Mexicano, (Bienes-Sucesiones),* México, FCE, 6ª edición, 1975, p. 41.
[6] Eduardo Betancourt López, *Teoría Del Delito,* México, Editorial Porrúa, 1994, p. 30.
[7] Ídem.
[8] José Arturo González Quintanilla, *Op. Cit*., p. 176.

A mayor abundamiento, el objeto del delito es sobre lo que debe recaer la acción del agente según la descripción legal respectiva y, por otra parte, el bien tutelado por las particulares normas penales y ofendidas por el delito. De tal enunciación aparecen dos conceptos completamente diferentes, el de objeto material y el de objeto jurídico del delito, que solo coinciden cuando la ofensa de un bien tutelado por el derecho penal consiste en la modificación de aquello sobre lo cual precisamente se verifica el resultado.

Por lo que hace al objeto material del delito, éste puede ser la formulación que antecede al que la descripción legal respectiva tiene por tal, de donde se infiere que no constituye objeto material, en sentido jurídico. Las cosas materiales con que se cometió el delito, o constituyen su producto, o son huellas de su perpetración, pues ellas conciernen al episodio delictivo concreto y no a su abstracta previsión legal.

El objeto material del delito puede ser tanto una persona como una cosa. El estado protege determinados bienes porque es necesario para asegurar las condiciones de la vida en común; no protege el interés en la observancia de los preceptos legales; es decir, se protege, por la norma penal, el derecho del particular, ya que no puede considerarse lógicamente que la norma jurídica, es decir, el objeto de la protección, pueda protegerse a sí misma.

Por lo que hace al objeto jurídico del delito, se conviene en que éste es el bien jurídico penalmente protegido que el delito ofende. Un bien jurídico puede ser tanto una persona, como una cosa, como una relación entre personas y una entre personas y cosas; entre estos bienes hay algunos que, por ser vitales para la colectividad y el individuo, reciben protección jurídica por su significación social y a los cuales el derecho acuerda su especial tutela erigiendo en tipos delictivos algunas formas especialmente criminosas de atentar contra ellos, por tanto, como objetos de interés jurídico vienen a constituir el objeto jurídico que se halla tras cada delito.[9]

La idea del bien jurídico es una de las ideas fundamentales, una de las piedras angulares del Derecho Penal. Ella nos muestra, no solo el objeto de la tutela penal, sino también la verdadera esencia del delito. Si formalmente el delito es violación de una norma jurídica, de índole penal, sustancialmente consiste en la ofensa al bien que esa norma trata de proteger. Dicha ofensa constituye el contenido sustancial del delito y en ella se compendia el denominado daño penal.

Es así como por bien jurídico en el campo del Derecho Penal, hay que entender, no ya una realidad natural, social o económica, protegida por el derecho, sino “el aspecto central de la

[9] Francisco González de la Vega, *Derecho Penal Mexicano*, México, Editorial Porrúa, 1996, p. 48.

finalidad de la proposición normativa, que expresa la razón de ser de la disposición incluida en el sistema de los valores jurídicos, pone atinadamente de relieve que la individualización del bien protegido es el resultado de la interpretación y, como tal, no puede ayudar a esta."[10]

De esta manera podemos estimar que, el delito será la acción u omisión ilícita y culpable expresamente descrita por la ley bajo la amenaza de una pena o sanción criminal. Por tanto, el solo pensamiento de cometer una acción no constituye delito alguno, ya que para la existencia de éste se requiere de una acción u omisión en el mundo físico. Desde luego, esa acción de traduce en un hacer (acción propiamente dicha) o en un no hacer (omisión), que produzcan un resultado en el mundo físico, es decir, consista en una acción u omisión previstas en la ley.

Como se puede observar de las definiciones anteriormente citadas, se hace abstracción de la imputabilidad, ya que ésta implica la capacidad de ser sujeto activo del delito, o sea, no es un comportamiento propio del delito. La imputabilidad no es mencionada, por tratarse de una referencia al delincuente y no al delito.

Como concepto penal la imputabilidad se reduce a la capacidad de ser activo del delito, con dos referencias:

a) un dato de orden objetivo, constituido por la mayoría de edad dentro del derecho penal, que puede o no coincidir con la mayoría de edad civil o política y;

b) un dato de orden subjetivo, el que expresado en sentido llano se reduce a la normalidad mental, normalidad que comprende la capacidad de querer y comprender "el significado de la acción."[11]

1.1. Elementos del delito

El delito tiene diversos elementos que conforman un todo. Para Maurach el delito es una acción típicamente antijurídica, atribuible;[12] para Berling es la acción típica, antijurídica, culpable, sometida a una adecuada sanción penal y que llena las condiciones objetivas de penalidad; Max Ernesto Mayer define al delito como acontecimiento típico, antijurídico e imputable; Eduardo Mezger afirma que el delito es una acción típicamente antijurídica y culpable; para Jiménez de Asúa es un acto típicamente antijurídico culpable, sometido a veces a condiciones objetivas de penalidad imputable a un hombre y sometido a una sanción penal.

[10] César, Beccaria, *Tratado de los Delitos y de las Penas*, México, Editorial Porrúa, 1995, p. 56.
[11] Eduardo Betancourt López, op. cit. p. 34.
[12] Eduardo Betancourt López, op. cit. p. 34.

Las definiciones anteriormente citadas así como las que se señalaron en párrafos anteriores, nos muestran como los elementos del delito, según su concepción positiva y negativa, son los siguientes:

Positivos	**Negativos.**
a) Conducta	**a) Ausencia de conducta**
b) Tipicidad	**b) Ausencia de tipo o atipicidad.**
c) Antijuricidad	**c) Causas de justificación.**
d) Imputabilidad.	**d) Inimputabilidad.**
e) Culpabilidad	**e) Inculpabilidad.**
f) Condicionalidad objetiva	**f) Falta de condiciones objetivas.**
g) Punibilidad	**g) Excusas absolutorias.**

De acuerdo a nuestro Derecho Positivo Mexicano, el Código Penal para el Distrito Federal, en su artículo séptimo define al delito como el "acto u omisión que sancionan las leyes penales,"[13] así la conducta o hecho se obtiene de este artículo y del núcleo respectivo de cada tipo o descripción legal.

La tipicidad se presentará cuando exista una adecuación de dicha conducta a alguno de los tipos descritos en el Código Penal; la antijuricidad se presentará cuando el sujeto no esté protegido por una causa de licitud descrita en el artículo 15 del Código Penal.

La imputabilidad se presenta cuando concurre la capacidad de obrar en el Derecho Penal, es decir, que no se presente la causa de inimputabilidad descrita en la fracción VII del artículo 15 de la Ley Penal Federal.[14]

Habrá culpabilidad de acuerdo a los artículos 8 y 9 de nuestra Ley Penal. La punibilidad existe cuando no se presentan las excusas absolutorias descritas por nuestro Derecho Positivo (federal).

Las condiciones objetivas de punibilidad se presentan cuando al definir la infracción punible se establecen requisitos constantes, pero aparecen variables de acuerdo a cada tipo penal; pueden o no presentarse.

[13] *Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal*, p. 19.
[14] Gabriela Barrios Garrido, *et al*., *Internet y Derecho en México*, México, Ed. Mc Graw Hill, 1998, p. 80.

Como se puede observar, el delito tiene un gran contenido en cuanto a los elementos que lo componen y en relación a éstos, existen diversas corrientes de la doctrina, los cuales tratan de explicar algunos de ellos, como la teoría causalista y finalista de la acción, la teoría psicologista y normativista, el modelo lógico y la teoría sociologista.

Ahora, entraremos al estudio de cada uno de los elementos que componen al delito.

1.1.1. La conducta

La conducta es el primer elemento básico del delito, y se define como el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito,[15] lo que significa que sólo los seres humanos pueden cometer conductas positivas o negativas, ya sea una actividad ó inactividad respectivamente. Es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito porque tiene una finalidad al realizarse la acción u omisión.

La conducta puede ser de acción o de omisión y esta última se subdivide en omisión simple y comisión por omisión.

La conducta tiene tres elementos:

1) un acto positivo o negativo (acción u omisión).
2) un resultado.
3) una relación de causalidad entre el acto y el resultado.

El acto, es el comportamiento humano positivo o negativo que produce un resultado. Un acto positivo será una acción, que consiste en una actividad, en un hacer; mientras que, lo negativo será la omisión, que es una inactividad, es decir, cuando la ley espera una conducta de un individuo y éste deja de hacerla.

Por su parte el delito de Acción se define como aquella actividad que realiza el sujeto, produciendo consecuencias en el mundo jurídico, en dicha acción debe de darse un movimiento por parte del sujeto, de esta manera, la conducta de acción tiene tres elementos:

a) movimiento;
b) resultado;
c) relación de causalidad.

La acción en sentido estricto, es la actividad voluntaria realizada por el sujeto, consta de un elemento físico y de un elemento psíquico, el primero es el movimiento y el segundo la voluntad

[15] Francisco González de la Vega, *op. cit*., p. 73.

del sujeto, esta actividad voluntaria produce un resultado y existe un nexo causal entre la conducta y el resultado.

Dicho resultado de la acción debe ser sancionado por la ley penal, es decir, deberá configurar un delito descrito y penado en la ley, será intrascendente que lesione intereses jurídicos protegidos por la ley o sólo los ponga en peligro según el tipo penal.

Según nuestro Derecho Positivo Mexicano, en el Código Penal en su artículo séptimo, el delito es "el acto u omisión que sancionan las leyes penales", de donde se desprende el elemento conducta, pudiéndose presentar como una acción u omisión.

Así pues, la omisión, es "la inactividad voluntaria cuando existe el deber jurídico de obrar."[16]

La omisión tiene cuatro elementos:

a) Manifestación de la voluntad.
b) Una conducta pasiva. (inactividad).
c) Deber jurídico de obrar.
d) Resultado típico jurídico.

Estos delitos se clasifican en delitos de omisión simple o propios y delitos de comisión por omisión o impropios, respondiendo a la naturaleza de la norma, los primeros consisten en omitir la ley, violan una preceptiva, mientras los segundos, en realizar la omisión con un resultado prohibido por la ley. La primera no produce un resultado material, la segunda sí.

En los delitos de simple omisión, se viola una norma preceptiva penal, mientras en los de comisión por omisión se viola una norma preceptiva penal o de otra rama del derecho y una norma prohibitiva penal.

Los delitos de omisión simple producen un resultado típico, y los de comisión por omisión un resultado típico y uno material. En los delitos de omisión simple, se sanciona la omisión y en los de comisión por omisión, no se sanciona la omisión en sí, sino el resultado producido.

Ahora bien, el aspecto negativo de la conducta es la ausencia de conducta, la cual abarca la ausencia de acción ó de omisión de la misma, en la realización de un ilícito.

Nuestro Derecho Positivo Mexicano, en el artículo 15 del Código Penal Federal, en su fracción primera, determina como causa de exclusión del delito que: "el hecho se realice sin intervención de la voluntad del agente,"[17] esto es la afirmación de que no puede constituir una conducta delictiva cuando no se presenta la voluntad del agente.

[16] José Arturo González Quintanilla, *op. cit*. p. 50.
[17] *Op. cit.* p. 19.

El artículo 12º del Código Penal, menciona como causas excluyentes de incriminación, en su fracción I: "el violar la ley penal por fuerza física irresistible o cuando haya ausencia de voluntad del agente…"[18]

1.1.2. La tipicidad

La tipicidad es la adecuación de la conducta al tipo penal. En este sentido diversos autores han dado su definición de tipicidad; dentro de las más importantes tenemos la expresada por Francisco Blasco y Fernández de Moreda, la cual dice: "la acción típica es sólo aquella que se acomoda a la descripción objetiva, aunque saturada a veces de referencia a elementos normativos y subjetivos del injusto de una conducta que generalmente se reputa delictuosa, por violar, en la generalidad de los casos, un precepto, una norma, penalmente protegida."[19]

Se debe tener cuidado de no confundir la tipicidad con tipo, la primera se refiere a la conducta, y el segundo pertenece a la ley, a la descripción o hipótesis plasmada por el legislador sobre un hecho ilícito, es la fórmula legal a la que se debe adecuar la conducta para la existencia de un delito.

La tipicidad se encuentra fundamentada en el artículo 14 Constitucional, párrafo tercero, que a la letra dice: "En los juicios de orden criminal, queda prohibido imponer, por simple analogía y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata."[20]

El aspecto negativo de la tipicidad es la atipicidad. La atipicidad es la falta de adecuación de la conducta al tipo penal. Es importante diferenciar la atipicidad de la falta de tipo, siendo que en el segundo caso, no existe descripción de la conducta o hecho, en la norma penal.

1.1.3. La antijuricidad

La antijuricidad la podemos considerar como un elemento positivo del delito, es decir, cuando una conducta es antijurídica, es considerada como delito. Para que la conducta de un ser humano sea delictiva, debe contravenir las normas penales, es decir, ha de ser antijurídica.

---

[18] *Ibidem*, p.17.
[19] José Arturo González Quintanilla, *op. cit*. p. 63.
[20] *Constitución Política de los Estados Unidos Mexicanos*, p. 10.

La antijuricidad es lo contrario a Derecho, por lo tanto, no basta que la conducta encuadre en el tipo penal, se necesita que esta conducta sea antijurídica, considerando como tal, a toda aquella definida por la ley, no protegida por causas de justificación, establecidas de manera expresa en la misma.[21]

La causa de justificación, es cuando en un hecho presumiblemente delictuoso falta la antijuricidad, por lo que se puede decir que, no hay delito por la existencia de una causa de justificación, es decir, el individuo ha actuado en determinada forma sin el ánimo de transgredir las normas penales. Así, si un hombre ha matado a otro, en defensa de su vida injustamente atacada, estará en una causa de justificación, excluyéndose la antijuricidad en la conducta del homicida.

1.1.4. La culpabilidad

El concepto de la culpabilidad, dependerá de la teoría que se adopte, pues no será igual el de un psicologista, el de un normativista o el de un finalista.

Así, el primero diría, la culpabilidad consiste en el nexo psicológico que une al sujeto con la conducta o el resultado material, el segundo expresaría, es el nexo psicológico entre el sujeto y la conducta o el resultado material, reprochable, y el tercero, afirmaría, que la culpabilidad es la reprochabilidad de la conducta, sin considerar el dolo como elemento de la culpabilidad, sino de la conducta.

La culpabilidad en la tesis finalista se reduce a la reprochabilidad y a diferencia de la teoría normativa el dolo y la culpa no son elementos de la culpabilidad porque son contenido del tipo.

"La culpabilidad es por lo tanto, responsabilidad, apartándose consecuentemente de los normativistas mantienen el dolo y la culpa en la culpabilidad, constituyendo como se afirma por un sector un *mixtum compositum*, de cosas no pueden mezclarse."[22]

El concepto de culpabilidad como tercer aspecto del delito y de acuerdo a la definición anterior, nos señala cuatro importantes elementos que la conforman y son: una ley, una acción, un contraste entre esta acción y esta ley, y el conocimiento de esta situación.

La culpabilidad es un elemento básico del delito y es el nexo intelectual y emocional que una al sujeto con el acto delictivo.

---

[21] Gustavo Malo Camacho, *Derecho Penal Mexicano*, México, Editorial Porrúa, 1998, p.68.
[22] Ibidem, p. 86.

1.1.5. La punibilidad

La punibilidad es un elemento secundario del delito, que consiste en el merecimiento de una pena, en función o por razón de la comisión de un delito; dichas penas se encuentran señaladas en nuestro Código Penal.

Cuello Calón, considera que la punibilidad no es más que un elemento de la tipicidad, pues el hecho de estar la acción conminada con una pena, constituye un elemento del tipo delictivo.

Morón Lerma, dice que la punibilidad "es el conjunto de los presupuestos normativos de la pena, para la ley y la sentencia, de acuerdo con las exigencias de la Idea del Derecho."[23]

Por su parte Ignacio Villalobos, tampoco considera a la punibilidad como elemento del delito, ya que el concepto de éste no concuerda con el de la norma jurídica: “Una acción o una abstención humana son penadas cuando se les califica de delictuosas, pero no adquieren este carácter porque se les sancione penalmente. Las conductas se revisten de delictuosidad por su pugna con aquellas exigencias establecidas por el Estado para la creación y conservación del orden en la vida gregaria y por ejecutarse culpablemente. Mas no se pueden tildar como delitos por ser punibles."[24]

El aspecto negativo de la punibilidad se llama excusa absolutoria. Son excusas absolutorias las causas que hacen que a un acto típico, antijurídico, imputable a un autor y culpable, no se asocie pena alguna por razones de utilidad pública. Las excusas absolutorias son aquellas circunstancias específicamente señaladas en la ley y por las cuales no se sanciona al agente. Así como la punibilidad no es considerada por muchos autores de elementos del delito, así tampoco la imputabilidad como se mencionará en el siguiente apartado.

1.1.6. La imputabilidad

La imputabilidad es la capacidad de querer y entender. En el campo del Derecho Penal, querer es estar en condiciones de aceptar o realizar algo voluntariamente y entender es tener la capacidad mental y la edad biológica para desplegar esa decisión.[25]

---

[23] Ernesto Morón Lerma, *Internet y derecho penal: hacking y otras conductas ilícitas en la red*, Madrid, Ed. Rústica, 1999, p. 145.
[24] Ignacio Villalobos, *op. cit*. p. 174.
[25] Gustavo Malo Camacho, *op. cit*., p. 76.

El aspecto negativo de la imputabilidad es la inimputabilidad, consistente en la incapacidad de querer y entender en el mundo del Derecho. Son aquellas causas en las que si bien el hecho es típico y antijurídico, no se encuentra el agente en condiciones de que se le pueda atribuir el acto que perpetró, por lo tanto, ésta implica la capacidad de ser sujeto activo del delito, no es un comportamiento propio del delito. La imputabilidad no es mencionada, por tratarse de una referencia al delincuente, no al delito.

Teniendo en cuenta los elementos antes mencionados, se puede afirmar que el delito es un hecho jurídico, es decir, es un hecho que tiene importancia jurídica, por cuanto el derecho le atribuye consecuencias jurídicas, el nacimiento de derechos para el agraviado y para el Estado, como el persecutor de los delitos, y pérdida de derechos para el delincuente.

1.2. Tipos de delito

Como el delito es un hecho jurídico voluntario, supone que él es ante todo un hecho humano y no un hecho natural. Es una acción, un obrar con efectos comprobables en el mundo exterior, y no una simple declaración de voluntad; y es, además, una acción voluntaria y consciente, y por tanto imputable, es decir, referible al sujeto activo como suya. Lo que da lugar a la codificación de los tipos de delito citados a continuación:

1.2.1. Delitos de acción y de omisión

Son delitos de acción los que se cometen por medio de una conducta positiva, es decir un hacer.[26] Los delitos por omisión se ejecutan por medio de un comportamiento negativo,[27] en no hacer determinada obligación o no ejecutar una acción. Además, existen delitos que, por su índole estructural, exigen para su existencia la incidencia de una acción y luego una omisión, o viceversa.

1.2.2. Delitos de sólo de conducta y de resultado

Los delitos que no necesitan resultado material, ya que la sola conducta del sujeto los realiza, son

[26] Eduardo Betancourt López, *op. cit.*, p. 98.
[27] *Idem.*

los que se perfeccionan con el cumplimiento de determinada acción u omisión,[28] cuya consecuencia es la no observación de una obligación o de un deber, pero cuyo resultado no se manifiesta en el mundo físico con un hecho, de momento, perceptible. En tanto, que los delitos de resultado son los que para su consumación exigen, además, de la conducta del sujeto activo que se produzca determinado efecto, distinto de la omisión o de la acción;[29] el resultado en estos delitos se observa físicamente en el mundo real. Los delitos se clasifican de esta manera, por que se atiende a la estructura exterior de ellos.

1.2.3. Delitos de daño y de peligro

Los delitos de daño requieren para su perfeccionamiento jurídico que el bien tutelado, jurídicamente protegido, sea destruido o disminuido;[30] en tanto en los delitos de peligro, basta que el bien jurídico sea amenazado al realizarse la conducta criminosa, acción u omisión,[31] con la causación de un daño o peligro inminente, determinado y grave.

1.2.4. Delitos instantáneos y permanentes

Son delitos instantáneos, aquellos que con la sola realización de la conducta, acción u omisión, por el sujeto activo quedan realizados o tipificados, sin que se requiera acción posterior para su continuidad o vigencia.[32] Los delitos permanentes, son los que se caracterizan porque el hecho que los constituye o realiza da lugar a una situación dañosa o de peligro, que se prolonga en el tiempo a causa de la continuidad del comportamiento del sujeto.[33] Para la existencia de estos delitos, es necesario que el estado dañoso o de peligro, provenga de la conducta del sujeto activo de manera continua, es decir, que no se agote en un solo instante, sino que prosiga durante determinado tiempo; y que la prórroga de la situación antijurídica se deba a la exclusiva conducta voluntaria del sujeto, que prosigue con ella ininterrumpidamente después de la realización del hecho que constituye el delito.

---

[28] *Ibidem*, p. 99.
[29] *Ídem.*
[30] *Ibidem*, p. 100.
[31] *Ídem.*
[32] Eduardo Betancourt López, *op. cit.*, p. 100.
[33] *Ídem.*

Ahora bien, dentro de las especies del delito, que por ser varias, conforme a los fines que se persigan para su tipificación, o conforme al bien jurídico que tutela la ley, entre otros aspectos tenemos ahora otra serie de clasificaciones:

- Conforme a su gravedad: aquí se puede hablar de delitos y faltas; habrá delito siempre que se realice la conducta prevista y sancionada por la ley penal o en alguna otra ley especial,[34] en tanto que la falta, no obstante ser una conducta contraria a la ley y sancionada por esta misma,[35] es penalizada y aplicada por una autoridad u órgano diferente al Poder Judicial o Tribunal, generalmente una autoridad de índole administrativa.
- Según la intención con que se comete o realiza la acción que da origen al delito, tenemos delitos con intención o dolosos, culposos o contra la intención y los que son cometidos más allá de la intención o preterintencionales.[36] Si se ha deseado realizar la acción u omisión para la comisión del delito y previsto el resultado del mismo, se está ante un delito doloso. En tanto, que sí de deseaba realizar la acción u omisión, pero no el resultado del delito, se trata de un delito culposo. Y cuando se ha deseado realizar la acción u omisión y no el resultado como consecuencia, en su integridad, sino un efecto menos grave, se trata de un delito preterintencional.
- Los delitos tipo, o también simples o netos,[37] son los que se presentan en su puro modelo legal, sin más características que sus elementos esenciales; y los delitos circunstanciados[38] son los que además de contar con los elementos esenciales, se presentan acompañados de circunstancias o accidentes a sus elementos.
- Por su efecto, los delitos se consideran simples y complejos, formales y materiales, de lesión y de peligro.[39] Son simples, o unisubsistentes, en el que coincide el momento ejecutivo y el momento consumativo, se realizan ambos en un sólo acto o momento. Los complejos o plurisubsistentes, son aquellos cuya acción ejecutiva consta de varios actos en que puede integrarse. El delito material es el que se consuma al momento de verificarse el resultado material de ése; en tanto que el delito formal se perfecciona con una simple acción u omisión, haciendo abstracción de la verificación del resultado.

[34] *Ibidem,* p. 102.
[35] *Ídem.*
[36] *Ídem.*
[37] Eduardo Betancourt López, *op. cit.*, p. 109.
[38] *Ídem.*
[39] *Ídem.*

- Según el objeto o fin que persiguen, la perturbación, daño, disminución o destrucción del bien jurídicamente protegido, son delitos contra la cosa pública o el Estado mismo o contra sus Instituciones y delitos contra las personas privadas, delitos políticos y no políticos.[40]
- Según los sujetos que los realizan, los delitos individuales y colectivos, comunes y especiales según la ley que los contenga; y ocasionales y habituales según la constancia con que delinque el sujeto que los realiza.[41]
- Según los requisitos para la procedibilidad o persecución de los delitos, conforme al bien jurídico protegido que afecta, de acuerdo a la naturaleza del daño afectación del bien, los delitos son de acción pública (denuncia) o de acción privada (querella).[42]

1.3. Clasificación de los delitos atendiendo a diversos criterios legales

Para el desarrollo de este punto se tomarán en cuenta las disposiciones legales que se contienen en el Código de Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, el Código de Procedimientos Penales para el Distrito Federal y el Código Federal de Procedimientos Penales. Por lo que, las clasificaciones de los delitos que ahora se presentarán será desde el punto de vista legal, es decir, atendiendo a lo dispuesto en los ordenamientos legales vigentes de índole penal, sustantiva y adjetiva, según se trate.

1.3.1. Desde el punto de vista de su persecución

Dado que el Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia Federal, contiene una gama muy amplia de conductas previstas como delitos, que tratan de abarcar la mejor protección a la sociedad y al Estado mismo; para proceder a la clasificación de la que se ocupa este punto, se ha considerado tomar en cuenta a los delitos más representativos de ese ordenamiento legal, a fin de que se tenga una visión general del mismo; pues el análisis del Código Penal que ahora nos ocupa, para ser completo y detallado, dada su amplitud, rebasaría, con mucho, los fines de este capítulo resumido del delito.

[40] Ignacio Villalobos, *op. cit*., p. 286.
[41] *Ibidem*, p. 290.
[42] *Idem*.

Así tenemos que un delito se perseguirá de oficio, sin que medie denuncia o querella alguna, cuando afecte un bien jurídico protegido que interese a la sociedad, la seguridad interna o externa del Estado y a las Instituciones del mismo,[43] tales como:

a) Los delitos ambientales, contenidos en la Ley Forestal y previstos en los artículos 416 al 420 del Código Penal, en atención a que se perjudiquen los recursos naturales de la Nación, la persecución de estos delitos es una obligación de las autoridades, cualquiera que tenga conocimiento del hecho delictivo.
b) Delitos cometidos en contra de las Instituciones del Estado, su seguridad, contenidos en los artículos 130, 131, 132, 140, entre otros, del Código Penal, que son los de sedición, motín, rebelión y sabotaje; su persecución es de oficio, ya que ponen en peligro al Estado mismo.
c) Los delitos cometidos en agravio del núcleo familiar en particular, se persiguen a petición de parte, es decir, por querella; entre estos tenemos a los siguientes: Abandono de personas (hijo o cónyuge), contenidos en el artículo 336 del Código Penal.
d) Los delitos cometidos en agravios del bien jurídico de la vida, la integridad corporal y la libertad sexual personal, representados por los delitos de homicidio, lesiones y violación, su persecución es de oficio, ya que no solamente interesan al individuo sino también a la sociedad, los bienes jurídicos protegidos por la ley penal.

De esta manera se pueden ir analizando todas las disposiciones legales contenidas en el código Penal, cualquiera, y se podrá determinar el bien jurídico protegido, y con ello la forma en que es perseguido ese delito, de oficio o por querella; por lo que se considera inútil proseguir con el desarrollo de este contenido.

1.3.2. Desde el punto de vista de su tipificación como delincuencia organizada

Este tipo de delitos están contenidos en una ley especial, íntimamente relacionada con el Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, ya que estos ilícitos se encuentran previstos en la ley penal, pero con una regulación deficiente que no permite la previsión de la gama completa de actividades o conductas que abarcan estos delitos. Esa legislación especial es la Ley Federal Contra la Delincuencia Organizada.

[43] *Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal*, p. 20

En el caso que ahora nos ocupa, como ya se apuntó, esos delitos se encuentran referidos al Código Penal de mérito. No obstante que no se mencione la pluralidad de sujetos activos en la comisión del delito, dada la propia naturaleza del delito que se comete, ya que para su comisión y/o existencia se requiere de una pluralidad de sujetos activos, ya que por uno sólo sería imposible de cometer, pues el bien jurídico que afecta implica diversas actividades que requieren en concurso de voluntades y actividades a un mismo fin específico.

A continuación se mencionan algunos delitos cometidos por la delincuencia organizada.

- La utilización de explosivos, sustancias tóxicas, armas de fuego o por incendio, inundación, o por cualquier otro medio violento, para la realización de actos en contra de las personas, las cosas o servicios al público, que produzcan alarma, temor, terror en la población o en un grupo o sector de ella, para perturbar la paz pública, o tratar de menoscabar la autoridad del Estado, o presionar a la autoridad para que tome una determinación.[44] Estos ilícitos van en detrimento de la paz pública y de las instituciones y la seguridad del Estado, ya que socavan su integridad y seguridad interna.[45]
- La producción, transporte, tráfico, comercio, suministro aún gratuitamente o prescripción alguna de los narcóticos señalados en el artículo 193 del Código Penal, sin la autorización correspondiente a que se refiere la Ley General de Salud; de acuerdo a lo previsto por el artículo 194 del citado Código. Se trata del caso de delitos contra la salud, narcotráfico, en las modalidades que se señalan.
- La posesión de alguno de los narcóticos señalados en el artículo 193 del Código Penal, sin la autorización correspondiente a que se refiere la Ley General de Salud, siempre y cuando esa posesión sea con la finalidad de realizar alguna de las conductas previstas en el artículo 194, del mismo Código; previsión penal contenida en el numeral 195, primer párrafo, del Código que nos ocupa. De igual forma que el anterior, es un caso de modalidad de los delitos contra la salud o narcotráfico de estupefacientes.
- La comisión de los delitos de falsificación de moneda, la alteración de moneda o la circulación de moneda alterada y la prestación de un servicio o desempeño de un cargo o comisión en la casa de moneda o cualquier empresa que fabrique copetes, y que por cualquier medio, haga de las monedas de oro, plata, platino o paladio contengan metal diverso al señalado por la ley o tengan menor peso que el legal o una ley de aleación inferior; Estos

[44] Estos delitos se encuentran detallados en el artículo 2º de la *Ley Federal contra la Delincuencia Organizada*.
[45] Conforme al primer párrafo del artículo 139 del Código Penal Federal.

delitos son cometidos en contra de la economía del Estado, ya que con ellos se le causan un grave perjuicio a la economía nacional.[46]

- Al que en despoblado o en paraje solitario haga uso de violencia sobre una persona con el propósito de causar un mal, obtener un lucro o de exigir su asentamiento para cualquier fin y cualesquiera que sean los medios y el grado de violencia que se empleen y a los salteadores que atacaren una población o al que en caminos o carreteras haga uso de la violencia en contra de los ocupantes de un vehículo, ya sea de transporte público o particular; conforme a los artículos 286 y 287 del código Penal Federal. Ya que este ilícito perturba de grave manera la seguridad pública.
- La privación de la libertad, como delito previsto por el artículo 366 del Código Penal.
- Toda persona que con el consentimiento de un ascendiente que ejerza la patria potestad o de quien tenga a su cargo la custodia de un menor, aunque esta no haya sido declarada, ilegítimamente lo entregue a un tercero para su custodia definitiva, a cambio de un beneficio económico.[47]

1.3.3. Desde el punto de vista de su tentativa punible

Como ya se apuntó en párrafos anteriores, la tentativa de un delito es la circunstancia que sucede, por parte del agente activo del delito, para no culminar la realización de la conducta constitutiva de delito; sin embargo, los hechos preparatorios para la comisión del delito, pueden en sí mismo constituir una conducta delictiva, cuando no un delito grave, cuya preparación debe ser sancionada para brindar la seguridad necesaria a los individuos, la sociedad y a las instituciones del Estado.

En este orden de ideas, es que conforme al artículo 194 del Código Federal de Procedimientos Penales, se prevén ciertas tentativas de delito punibles conforme a la gravedad de los delitos cuya consecuencia sería la lógica; pues de no ser así, el orden público y la seguridad social y nacional, de manera continua estarían en peligro, ya que esos delitos y sus tentativas, casi siempre constituyen delitos en los que el sujeto pasivo es el Estado mismo y las Instituciones que lo representan.

[46] Conforme a los artículos 234, 236 y 237 del Código Penal Federal.
[47] Delito previsto por el artículo 366, tercer párrafo, del Código Penal, en el que el sujeto pasivo es el menor y la sociedad, además de la familia, de ahí la gravedad del mismo.

Para el caso de que la tentativa suceda, conforme a la ley penal, solamente se castiga la conducta delictiva que haya sucedido hasta el momento en que el agente activo del delito desistió de su intento de delinquir; pero cuando se trata de delitos que no son considerados graves, esa tentativa sólo será punible a petición de la parte agraviada, por medio de la formulación de la querella correspondiente.

A continuación se señalarán los delitos graves, cuya tentativa es penada por la ley penal, concretamente en el numeral 194 del Código Federal de Procedimientos Penales conforme los prevé el Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal, como ya fue apuntado.

- La tentativa del delito de genocidio, homicidio genérico y por culpa grave, previstos en los artículos 149 bis, 302 al 307, 313, 315 bis, 320, 323 y 60, párrafo tercero, del Código Penal, respectivamente, que afecta el bien jurídico protegido de la vida humana.
- La tentativa de los delitos de Traición a la patria, espionaje, terrorismo, sabotaje, piratería, evasión de presos y falsificación y alteración de moneda, los que afectan a la seguridad interna y externa del Estado y a sus Instituciones representativas, así como a la paz interior y a la seguridad nacional, no solamente en tiempos de guerra, sino en cualquier momento.[48]
- La tentativa de los delitos de ataques a las vías de comunicación y el uso ilícito de instalaciones destinadas al tránsito aéreo, previstos en los artículos 168, 170 y 172 bis, respectivamente, del Código Penal; en los que el bien jurídico protegido la libertad en el uso de las instalaciones de las vías de comunicación y de tránsito aéreo, bajo las condiciones que señale la misma ley que las regula.
- La tentativa de los delitos contra la salud, en cualquiera de sus modalidades, previstos en los artículos 194 al 198 del Código Penal; ya que el bien jurídicamente protegido por la ley penal es la salud pública y el bienestar social.
- La tentativa de los delitos de corrupción de menores, trata de personas, la explotación de un menor de edad por medio del comercio carnal y violación, previstos en los artículos 201, 205, segundo párrafo, 208, 265, al 266 bis, respectivamente, del Código Penal; en los que la persona, menor de edad, la familia y la libertad sexual, son los bienes jurídicos protegidos por la ley penal.

[48] Previstos en los artículos 123, 124, 125, - 126, 127, 128, 139, 140, 142, 145, 146, 147, 234, 236 y 237, respectivamente, del Código Penal.

- La tentativa de los delitos de asalto en carreteras o caminos y el de robo calificado, previstos en los artículos 286 y 367, respectivamente, del Código Penal; donde se protege el patrimonio de las personas, en cualquier sitio en que se encuentren.
- La tentativa de los delitos de extorsión y tortura, previstos en los artículos 390 del Código Penal y 3 y 5 de la Ley Federal para Prevenir la Tortura, respectivamente; en los que se protege al particular en contra de los abusos de la autoridad, a fin de que no quede impune la actitud deshonesta de ésa.
- La tentativa del delito de operaciones con recursos de procedencia ilícita. El bien jurídico protegido es la economía, a fin de evitar la desleal competencia por la desproporción de recursos económicos de algunas personas.[49]
- La tentativa de los delitos previstos en los artículos 104, fracciones II y III, último párrafo y 105, fracción IV, del Código Fiscal de la Federación; en los que el bien jurídico protegido por esta ley especial, es el erario público del Estado.
- La tentativa de los delitos previstos en la Ley General de Población, tales como el tráfico de indocumentados.
- La tentativa de los delitos previstos en los artículos 83, fracción III, 83 bis y 84 de la Ley de Armas de Fuego y Explosivos.
- La tentativa del delito de secuestro, previsto en el artículo 366 del Código Penal, en el que bien jurídico protegido es la libertad de la persona.

1.3.4. Desde el punto de vista de su gravedad

La clasificación que se da a continuación es conforme al artículo 268 del Código de Procedimientos Penales para el Distrito Federal; aclarándose, también, que la referencia a la legislación sustantiva lo es el Código Penal para el Distrito Federal en Materia de Fuero Común y para toda República en Materia de Fuero Federal.

En este caso, como ya fue apuntado, los delitos se consideran graves en atención al bien jurídico protegido, por la ley penal, que afectan; el que no solamente repercute en la persona del ofendido directamente, como en el caso del homicidio, sino también en la familia, como la

[49] Previsto en el artículo 400 bis del Código Penal, referido a los recursos provenientes del narcotráfico, sobre todo, o de algún otro tipo de delito grave, como el secuestro.

corrupción de menores, entre otros, al Estado mismo, tratándose del caso del terrorismo, al patrimonio de cualquier persona, como se verá a continuación:

- El delito de homicidio, cualesquiera que sean las circunstancias de su comisión, previsto en los artículos 302 al 307, 313, 315 bis, 320 y 323, y tratándose del causado por culpa grave en relación con el 80, párrafo tercero, del Código Penal. Que afecta, en primer término al sujeto pasivo del delito, el occiso, el que sufre la privación de la vida.
- Los delitos de Terrorismo, sabotaje, evasión de presos y ataques a las vías de comunicación,[50] en los que el sujeto pasivo es la seguridad de las instituciones del Estado y la sociedad.
- Los delitos de corrupción de menores, trata de personas, explotación del cuerpo de un menor de edad por medio del comercio carnal y violación, previstos en los artículos 201, 205, segundo párrafo, 208, 265 al 266 bis, respectivamente, del Código Penal; en los que el sujeto pasivo es la familia y la sociedad, el cuerpo del menor y la libertad sexual del agredido.
- Los delitos de asalto, robo y despojo.[51] Este ilícito lo resiente el patrimonio del sujeto pasivo, al ser privado, con la realización de la conducta delictiva, de la propiedad y posesión de sus bienes.
- El delito de secuestro, previsto en el penúltimo párrafo del artículo 366 del Código Penal; en el que el bien jurídico protegido es la libertad y el patrimonio del individuo.
- Los delitos de extorsión y tortura,[52] en los cuales el bien jurídico protegido es la libertad de la persona y su seguridad en su trato para con las autoridades.

1.4. Los delitos conforme a la legislación que los tipifica

Los delitos, desde este punto de vista, son delitos del fuero común y delitos del fuero federal, conforme a la ley en que están previstos; delitos comunes y delitos especiales, atendiendo a la ley que los contiene.[53] Los delitos del fuero común en cuanto a conductas ilícitas previstas y sancionadas en la ley correspondiente, delimitan el delito cuando éste afecta los intereses de la entidad federativa o de la población de la misma; por otra parte, en la República Mexicana, por

[50] Previstos en los artículos 139, párrafo primero, 140, primer párrafo, 150, 152, 168 y 170 del Código Penal, respectivamente.
[51] Previstos en los artículos 286, párrafo segundo, 287, 367, 370, párrafos segundo y tercero, 372, 377, 381, fracciones VIII, IX y X, y 381 bis, 395, último párrafo, respectivamente, del Código Penal.
[52] Previstos en los artículos 390 del Código Penal y 3 y 5 de la Ley Federal para Prevenir y Sancionar la Tortura, respectivamente;
[53] Ignacio Villalobos, *op. cit*. p. 293.

ser una federación, existen entidades federativas, soberanas e independientes entre sí, con un gobierno interno propio, pero que unidas dan lugar a la federación, representado por el Gobierno Federal; lo anterior da lugar a que cada entidad federativa tenga sus propias leyes internas, como el Código Penal y el Código de Procedimientos Penales, con aplicación y vigencia únicamente en la circunscripción territorial de la entidad federativa; en tanto que la federación representada por el Gobierno Federal y sus instituciones, tienen la facultad de promulgar leyes que regulen situaciones que atañan a la federación y a las entidades federativas, en lo individual o en conjunto. A estas leyes se les denomina del fuero federal, y así tenemos al Código Penal Federal y al Código Federal de Procedimientos Penales, entre otros ordenamientos o leyes.[54]

Las leyes federales al regular u ocuparse de situaciones que son propias a la federación, sus instituciones, cuestiones que importen a dos o más entidades federativas, en la ley penal de este orden las conductas ilícitas que se prevean y sancionen en el Código Penal Federal, tendrán el carácter de delitos del fuero federal, en tanto que los que se contengan en el Código Penal de la entidad federativa, serán delitos del fuero común, porque las conductas que prevén en ese Código sólo interesan a la entidad federativa, a sus instituciones y la población de la entidad. En estos delitos del fuero federal el delito afectará los intereses de la federación.

Existen también los denominados delitos especiales, los cuales requieren para su comisión y existencia de elementos que específicamente señala la ley que los regula, tales como la calidad del sujeto activo, el bien jurídico protegido, o la forma de comisión del delito; en tanto que los delitos comunes no requieren mayores requisitos que los que señala la ley penal sustantiva.[55]

Estos delitos se encuentran tipificados en una ley especial o ajena al Código Penal, que se ocupa de cuestiones de muy diversa índole, pero que prevé conductas ilícitas, delitos, que deben ser castigados por ser contrarios a la ley y a los intereses de la sociedad.

1.5. Las circunstancias de la comisión del delito

Ya se acotó en los puntos anteriores que el delito se comete por medio de una acción u omisión, por parte del sujeto activo del mismo, y que en la comisión de esos ilícitos no solamente intervienen los sujetos activo y pasivo del mismo, sino que existe la intervención de otros sujetos, que si materialmente no realizan el delito sí cooperan con el activo para la realización de ése;

[54] Ignacio Villalobos, *op. cit*. p. 296.
[55] *Ibidem*, p. 290.

éstos son los llamados encubridores y cómplices del sujeto activo del delito,[56] no del delito en sí mismo, ya que el delito es exclusivo del sujeto que realiza la conducta criminosa, pero el auxilio para la comisión de esa conducta es directamente al activo, son las circunstancias que rodean a la comisión del delito y van íntimamente ligadas con el sujeto activo, como se verá a continuación de ese ilícito.

"El encubridor de un delito, o de la conducta delictiva, la que necesariamente será referida a un sujeto, el activo, es toda persona que teniendo conocimiento del delito y del sujeto que lo cometió, no lo denuncia a la autoridad competente o no da la debida cooperación a la investigación y persecución del mismo, teniendo la obligación de hacerlo."[57]

El encubridor no participa ni coopera de ninguna manera en la planeación, ejecución y materialización del delito o de la conducta delictiva, cuando éstos no requieran resultado material, sino que éste únicamente tiene conocimiento de la realización del delito y de sus sujetos activos y los protege, auxilia o asesora para librarse de la acción persecutora de la justicia; la comisión del delito de encubrimiento se da después de que se comete el delito principal, que es el que se trata de encubrir para que no se conozca por la autoridad o para que no sea perseguido y sancionado.

Por su parte, el cómplice del delito y del agente que comete la conducta delictiva, figura antes de la realización del delito; pues es la persona que auxilia al delincuente, o ejecutor material del delito, a la planeación, ejecución y materialización del delito. La actuación del cómplice llega hasta el momento último inmediato antes de la ejecución del delito, ya que entonces se trataría de una coautoría del delito o pluralidad de sujetos activos.[58]

El cómplice es del delincuente, que es el comete la conducta considerada delictiva, no del delito en sí mismo, ya que éste solamente es el resultado que es propio y exclusivo del delincuente. Y esta complicidad abarca cualquier actividad que sea necesaria o complementaria para la realización o materialización del delito, no solamente la actividad material ya que también abarca la intelectual.

Por otra parte, la comisión del delito consistente en un hacer determinada conducta, de manera consiente sobre todo; el delito es el resultado material de una conducta considerada como tal, por tanto, la actividad delictiva sólo culminará con la materialización del resultado previsto con ella, es decir, con la obtención del daño al bien jurídico protegido, no antes; por lo tanto, la

[56] José Arturo González Quintanilla, *op. cit.*, p. 102.
[57] *Idem*.
[58] *Idem*.

complicidad será respecto de la conducta del sujeto que va a delinquir, no del delito mismo, en tanto que el encubrimiento será sobre el delito cometido y el sujeto activo del mismo, con lo que se demuestra que esta conducta es más amplia.[59]

Lo anterior es así, porque la planeación y la idea de cometer un delito, a menos que se trate de uno grave como ya se apuntó, como tentativa no es punible;[60] en tanto, que el incumplimiento de la obligación de dar parte a la autoridad de la comisión de un delito o del delincuente, es un delito diferente al del encubrimiento, ya que éste se dará en cuanto se preste alguna ayuda a ese sujeto activo del delito.[61] Desde luego, existen excepciones a este efecto, conocidas como de causas de inimputabilidad que reconoce la misma ley penal.

De esta manera se han descrito las circunstancias bajo las cuales se desarrolla la comisión del delito, respecto de las personas que intervienen en su comisión, partiendo desde su planeación y preparación hasta su consumación, para después de ésta proceder a la protección del sujeto activo y a la ocultación del delito, con el fin de evitar la sanción a que se ha hecho acreedor el sujeto activo del delito con su conducta. Pues la realización o materialización del delito sólo corresponde al sujeto activo del mismo.

1.6. Las consecuencias del delito

En este punto se desarrollaran las consecuencias legales de la comisión del delito, desde dos aspectos: el legal de la comisión del delito en sí mismo y las que son propias del sujeto activo del delito, además de las que repercuten en el mundo físico por la comisión del delito, como un hecho que puede apreciarse por medio de los sentidos.

Desde el punto de vista del suceso en el mundo físico, la comisión del delito sucede con la realización de un hecho físico, que puede apreciarse fácilmente, como en el caso del delito de homicidio o de lesiones,[62] no así cuando el delito es de mera conducta, caso en el cual sólo pueden apreciarse las consecuencias del delito ligadas a otro hecho físico, como el caso de las calumnias, donde el desprestigio del sujeto pasivo, en caso de darse, depende de la apreciación subjetiva del sujeto pasivo y de la sociedad.[63]

---

[59] José Arturo González Quintanilla, *op. cit*., p. 109.
[60] *Ibidem*, p.112.
[61] *Ídem*.
[62] Francisco González de la Vega, *op. cit*., p.119.
[63] *Ídem*.

En este caso, la consecuencia del delito será aparte de la que prevé la misma ley penal, pues si bien es cierto que se castiga el hecho, desde el punto de vista jurídico, el suceso en el mundo físico no puede remediarse sólo con una disposición legal. Tal es el caso de los delitos de homicidio o de lesiones, a manera de ejemplo, en los que no obstante se castigue al causante del daño en los bienes jurídicos que protege la ley, como la vida humana en el caso del homicidio, o la integridad del cuerpo y la salud del individuo en el delito de lesiones, no puede darse o reintegrarse el suceso a su estado anterior, pues la vida perdida ya no se recupera, y cuando las lesiones dejan secuela por imposibilidad de recuperar los miembros lesionados, la consecuencia del delito en el mundo físico es irreparable.

Todo lo anterior, deriva en el aspecto causal del delito,[64] es decir, las causas que motivan esa conducta ilícita, lo cual corresponde a la sociología del delito, que es tema aparte del que ahora nos ocupa, por lo que no nos ocuparemos más de éste, aunque sí podemos apuntar que, el hecho que sucede en el mundo físico que da origen al delito, adquiere el carácter de jurídico, por tener consecuencias en el mundo jurídico o del derecho penal, ya que con ese hecho físico se actualiza la hipótesis normativa prevista en la ley penal, con lo cual se convierte en jurídico, con las consecuencias que ya se han apuntado al realizarse el delito.[65]

En conclusión, las consecuencias del delito en el mundo físico, dependerán del tipo de delitos que se cometa, es decir de resultado o de mera conducta, en los que la apreciación de las consecuencias variarán; pero siempre habrá consecuencias en éste.

Ahora, por lo que respecta a las circunstancias de comisión del delito, son las propias que rodean al hecho delictivo, los que constituyen los elementos del mismo, tales como el cuerpo del delito, la conducta típica, antijurídica y culpable, así como la presunta responsabilidad del sujeto activo en el ilícito. Son propiamente las circunstancias que rodean la comisión del delito.[66]

La comisión del delito no es únicamente el suceso previsto en la ley penal, con la afectación del bien jurídico protegido, sino que ése está rodeado de varias circunstancias, tales como la elección de los medios adecuados para lesionar ese bien, que la conducta a desarrollar no tenga alguna excluyente de responsabilidad o inimputabilidad, que no incidan en el sujeto activo; además de que real y efectivamente se obtenga el daño deseado del bien jurídico. Ya que en caso contrario, podemos estar frente a una conducta que no obstante pretenda ser delictuosa no constituya delito por la ausencia de ése, como fin.

---

[64] Francisco González de la Vega, *op. cit*., p.119.
[65] *Ibidem*, p. 113.
[66] *Ídem*.

Lo anterior es entendible, ya que si se pretende causar la muerte a un individuo, estaremos ante el delito de homicidio, pero para ello se requiere que el sujeto a quien se desea privar de la vida, tenga ésta precisamente, vida, pues no se puede matar a un muerto, debe de poseer el bien jurídico protegido por la ley penal, para que pueda darse el resultado previsto, la privación de la vida; de igual manera, que el medio a utilizar o emplear para la comisión del delito sea el idóneo, pues no se puede matar a un individuo con solo desearlo, ya que tiene que emplearse algún medio u objeto apropiado para ello, en este caso el objeto con el que se ejecutará el delito tiene importancia. Y, por último, que efectivamente se realice la conducta que produzca como resulta el delito, es decir, se realice la acción de privar de la vida al individuo, es la realización material del delito.

De no darse las tres circunstancias anteriores, no existirá el delito, ya que no se producirá el resultado previsto en la ley penal, ya sea por la falta de la realización de la conducta adecuada, por la falta del objeto jurídico protegido o por la falta de los medios adecuados a tal fin.[67] En este caso, estaremos ante la tentativa de la comisión de un delito, el de homicidio conforme al ejemplo, o ante un delito imposible, ya que no se dan los elementos del mismo previstos en la ley penal.

La tentativa del delito ya se vio en un punto aparte de este mismo estudio, pero ratificaremos que la falta de la realización de la conducta para la comisión del delito, en el caso que nos ocupa, la privación de la vida, no constituirá la comisión del delito de homicidio, sino solamente la tentativa del mismo.

Ahora respecto del delito imposible, este se da por la falta o la inexistencia del bien jurídico protegido por la ley penal,[68] en el caso del delito de homicidio la falta de vida en el individuo, de cuya vida se desea privar; ya que no obstan te que el sujeto muera, puede ser que al momento de pretender privarlo de la vida ya esté muerto, o la causa de la muerte sea una diferente a la que se hubiere empleado para cometer el delito de homicidio.

Ahora, por lo que respecta a las circunstancias propias del sujeto activo del delito, estas se refieren al motivo, causa o conducta que desarrolle el sujeto para la comisión del delito;[69] es decir, el deseo o animo de cometer efectiva y realmente el delito, o solamente de pretender amenazar con cometerlo y, en último caso, cometerlo pretendiendo haberlo realizado sin ánimo alguno de hacerlo.

---

[67] Francisco González de la Vega, *op. cit*., p. 116.
[68] *Ibidem*, p.120.
[69] Francisco González de la Vega, *op. cit*., p. 120.

A partir de estos supuestos es que cobra validez la clasificación de los delitos conforme a la conducta desplegada para su comisión; delitos dolosos, culposos y preterintencionales. Resultando dolosos, aquellos en los que se realizó la conducta conveniente, utilizando los medios idóneos, para obtener el resultado deseado, la comisión del delito ya previsto. Lo que no sucede en los delitos culposos, en los que se presenta el resultado, el delito, sin que se haya deseado cometerlo; pero que, sin embargo, debido a la conducta negligente que observa el sujeto se da el resultado que prevé la norma penal como delito.

Para la imposición de la pena al sujeto activo del delito, es importante que se determine la conducta que desarrolló éste, el ánimo que tuvo para cometer el delito, ya que con ello se demuestra la peligrosidad del sujeto y las posibilidades de reincidencia en el delito de ése, lo que conllevaría la situación de la habitualidad del sujeto activo para el delito.

Como se apuntó a lo largo de este capítulo, el delito es toda acción u omisión punible, objetivizada en la manifestación de un hecho previsto en la ley penal, al cual le recae una sanción, también prevista en la misma ley penal, a fin de que inhibir al individuo a la comisión de esas conductas consideradas como delitos.

En cuanto a las formas de comisión de los delitos, ya se trate de acción o de omisión, éste siempre será una conducta, es decir un hacer o un no hacer, cuyos resultados prevé la ley penal, los que tienen trascendencia en el mundo físico y en el del derecho.

Es de hacer notar que la clasificación de los delitos no es únicamente para fines didácticos o teóricos, sino de índole práctica, ya que con éstas es posible ubicar a los delitos dentro los parámetros que ordenan la persecución de los mismos, la gravedad que les asigna la ley, en cuanto a las consecuencias que tienen dentro de la sociedad, por afectar determinado bien jurídico protegido por la ley penal; la tipificación de los delitos en cuanto a su comisión, así como la punibilidad de los mismos tratándose de la tentativa, etcétera.

Por otra parte, si bien es cierto que solamente las conductas que prevé la ley penal pueden ser consideradas como delitos, la preparación de esas conductas, no obstante que no constituyan propiamente un delito, sí son la tentativa del mismo, la que será penada cuando se pretenda afectar un bien jurídico que trascienda a la seguridad de la sociedad, además del individuo que sufre la lesión causada por el delito.

Dentro de los individuos que intervienen en la preparación del delito, la comisión del mismo y el encubrimiento después de su perpetración, no forman parte del tema del delito, aunque sí muy íntimamente relacionados, ya que el delito será tipificado conforme a las

circunstancias en que sea cometido, las que influirán en el la sanción que le sea impuesta a los delincuentes.

Por último, el delito como figura principal en el Derecho Penal, es la que le da contenido a éste, pues es el objeto principal de su materia a estudio, con todas las características que el mismo envuelve.

CAPÍTULO II

Conceptos y antecedentes de Internet y de los delitos informáticos, su clasificación y características.

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Los llamados delitos informáticos, no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de esta.

Es indudable que la computadora se ha convertido en una herramienta indispensable para el desarrollo humano, pero es más sorprendente la rapidez con la que la supercarretera de la información (Internet), ha logrado cautivar a millones de adeptos a sus diferentes y diversos servicios. Gracias a toda esta tecnología computacional podemos hacer uso de estos servicios libremente con el sólo hecho de conectarnos a la Internet, por medio de una línea telefónica y un módem.

Lamentablemente la tecnología no se ha ocupado solamente para el beneficio del hombre, sino que algunos individuos sin escrúpulos han traspasado los límites de la seguridad y han realizado actos ilícitos, lo cual ha generado una gran preocupación por parte de los usuarios de este medio informático.

Pero existen muchos otros delitos que difícilmente podemos tipificar con las leyes actuales, y que estas rápidamente se tendrán que adaptar o redactar acorde a los nuevos tiempos que impone el uso de las tecnologías de la información.

¿Cómo no se va ha hablar constantemente de lagunas o de falta de regulación si las leyes no cambian ó se transforman con el desarrollo de la sociedad?

La insuficiencia de los instrumentos penales del presente para evitar y castigar las distintas formas de delitos informáticos supone un reto tanto a los estudiosos del derecho como a nuestros legisladores.

La dificultad de tipificar penalmente situaciones sometidas a un constante cambio tecnológico, la manifiesta insuficiencia de las sanciones en relación con la gravedad y el daño de los delitos informáticos y la propia inadecuación de los medios penales tradicionales para

remediar esta situación ha venido favoreciendo a que dichas conductas se realicen más usualmente sin ser castigadas.

2.1. Conceptos y antecedentes de Internet

Para adentrarnos al estudio de los llamados Delitos Informáticos, o en sus diferentes denominaciones como delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora o delincuencia relacionada con el ordenador, etc., entraremos al conocimiento y manejo de lo que es la computadora en nivel operacional y de estructuración, (ya que ésta como se verá más adelante puede ser objeto o fin de dichos delitos), así como la noción de diferentes conceptos relacionados con la computadora y el Internet, esto es para poder tener un mejor manejo del tema.

Ahora bien, el concepto y noción 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.[70]

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.[71]

La noción 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.

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. Mario G. Losano, caracteriza a la informática como un producto de la cibernética, en tanto un proceso científico relacionado con el tratamiento automatizado de la información en un plano interdisciplinario.[72] La definición que podemos dar del Internet, es que

[70] *Diccionario de la Real Academia Española*, p. 459.
[71] En http://www.freebsd.org/es/copyright/freebsd-license.html [consultado el 6 de junio de 2006]
[72] José Luis Mora, Enzo Molina, *Introducción a La Informática*, 1974, p. 52.

este no es un cuerpo físico o tangible, sino una red gigante que interconecta una innumerable cantidad de redes locales de computadoras. Es la red de redes.[73]

En términos generales, Internet se ha convertido en un polémico escenario de contrastes en donde todo es posible: desde encontrar información de contenido invaluable, de alcances insospechados en el ámbito de la cultura, la ciencia y el desarrollo personal, hasta caer en el terreno del engaño, la estafa o la corrupción de menores.

Se calcula que Internet enlaza hoy día a más de 60 millones[74] de computadoras personales en un extenso tejido electrónico mundial, lo cual hace necesario entenderla como un fenómeno social, dado el crecimiento exponencial que ha mostrado.[75]

Así pues, se habla constantemente de los beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual, más sin embargo, también dicho avance nos muestra otra cara de la moneda, siendo ésta, las conductas delictivas, pues se abrió la puerta a conductas antisociales que se manifiestan en formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas para infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

El inicio del Internet, se remonta a 1969, cuando la Agencia de Proyectos de Investigación Avanzada en Estados Unidos, (conocida por sus siglas "ARPA"), desarrolló ARPANET, una especie de red que unía redes de cómputo del ejército y de laboratorios universitarios que hacían investigaciones sobre la defensa.[76] Esta red, permitió primero a los investigadores de Estados Unidos acceder y usar directamente súper computadoras localizadas en algunas universidades y laboratorios clave; después, compartir archivos y enviar correspondencia electrónica. A finales de 1970 se crearon redes cooperativas descentralizadas, como UUCP, una red de comunicación mundial basada en UNIX y USENET (red de usuarios), la cual daba servicio a la comunidad universitaria y más adelante a algunas organizaciones comerciales.[77]

---

[73] También podemos considerar que Internet es un sistema internacional de intercambio de información que une a personas, instituciones, compañías y gobiernos alrededor del mundo, de manera casi instantánea, a través del cual es posible comunicarse, con un solo individuo, con un grupo amplio de personas interesadas en un tema específico o con el mundo en general.

[74] En http://es.gnu.org/Licencias/gples.html [consultado el 16 de agosto de 2006]

[75] Entendiendo al Internet como la red de redes, donde como se mencionó, entrelaza a más de 60 millones de computadoras personales a nivel mundial, (sin tomar en cuenta la cantidad de personas que puedan conectarse a la red de redes sin tener una computadora personalizada), nos da una idea del desarrollo tan amplio que ha tenido en las últimas décadas.

[76] Víctor Flores Olea, *Internet y la Revolución Cibernética*, México, Ed. Océano de México, 1997, p. 23.

[77] Denis Mc Quail, *Introducción a la Teoría de Comunicación de Masas*, Barcelona, Paidos Comunicación, 1983, p. 56.

En 1980, las redes más coordinadas, como CSNET (red de ciencias de cómputo), y BITNET, empezaron a proporcionar redes de alcance nacional, a las comunidades 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 macrocentros 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 centro 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, cediendo su lugar a INTERNET.[78] 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 reenrutar datos si una o más uniones individuales se dañan o están por alguna razón inaccesibles.[79]

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 reenrutado 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.[80]

El espíritu de la información que se maneja en Internet es que sea pública, libre y accesible a quien tenga la oportunidad de entrar a la red, lo cual marca un principio universalmente aceptado por los usuarios y que a dado lugar a una normativa sin fronteras y de lo cual podemos deducir, en términos jurídicos, cual sería la *ratio iuris,* o razón de ser de esta especial normatividad. Se intenta que Internet, sea, un medio interactivo viable para la libre expresión, la educación y el comercio. No existe institución académica, comercial, social o gubernamental que pueda administrarla. Son cientos de miles de operadores y redes de cómputo, que de manera independiente, deciden usar los protocolos de transferencia y recepción de datos

[78] Víctor Flores Olea, *op. cit*., pp. 44-60.
[79] 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.
[80] 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.

para intercambiar comunicaciones, información. No existe un lugar que concentre o centralice la información de Internet. Sería técnicamente imposible.

Los individuos tienen una amplia gama de formas de introducirse al Internet, a través de los proveedores de acceso a Internet.[81] En términos de acceso físico, se puede usar una computadora personal, conectada directamente (por cable coaxial o de fibra óptica) a una red, (un proveedor de servicios de Internet por ejemplo), que a su vez, se conecta a Internet; o puede usarse una computadora personal con un módem conectado a una línea telefónica a fin de enlazarse a través de ésta a una computadora más grande o a una red, que esté directa o indirectamente conectada a Internet.

Ambas formas de conexión son accesibles a las personas en una amplia variedad de Instituciones académicas, gubernamentales o comerciales. Lo cierto es que hoy en día el acceso a la red de Internet es cada vez más sencillo en Universidades, bibliotecas y cibercafeterias, lo cual está estrechamente relacionado con el número de proveedores de servicios de Internet.

2.2. Conceptos de delitos informáticos, características y clasificación.

Como se señaló, es indispensable el uso de la computadora y del manejo del Internet, para la comisión de conductas delictivas denominadas "Delitos Informáticos", sin embargo, aún en la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe una concepto propio de los llamados delitos informáticos. Aún cuando no existe dicha definición con carácter universal, se han formulado conceptos funcionales atendiendo a las realidades concretas de cada país.

Por lo que se refiere a nuestro país, cabe destacar lo mencionado por Julio Téllez Valdés, al decir 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,[82] lo cual en México, al igual que en otros muchos no ha sido objeto de tipificación aún.

Mencionando algunas de las diferentes definiciones que nos aportan estudiosos en la materia, sobre los Delitos Informáticos, diremos que para Lidia Callegari, el delito informático es

[81] Conocidos en el medio de las telecomunicaciones como ISP (Internet Service Provider).
[82] Julio Téllez Valdés, *op. cit.*, p. 53.

"aquel que se da con la ayuda de la informática o de técnicas anexas."[83] Rafael Fernández Calvo, define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos."[84] 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."[85]

Ahora bien, el Dr. Téllez Valdés, menciona dos clasificaciones del Delito Informático para efectos de conceptualización, donde parte de lo típico y lo atípico, de esta manera, 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."[86] En el concepto atípico menciona que "son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin."[87]

El Departamento de Ciencias de la Computación de la Universidad Nacional Autónoma 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."[88]

Así pues, y realizando una definición propia sobre los delitos informáticos, se entenderá por éstos como: *" 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".*

En forma general, dentro de las principales características que revisten los Delitos informáticos tenemos que:

a) Son conductas criminales de cuello blanco.

b) Son acciones ocupacionales, (en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando), y acciones de oportunidad, (en cuanto a que se

[83] Lidia Callegari, *Delitos Informáticos y Legislación* en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana, Medellín, Colombia, No. 70 Julio-Agosto-Septiembre, 1985, p. 47.
[84] Rafael Fernández Calvo, *El tratamiento de llamado "delito informático" en el proyecto de lo Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática),* en Informática y Derecho. p. 86.
[85] María Lima de la Luz, *Delitos Electrónicos*, en Criminalia, México, Academia Mexicana de Ciencias Penales, Porrúa, No. 1-6. Año L. Enero-Junio 1984, p. 26.
[86] Julio Téllez Valdéz, *op. cit*., p. 59.
[87] *Ídem*
[88] En http://www.turing.iimas.unam.mx [consultado el 4 de febrero de 2007]

aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico).

c) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse, además de que son muchos los casos y pocas las denuncias, debido a la misma falta de regulación por parte del Derecho.

d) Son muy sofisticados y relativamente frecuentes en el ámbito militar, asimismo, presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

e) En su mayoría son imprudenciales y no necesariamente se cometen con intención, al mismo tiempo que ofrecen facilidades para su comisión a los menores de edad, por lo que tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

f) Por el momento siguen siendo ilícitos e 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 en la presente investigación se pretende, crear una conciencia sobre la necesidad urgente de regular estas conductas dentro del ciberespacio, 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.

Después de ubicar las características que tienen el tipo de delitos informáticos así como sus sujetos y víctimas, se entrará al estudio de su clasificación.

La mayoría de los estudiosos en la materia clasifican a este tipo de acciones de dos formas, como instrumento o medio y como fin u objeto. Julio Téllez Valdés, clasifica a los delitos informáticos, en dos vertientes principales:

1.- Como Instrumento o medio: en donde dichas conductas criminógenas se valen de las computadoras como método, medio o símbolo en la comisión del ilícito,[89] y;

2.- Como Fin y Objeto: En esta categoría se enmarcan las conductas delictivas que van dirigidas en contra de la computadora, accesorios o programas como entidad física, los cuales pueden ser la programación de instrucciones que producen un bloqueo total al sistema, la destrucción de programas por cualquier método, el daño a la memoria, o el atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).[90]

Por su parte María de la Luz Lima, en su trabajo sobre Delitos Electrónicos, los clasifica en tres categorías, a saber:

1.- Los que utilizan la tecnología electrónica como método;

2.- Los que utilizan la tecnología electrónica como medio y;

3.- Los que utilizan la tecnología electrónica como fin.

En donde como método, los individuos utilizan procedimientos electrónicos para llegar a un resultado ilícito, como medio, son aquellas conductas criminógenas en donde para realizar un delito, utilizan una computadora como medio o símbolo y como fin, son las dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.[91]

Si bien existen en la actualidad distintas modalidades delictivas relacionadas con la informática, se pueden clasificar principalmente en dos tipos:

- **Delitos Computacionales:** entendiéndose como conductas criminales tradicionales, en donde se utiliza a los medios informáticos como medio de comisión.[92]
- **Delitos Informáticos:** son aquellas conductas delictivas en las que se ataca bienes informáticos en si mismos, no como medio, sino como fin.[93]

---

[89] Por ejemplo, la falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera), la variación de los activos y pasivos en la situación contable de las empresas, la planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera), la lectura, sustracción o copiado de información confidencial, el aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas, la alteración en el funcionamiento de los sistemas (virus informáticos) y el acceso a áreas informatizadas en forma no autorizadas entre muchas más

[90] Julio Téllez Valdéz, *op. cit.*, p. 63.

[91] María Lima de la Luz, *op. cit.*, p. 33.

[92] Por ejemplo: realizar una estafa, robo o hurto, por medio de la utilización de una computadora conectada a una red bancaria, ya que en estos casos se tutela los bienes jurídicos tradicionales como el patrimonio.

[93] Tal es el caso del daño en el Software por la intromisión de un virus, o accediendo sin autorización a una PC, o la piratería (copia ilegal) de software.

De esta manera, podemos decir ahora, que el verdadero concepto de **Delito Informático**, es el siguiente: ***"toda conducta que revista características delictivas, es decir sea típica, antijurídica y culpable, y que atente contra el soporte lógico o Software de un sistema de procesamiento de información, sea un programa o dato relevante."***[94]

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.[95]

Los crímenes por computadora comprenden cualquier comportamiento criminal en el cual la computadora ha estado involucrada como material o como objeto de la acción delictiva, o como mero símbolo.

Dado que es profusa la literatura sobre los denominados delitos informáticos, es necesario encarar desde el punto de vista criminológico, el estudio sobre la perpetración de conductas que, sucedidas o no a través de la red, pueden llegar a constituir ilícitos penales, de existir una legislación que así los contemple.

El continuo avance de la tecnología en el mundo globalizado está provocando un fenómeno de poder que desborda a los poderes políticos locales y no resulta fácil hallar soluciones a conflictos como éste en el que las acciones criminales trascienden tales límites.

Si tomamos las acciones que se producen en Internet como todas aquellas que vulneran la privacidad de determinados datos, y las conductas perjudiciales que se efectivizan utilizando el medio informático en general, vemos que su causa puede obedecer a factores:

- Sociales: ya que el nivel social al que pertenecen los sujetos que pueblan el mundo de la informática, por lo general es de medio a alto, por cuanto provienen de una extracción que

[94] Definición propia adoptada mediante la lectura de diferentes definiciones.
[95] Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora" ó "delincuencia relacionada con el ordenador".

les pudo proporcionar estas herramientas para alcanzar las metas que la cultura social les estaba proponiendo.[96]

- Económicos: La tendencia al agrupamiento o formación de "grupos económicos" en continua expansión y la globalización de la economía son factores que dieron plafón al crecimiento de la informática y paralelamente la aparición de Internet con las ventajas que ello les ofrecía, en una palabra el progreso tecnológico de las comunicaciones permitieron transacciones que, en segundos conllevaron a un mayor poder económico y político extranacional.[97]

Desde que surge el auge de la informática es notorio que todo aquél que desconoce el manejo de una computadora cae en la obsolencia y ya desde muy pequeños se les inculca a los niños sobre este tema que a su vez por las características técnicas que presenta requiere de ciertas condiciones de aptitud para encararlas y que facilitan la agilidad mental, de modo que va haciendo nacer en el sujeto el deseo de ser ese prototipo del ideal actual de la comunidad.

Es peligroso pensar que el estereotipo de quienes violan la seguridad de los sistemas computacionales son solo brillantes estudiantes o graduados en ciencias de la computación, sentados en sus laboratorios en un lugar remoto del mundo. A pesar de que tales sujetos existen, la mayoría de las violaciones a la seguridad son hechas desde dentro de las organizaciones.

Cualquiera que sea la motivación de las empresas que hacen esto, se pueden caracterizar en las siguientes categorías:

a) Personas dentro de una organización:

- Autorizados para ingresar al sistema (ejemplo: miembros legítimos de la empresa que acceden a cuentas corrientes o al departamento de personal).
- No están autorizados a ingresar al sistema (ejemplo: personal contratista, aseo, eventual, etc.)

b) Personas fuera de la organización:

- Autorizadas para ingresar al sistema (ejemplo: soporte técnico, soporte remoto de organizaciones de mantenimiento de software y equipos, etc.)

[96] Es importante mencionar que el acceso a esta tecnología no es propio de zonas marginales en las que, pese a los animosos esfuerzos gubernamentales de lograr llevar la computación (y el uso de Internet) hacia todos los rincones del país y del mundo, no es fácil aún encontrar a niños del Altiplano accediendo a ellos.

[97] María Luisa Fernández Esteban, *Nuevas tecnologías, Internet y derechos fundamentales*, Madrid, Editorial Mc Graw Hill, 1998, p. 69.

- No están autorizados para ingresar al sistema (ejemplo: usuarios de Internet o de acceso remoto, sin relación con la institución).[98]

Ahora bien, dentro de la clasificación de los delitos informáticos, obviamente existen sujetos involucrados en la comisión de estos delitos, los cuales se clasifican en dos grupos:

1. Sujetos Activos: 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 puede ocurrir que por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que la diferencia entre sí, es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiara que desvía fondos de las cuentas de sus clientes.

Sin embargo, teniendo en cuenta las características de las personas que cometen los delitos informáticos, doctrinarios en la materia los han catalogado como "delitos de cuello blanco", termino introducido por primera vez por Edwin Sutherland. Este penalista estadounidense dice que tanto la definición de los delitos informáticos como los denominados de cuello blanco, no es de acuerdo con el interés protegido, como sucede en los delitos convencionales, sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por poca inteligencia.

Existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad, ya que ésta no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, por el contrario, el autor de este tipo de delitos se considera a sí mismo "respetable". Otra coincidencia que tiene estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.[99]

2. Sujetos Pasivos: Tenemos que distinguir que sujeto pasivo ó 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, gobiernos, etc., que

[98] Un buen sistema para fiscalizar la seguridad informática debe considerar todas las categorías anteriormente señaladas. Estos riesgos se controlan con los denominados firewalls o paredes de fuegos, que se detallarán más adelante.
[99] Julio Téllez Valdéz, *op. cit.*, p. 83.

usan sistemas automatizados de información, generalmente conectados a otros. El sujeto pasivo del delito que nos ocupa, es sumamente importante, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, debido a que muchos de los delitos son descubiertos casualmente por el desconocimiento del modus operandi de los sujetos activos.

Debido a esto, ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables y si a esto se le suma la falta de leyes que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga oculta.

Por todo esto se reconoce que para conseguir una previsión efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

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

2.3. La Piratería Informática. Concepto y tipos.

Internet en apenas diez años, ha conseguido revolucionar aspectos diversos de las relaciones comerciales entre empresas y de estas con los consumidores, de la información y de la comunicación en línea, del acceso y el compartir del conocimiento y de los contenidos audiovisuales.[100] El desarrollo de Internet, como un nuevo medio de difusión masiva de contenidos se erige como una realidad incontestable, con todos los visos de seguir experimentando un crecimiento exponencial en los próximos años. Este crecimiento no se

[100] Dentro de estos se encuentra la publicidad audiovisual, también presente con gran fuerza en Internet, mediante los "baners", los patrocinios y los propios sitios "web", por solo citar algunas formas de difusión de la comunicación comercial en este medio interactivo.

encuentra exento de fuertes tensiones derivadas de las potencialidades que encierra el uso de la tecnología digital, y de las facilidades intrínsecas del sistema para acceder y transmitir datos de una máquina a otra, sin que las fronteras políticas supongan barrea efectiva para ello.

De esta manera, hoy en día, muchas empresas, organizaciones y personas en general, no son conscientes de que quizá estén usando software ilegal y que la distribución y uso ilegales de éste, constituyen un problema importante que afecta negativamente a los proveedores de estos programas; mucho menos se imaginan que están cometiendo un delito, conocido como piratería informática.

La piratería informática como delito consiste en la distribución y/o reproducción ilegales de software. Comprar software significa en realidad comprar una licencia para usar el software, y esta licencia especifica la forma legal de usar dicho software. Cualquier uso que se haga del software más allá de lo estipulado en la licencia constituye una violación de ésta y posiblemente, de las leyes que amparan los derechos de propiedad intelectual. La piratería informática es ilegal y sancionable según la ley, tanto si es deliberada como si no.[101]

Otro de los delitos que empieza a ser ya habitual en el uso ilegal de las nuevas tecnologías se basa en la presencia de manifestaciones ideológicas, normalmente de carácter político, en algunas de las páginas de Internet de organismos oficiales, partidos políticos o entidades institucionales.[102]

Lo cierto es que los delitos predominantes a través de las nuevas tecnologías de la información son aquellos que podemos considerar como los "tradicionales", que comprenderían toda la galería de estafas y "timos" que pueden llevarse a cabo electrónicamente. Así, las redes de la información son propicias para extender amplias innovaciones delictivas como el fraude a través de tarjetas de crédito, la intrusión en las redes de empresas y administraciones públicas, los virus informáticos, las falsas oportunidades de negocio, los engaños en vacaciones y viajes o la piratería de programas. Al mismo tiempo, aparecen nuevas formas de negocio que escapan de los cauces legales como la novedosa venta ilegal de medicamentos a través de Internet.

Así, la piratería informática adopta diversas formas que afectan tanto a los usuarios como a los prestadores del servicio, enfatizándose las siguientes:

[101] En http://mcAfee.com [consultado el 10 de febrero de 2007]

[102] Básicamente, este conjunto de delitos es llevado a cabo por activistas motivados por razones políticas y sociales que acaban constituyendo una nueva variedad de criminal cibernético.

- Informar de un número inferior al real de las instalaciones de software adquiridas mediante acuerdos de compra de gran volumen, hacer copias adicionales del software sin tener el número de licencias necesario para ello.[103]
- Usar software de licencia de suscripción más allá de la fecha de vencimiento.
- Dar acceso al software, generadores de claves, claves de activación, números de serie y similares que permitan instalar el software, mediante descarga, desde CD grabados o desde el soporte original
- Falsificación: cuando se intenta copiar el producto y su presentación de forma que parezca original.
- Carga en el disco duro: es el caso de ciertos proveedores que instalan software ilegalmente para vender mejor sus equipos. Si bien son muchos los proveedores autorizados a instalar productos en los equipos que venden, los proveedores justos suministran el software mediante acuerdos con los proveedores de dicho software.[104]

Debido a los problemas anteriormente citados, han surgido Organizaciones Internacionales en contra de la piratería informática, las cuales ofrecen información a los consumidores sobre la protección del software, propiedad intelectual, comercio electrónico y otros temas relacionados con Internet, destacándose las siguientes:

- Business Software Alliance (BSA): es la principal organización dedicada a promover un mundo digital seguro y legal. BSA es la voz del sector del software comercial mundial ante las administraciones y en el mercado internacional. Sus miembros representan el sector de crecimiento más rápido del mundo.[105]
- Canadian Alliance Against Software Theft (CAAST): Establecida en 1990, es una alianza sectorial de fabricantes de software que comparten el objetivo común de reducir la piratería informática.[106]
- La Federation Against Software Theft (FAST): fue establecida en 1984 por el British Computer Society's Copyright Committee.[107] Fue la primera organización para los derechos de propiedad intelectual. La primera medida que adoptó fue aumentar la sensibilización hacia la piratería informática y presionar al Parlamento para que

[103] Por ejemplo, se dispone de 1 copia con licencia, pero se hacen cinco copias adicionales, ó instalar el software en un servidor al que todo el personal tiene acceso ilimitado (sin mecanismos de bloqueo, contadores, etc.)
[104] En http://mcAfee.com [consultado el 22 de febrero de 2007]
[105] En http://www.bsa.org [consultado el 22 de febrero de 2007]
[106] En http://www.caast.org [consultado el 22 de febrero de 2007]
[107] Comité de derechos de propiedad intelectual de la sociedad británica de informática.

introdujera cambios en la Ley de propiedad intelectual de 1956 que reflejaran las necesidades de los autores y editores de software. Esta campaña tuvo éxito y desde entonces ha podido influir en otras leyes que afectan a la protección adecuada del software.[108]

- La Software & Information Industry Association (SIIA): Los trabajos de esta asociación han reunido a las principales compañías del sector del software y la información, ampliando las oportunidades de mercado y abriendo camino a un sector más fuerte. SIIA protege la propiedad intelectual de sus miembros y aboga por un entorno legal y normativo que beneficie a todo el sector.[109]

Si bien estas organizaciones luchan por un entorno donde el marco legal sea benéfico para todos, con el uso cada vez más amplio de Internet, la piratería informática se simplificó, ya que, los programas fueron puestos a disposición del público en la misma red.

Resulta obvio pues, que la piratería informática no se realiza por sí misma, sino por determinados grupos de personas, las cuales, tienen una "distinción" por los grados de conocimiento y la esfera de su actuar. Así nos encontramos con los Hackers, los Crackers y los Phreakers, quienes son los tres grupos originarios de los que se subdividen otros tantos. A continuación distinguiré cada uno de ellos.

- Hacker: Es una persona muy interesada en el funcionamiento de sistemas operativos; aquel curioso que simplemente le gusta husmear por todas partes, llegar a conocer el funcionamiento de cualquier sistema informático mejor que quiénes lo inventaron. La palabra es un término inglés que caracteriza al delincuente silencioso o tecnológico. Ellos son capaces de crear sus propios softwares para entrar a los sistemas. Toma su actividad como un reto intelectual, no pretende producir daños e incluso se apoya en un código ético.[110] Estos suelen ser verdaderos expertos en el uso de las computadoras y por lo general rechazan hacer un uso delictivo de sus conocimientos, aunque no tienen reparo en intentar acceder a cualquier máquina conectada a la red, o incluso penetrar a una Intranet privada, siempre con el declarado fin de investigar las defensas de estos sistemas, sus lados débiles y "anotarse" el mérito de haber logrado burlar a sus administradores.

[108] En http://www.fast.org.uk [consultado el 22 de febrero de 2007]
[109] En http://www.siia.net [consultado el 22 de febrero de 2007]
[110] Dentro de su "código ético" se destaca: El acceso a los ordenadores y a cualquier cosa le puede enseñar como funciona el mundo, debería ser limitado y total. Toda la información deberá ser libre y gratuita. Desconfía de la autoridad. Promueve la descentralización. Los Hackers deberán ser juzgados por sus hacks, no por criterios sin sentido como calificaciones académicas, edad, raza, o posición social. Se puede crear arte y belleza en un ordenador. Los ordenadores pueden mejorar tu vida.

Muchos de ellos dan a conocer a sus víctimas los "huecos" encontrados en la seguridad e incluso sugieren cómo corregirlos, otros llegan a publicar sus hallazgos en revistas o páginas Web.

- Cracker: son llamadas así, las personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas. Tiene dos variantes: a) El que penetra en un sistema informático y roba información o se produce destrozos en el mismo y b) 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 anti-copia. Esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.[111] Como su nombre indica se dedican a romper, por supuesto las protecciones y otros elementos de seguridad de los programas comerciales, en su mayoría con el fin confeso de sacar provecho de los mismos del mercado negro. Estos crean códigos para utilizarlos en la copia de archivos. Sus acciones pueden ir desde la destrucción de información ya sea a través de virus u otros medios, hasta el robo de datos y venta de ellos.[112]
- Phreaker: Es el especialista en conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles.[113] Estos buscan burlar la protección de las redes públicas y corporativas de telefonía, con el declarado fin de poner a prueba conocimientos y habilidades, pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas

[111] En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado más adelante.

[112] Ejemplo de su actuar ilegal son los millones de CDs con software pirata que circulan por el mundo entero y de hecho, muchas personas no llegan a sospechar que parte del software que tienen en sus máquinas, incluso con certificados de garantía de procedencia, es craqueado. Esto sucede sobre todo en los países del tercer mundo; se agrupan en pequeñas compañías y contratan especialistas de alto nivel. Claro que la prensa, e incluso autoridades del mundo entero, diferencian al estudiante sin recursos que "craquea" un programa para su uso, de los que hacen de ello un negocio, aunque insisten que nadie debe actuar así. Lo cierto es que la principal condición para que florezca el negocio del cracking es el precio, siempre en ascenso y en algunos casos exorbitantes, de los programas de mayor utilidad en contraposición con el del hardware que ha mantenido una tendencia decreciente, por lo que no es de extrañar que con frecuencia el costo del software que soporta una máquina, aun una de última generación, sea superior al de ésta.

[113] En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.

telefónicas,[114] cuyos códigos obtienen al lograr el acceso mediante técnicas de "Hacking" a sus servidores. Dentro de las actuales manifestaciones de phreaking podríamos distinguir: a) Shoulder-surfing: esta conducta se realiza por el agente mediante la observación del código secreto de acceso telefónico que pertenece a su potencial víctima, el cual lo obtiene al momento en que ella lo utiliza, sin que la víctima pueda percatarse de que está siendo observada por este sujeto quien, posteriormente, aprovechará esa información para beneficiarse con el uso del servicio telefónico ajeno. b) Call-sell operations: el accionar del sujeto activo consiste en presentar un código identificador de usuario que no le pertenece y carga el costo de la llamada a la cuenta de la víctima.[115] c) Diverting: consiste en la penetración ilícita a centrales telefónicas privadas, utilizando éstas para la realización de llamadas de larga distancia que se cargan posteriormente al dueño de la central a la que se ingresó clandestinamente. d) Acceso no autorizado a sistemas de correos de voz: el agente ataca por esta vía las máquinas destinadas a realizar el almacenamiento de mensajes telefónicos destinados al conocimiento exclusivo de los usuarios suscriptores del servicio.[116] e) Monitoreo pasivo: por medio de esta conducta el agente intercepta ondas radiales para tener acceso a información transmitida por las frecuencias utilizadas por los teléfonos inalámbricos y los celulares.

La gran mayoría de los delincuentes informáticos,[117] utilizan las mismas técnicas para realizar conductas criminales, es decir, copian herramientas que desarrollaron otros. Actualmente,

[114] En nuestros días se preocupan más de las tarjetas prepago, ya que suelen operar desde cabinas telefónicas o móviles. Un sistema de retos, es capaz de captar los números de abonado en el aire. De esta forma es posible crear clones de tarjetas telefónicas a distancia.

[115] Esta acción aprovecha la especial vulnerabilidad de los teléfonos celulares y principalmente ha sido aprovechada a nivel internacional por los traficantes de drogas.

[116] A través de esta conducta el sujeto activo puede perseguir principalmente dos objetivos: 1) Utilizar los códigos de transferencia de mensajería automática manejados por el sistema y 2) Lograr el conocimiento ilícito de la información recibida y grabada por el sistema.

[117] Además de los hackers, Crackers y phreakers, también se desarrollan (junto con los avances de la tecnología y la informática), nuevos delincuentes y técnicas que, por su nula experiencia o práctica son poco conocidos, a saber: Lammers: Aquellos que aprovechan el conocimiento adquirido y publicado por los expertos. Gurus: Son los maestros y enseñan a los futuros Hackers. Normalmente se trata se personas adultas, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma para enseñar o sacar de cualquier duda al joven iniciativo al tema. Bucaneros: En realidad se trata de comerciantes. Los bucaneros venden los productos crackeados como tarjetas de control de acceso de canales de pago. Newbie: Traducción literal de novato. Es alguien que empieza a partir de una WEB basada en Hacking. Inicialmente es un novato, no hace nada y aprende lentamente. Trashing: Esta conducta tiene la particularidad de haber sido considerada recientemente en relación con los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas. Estas actividades pueden tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada.

existen alrededor de 60 mil páginas que explican con todo detalle muchos de los trucos para piratear. Sólo basta con bajar un programa y comenzar a bombardear un sitio para lograr las primeras experiencias. Incluso, hay algunas páginas que ofrecen laboratorios de virus, donde la persona puede crearlos a su medida, siguiendo instrucciones básicas. Además por medio de estos programas van aprendiendo a desarrollar sus propias herramientas.

Estos sujetos especiales por su modo de actuar y los medios que utilizan para ello, trascienden por su relevancia en la historia de la humanidad y más aun en la historia del derecho. Realmente su presencia en la comisión de un hecho delictivo es sumamente importante pues, en una gran mayoría, son individuos que comienzan a forjarse dentro del mundo de las acciones antijurídicas y por otra parte, son los responsables directos de mantener en pie la falta de acciones jurídicas dentro de este mundo, que lucha por el pleno y total desarrollo de los sistemas computarizados, y entre estos últimos están inmiscuidos tanto los que llevan a cabo la acción como aquellos que se niegan a denunciar las acciones negativas que han sido realizadas en su contra.

2.4. El derecho en la regulación. Principales teorías.

Internet está constituido por una comunidad heterogénea e invisible que no está unida bajo los tradicionales cánones de territorio, política, religión, población, lengua, etc. Por ello ha sido extremadamente complejo establecer la forma idónea de regular ciertas conductas que son una realidad dentro de las relaciones de comerciales y humanas facilitadas por este medio de comunicación, y que algunas veces podrías hasta constituir una vulneración real a los derechos humanos. Tal es el caso de la pornografía infantil, la violación de la intimidad en el tratamiento de datos personales, el fomento del terrorismo y la violación de las comunicaciones personales, entre otras irregularidades. Con el nuevo ámbito de aplicación que han adquirido los derechos en Internet, y vistas las propuestas desde las cuales puede existir una jurisdicción en la red, es necesario indicar que en la doctrina ya se empiezan a esgrimir las teorías en torno al alcances que debe tener el derecho una vez determinada la jurisdicción a la que le compete aplicar ese derecho. Así, las teorías doctrinales en cuanto al presente tema, son las siguientes:

2.4.1. Teorías conservadoras

Quienes esgrimen esta teoría consideran que el derecho actual es completamente aplicable a la era digital y por ende no se requieren nuevas interpretaciones sobre nuevos derechos, sino concreciones en el ámbito digital con respecto a derechos ya existentes. Se trata por tanto no sólo de aplicar los derechos tradicionales en el ámbito informático, sino de ampliarlos y reformarlos.

"Las posturas más radicales tienden a diabolizar (sic) la era informática como una amenaza a todo derecho que ostente la persona desde el derecho de autor hasta el derecho a la intimidad y la libertad humana. Dentro de esta postura, encontramos a grupos que abogan principalmente por un interés económico potencial ante la expansión del derecho en todos los ámbitos de la Red que tienden a proponer mecanismos de control excesivos para el usuario, prohibiciones explícitas o servicios prepago."[118]

Aquí se ve al Internet como una forma más de comercio por la cual se debe establecer un mecanismo normal de mercado en donde se ofrezca un producto a un precio determinado y con las ventajas del formato digital y el usuario accede a dicho bien, compensando el servicio que recibe o más bien que adquiere o compra, en un mundo virtual que se rige por la competencia.

Las posturas conservadoras moderadas si bien respaldan las fuerzas propias del mercado, propio de los neoclásicos, también defienden como punto de equilibrio la intermediación de las entidades de gestión colectiva de derechos o entidades de control privado que puedan ponderar el derecho de los usuarios de Internet por cuanto reconocen la necesidad de imponer límites y controles justo a la autonomía de la voluntad de las partes.

2.4.2. Teorías liberales (minimalistas, pro-informáticas, de autorregulación o doctrina del Fair Use)

Las posturas liberales consideran que cualquier imposición o aplicación de las normas tradicionales del derecho en el ámbito de Internet, implica un menoscabo en la libertad informática entendida como un derecho de los usuarios a la libre circulación y acceso en la Red.[119]

[118]Alejandra Castro Bonilla. "La regulación de Internet un reto jurídico", en http://www.uned.ac.cr/redti/documentos/regulacion.pdf

[119]Ignacio Garrote las denomina como teorías neoclásicas, minimalistas y eclécticas, para lo cual recomiendo la consulta de su obra: Ignacio Garrote Fernández-Díez. "El Derecho de Autor en Internet. La directiva sobre derechos de autor y derechos afines en la sociedad de la información". Editorial Comares, Granada, 2001, p.67 y ss.

Consideran que la regulación jurídica pertenece al mundo analógico pero no al mundo digital, por cuanto en Internet impera el derecho e interés del usuario. Sostienen que si las normas tradicionales se aplican en Internet, se restringe tanto el acceso a obras literarias, artísticas o científicas, como la limitación real de derechos como el de acceso a la cultura, a la educación y al derecho a la libertad de información, además se obstaculizarían transacciones comerciales y el libre flujo de datos que impidan monopolizar el conocimiento.

Consideran que el derecho no puede adaptarse a la dinámica de Internet por cuanto no pueden existir controles sobre el uso, destino y comunicación de las comunicaciones, ni imponer responsabilidades que son imposibles de identificar en el ciberespacio.

Por ello, dentro de estas teorías se ubican los que defienden la autorregulación de la Red,[120] que explica Asensio de la siguiente forma: "En efecto, con base también en la pretendida incapacidad (e incluso falta de legitimación) de los ordenamientos jurídicos estatales (de base territorial) para regular y controlar los flujos transfronterizos de información por Internet y para dar respuesta a los conflictos de intereses planteados en la Red, que produciría situaciones hasta ahora desconocidas (en particular, como consecuencia del carácter digital e inmaterial del nuevo contexto), se ha propuesto un modelo de reglamentación descentralizado, basado en la creación al margen de los legisladores estatales de normas propias para regular Internet y sus relaciones, en gran medida por parte de los actores de la Red. Se ha llegado a proponer la consideración del ciberespacio como una jurisdicción independiente, diferenciada de las estatales, con mecanismos propios de producción de normas y órganos específicos de solución de controversias."[121]

Los liberales señalan que aplicar los principios del derecho analógico a Internet, afectaría sobre todo a países en vías de desarrollo a quienes se les coartaría el acceso a bibliotecas virtuales, centros de archivo y documentación y demás recursos culturales, informativos y artísticos en línea; a los cuales no pueden acceder desde su situación geográfica tradicional. Internet, para ellos, se hizo para romper fronteras, por lo que el derecho no puede venir a imponerlas nuevamente, pues se estaría legitimando un retroceso en los beneficios que trajo el desarrollo tecnológico de la era digital.

Dentro del grupo de minimalistas moderados, se incluyen quienes abogan por la doctrina del *Fair Use*, propia del sistema de Copyright. La doctrina del *Fair Use*, que se asemeja de manera muy elocuente a la naturaleza de las limitaciones al derecho de autor, puede ser un

[120] Recordemos que en la actualidad existen organismos-Internet que poseen autoridad sobre el ciberespacio sin estar adscritos aun órgano político geográfico, tales como el ICANN, ISOC, IRTF, etc.
[121] Pedro de Miguel Asensio, *Derecho privado de Internet*, Madrid, Editorial Civitas, 2ª Edición, 2001, pp.75-76.

mecanismo eficaz para lograr que el ciudadano tenga un acceso real a la educación y a la cultura, en ejercicio de los derechos constitucionales que lo amparan.

En la declaración de la asociación de bibliotecas con respecto a la propiedad intelectual, denominada "Fair Use in the Electronic Age: Serving the Public Interest", se discutió que la doctrina del Fair Use en concordancia con la ley The Copyright Act estadounidense y la DMCA, permiten la reproducción y otras disposiciones de los trabajos protegidos por el derecho de autor bajo ciertas condiciones de uso con propósitos críticos, de comentario, noticiosos, educativos (incluyendo múltiples copias para el uso en clase), escolares o de investigación.[122]

El Fair Use también permite ciertos usos abiertos realizados por agentes participantes de la educación superior y por las bibliotecas, lo que asegura la libre circulación de la información y el desarrollo de una estructura informativa de interés público.[123]

2.4.3. Teorías moderadas o eclécticas

Quienes esgrimen la teoría moderada, abogan por buscar un equilibrio entre el interés de los titulares de los derechos que circulan en la red, los usuarios, los proveedores de servicios de Internet y los proveedores de contenido. Para ello, reconocen la necesidad de adaptar el derecho a las exigencias de las TIC,[124] con el fin de lograr esa armonización de intereses de todas las partes.

Se trata de crear un nuevo derecho aplicable a las TC[125] que permita un equilibrio de intereses entre las partes para armonizar su situación de protección y minimizar el riesgo sobre sus derechos. Estas teorías, sin embargo, deben partir de una definición previa del poder que rige en la

[122] Working Document 1/18/95, en http://arl.cni.org/scomm/copyright/uses.html

[123] Para muchos autores, el Fair Use es la doctrina que establece el balance entre los derechos de la propiedad intelectual y los derechos de la sociedad. Los usos libres que permiten incluyen desde la crítica, la investigación, la educación, enseñanza, comentarios, reportajes periodísticos y uso privado para esos mismos fines.

[124] TIC es el acrónimo de Tecnologías de la Información y la Comunicación. Sin embargo, no existe una definición precisa y uniforme del término. Por ejemplo, fue definido por el PNUD (2002) en el Informe sobre Desarrollo Humano en Venezuela del siguiente modo: ·Las TIC se conciben como el universo de dos conjuntos, representados por las tradicionales Tecnologías de la Comunicación (TC), constituidas principalmente por la radio, la televisión y la telefonía convencional y por las Tecnologías de la Información (TI) caracterizadas por la digitalización de las tecnologías de registros de contenidos (informática, de las comunicaciones, telemática y de las interfases). Según el Portal de la Sociedad de la Información de Telefónica de España: Las TIC (Tecnologías de la Información y Comunicaciones) son las tecnologías que se necesitan para la gestión y transformación de la información, y muy en particular el uso de ordenadores y programas que permiten crear, modificar, almacenar, proteger y recuperar esa información. Así, se trataría de un concepto difuso que agruparía al conjunto de tecnologías ligada a las comunicaciones, la informática y los medios de comunicación y al aspecto social de éstas.

[125] Tecnologías de la Comunicación (TC), constituidas principalmente por la radio, la televisión y la telefonía convencional.

Red, pues toda aplicación jurídica, dependerá de la jurisdicción que se decida imponer en la misma.

En este sentido, consideran que el sujeto pasivo de Internet no puede ser considerado siempre bajo el sentido iusprivatista de un "consumidor", pues no se trata de un mercado económico sino de un campus virtual que define a un sujeto que ostenta por lo general un interés no lucrativo sobre la información a la que tiene posibilidad de acceder. Considerar al usuario como un consumidor, sería equiparar su condición a las consideraciones que harían los defensores de la naturaleza de Internet como un mercado global, no como una instancia de comunicación universal que por ende facilita el acceso a bienes culturales, artísticos, científicos, educativos y que conllevan implícito un fin social que en principio debería ser gratuito.

2.4.4. La Autorregulación

La autorregulación está justificada por sus defensores como la alternativa ante la sociedad virtual entendida como una sociedad sin fronteras, que por ende no necesita de límites jurídicos pues tampoco los tiene territoriales. La justificación territorial es válida en tanto un Estado no puede efectivamente imponer sus reglas sobre una actividad de la que se sirve la comunidad internacional, porque quebrantaría los principios de la soberanía del resto de las naciones y del principio de jurisdicción; aunque no han faltado iniciativas autónomas en este sentido.

La justificación de fondo la esgrimen quienes abogan por la protección de los intereses comerciales de Internet, por cuanto entienden la autorregulación como las reglas del mercado, por ende libres y basadas en la competencia. En este sentido, la autorregulación se manifiesta a través de dos tendencias:

2.4.4.1. Por organismos privados

Es la que aboga por imponer medidas de recomendación a partir de organizaciones privadas conformadas por cualquier prestador o grupo de prestadores de servicios o bien individuos (usuarios de Internet) que estén interesados en aportar recomendaciones vinculantes que se estudian por parte de miembros de la comunidad de Internet hasta que se logre una intersubjetividad que permita la difusión de tales medidas para su implantación.

Consiste en una jurisdicción no localizable geográficamente y ajena a la intervención de cualquier Estado o comunidades regionales de orden público, por lo que se trata de organizaciones privadas y descentralizadas con sus propios mecanismos de organización, recomendaciones, medidas y soluciones de conflictos.[126] Es claro que la autorregulación auspiciada por esas instancias no es una actividad en la que participen todos los agentes interesados y ni siquiera los que elaboran las recomendaciones poseen algún tipo de legitimación o representación democrática.[127] Esta propuesta, pese a su apoyo a favor de la libertad del mercado, aboga por un tratamiento civilista de las actividades de Internet, por cuanto proponen la suscripción de contratos entre proveedores y usuarios, con el fin de salvaguardar los intereses de las partes y evitar conductas ilícitas. Con ello, se procuraría evitar la anarquía absoluta de las relaciones en la Red.

2.4.4.2. La Teoría del caos

Es la que aboga por eliminar incluso las regulaciones de la comunidad de Internet, para dejar plena libertad a los agentes que intervienen día a día en este nuevo mercado. Esta postura, por su radicalidad, consistiría en respaldar una anarquía de Internet que reivindica el caos.

La total libertad en el funcionamiento de la Red no se ha llevado aún a la práctica, aunque existen varios defensores de ella.[128] Se trata de eliminar incluso las reglas de acceso que imponen servidores privados y evitar la adopción de medidas de control privado o público, haciendo de Internet un espacio donde reine la anarquía y se permita todo, incluso la pornografía infantil, el tratamiento invisible de datos y otra serie de faltas que, desafortunadamente también han aumentado con la tecnología en las comunicaciones.

Esta postura se conoce como la *teoría del caos*, por valorar la desorganización como forma de desarrollo tecnológico.[129]

---

[126] Se trata de organismos como el ISOC, el ICANN o el IANA con un origen comercial y generalmente con una importante incidencia estadounidense.

[127] Algunas instancias incluso están financiadas por intereses particulares de grandes empresas con actividades monopolísticas en el mercado de la informática (productores de software o hardware) que hacen dudar de la objetividad de las soluciones que derivan de tales órganos.

[128] La Electronic Frontier Foundation ha defendido reiteradamente la autorregulación del libre mercado en Internet.

[129] George Orwell en su novela *1984*, presentaba las consecuencias de una sociedad bajo el imperio del mercado tecnológico, bajo una perspectiva coincidente con la Teoría del Caos, obra de referencia continua para quienes se han abocado al análisis de este tema. En su obra Orwell daba una visión pesimista del futuro de la humanidad en donde la guerra es la paz, la libertad es la esclavitud y la ignorancia es la fuerza. En conclusión, resume los peligros de la convivencia en libertad sin límites donde la única dirección es el desarrollo tecnológico sin reglas humanas que sirvan de intermediarios mínimos para el respeto de los derechos humanos.

Por lo anterior, dentro de las propuestas de autorregulación la primera tendencia (autorregulación por organismos privados) es la que mejor se perfila dentro de sus defensores, e incluso se han llegado a implementar ciertas proposiciones derivadas de ella, como las condiciones de acceso que ofrecen proveedores de servicios en Internet.

"El uso de directrices que imponen los proveedores de acceso y otras entidades es creciente. Numerosas universidades han establecido sus propias normas respecto a la publicación en la WWW. También es cada vez más común que los proveedores de acceso establezcan sectores de servicio claramente identificables y que los que hayan suscrito el servicio e incumplan estas normas puedan ver cancelado su acceso. La adopción de directrices por proveedores de acceso y otras regulaciones privadas son auspiciadas desde las instituciones comunitarias como un método más eficaz que la regulación estatal para controlar la información."[130]

La autorregulación, como se estipula en su primera versión, necesita y de hecho se sirve de ciertas reglas denominadas códigos de conducta,[131] en virtud de los cuales es posible llevar relaciones de intercambio de bienes y servicios de forma armónica, aunque no sean homogéneas en la Red. Básicamente están referidas a la protección de los derechos humanos y las libertades públicas, la libertad de mercado bajo el respeto de la libre competencia, la conformación de centros de información virtual y una garantía de publicidad de tales reglas.

2.4.5. El Estado Universal

Esta propuesta de regulación de Internet consiste en la conformación de un Estado Universal como un ente único compuesto por instancias públicas, internacionales, locales y privadas que adquiere cualidad estatal en virtud de sus competencias universales. Esta propuesta contiene dos soportes teóricos importantes:

2.4.5.1. El Estado Cosmopolita

Habermas propone este Estado a partir de una asociación de naciones defendida inicialmente por Kant, pero superándola, pues el Estado Kantiano o Asociación de Naciones, no está pensado

[130] María Luisa Fernández Esteban, *op. cit*., p. 102.
[131] Como las Request for Comments o las Netiquette.

como una unidad sino como una reunión de entidades disímiles que por ende mantendrían las controversias en muchos temas.

Habermas concibe la conformación de un Estado Universal con cualidad estatal por cuanto requeriría también de una autoridad coercitiva que hiciese eficaz la vinculación de las partes a la decisión del órgano central. Esa noción de obligación jurídica que supera una vinculación de corte moral, es la que daría un poder real a esa autoridad. Se trata pues de un Estado Cosmopolita en el cual el derecho que se violente en una parte del mundo afectará a todos por igual, haciendo con ello públicos los derechos humanos (en una esfera pública mundial) que se defenderán bajo una noción de consolidación de la paz perpetua. El Estado será por tanto una unidad que defienda la universalidad de los derechos del ser humano.

El filósofo alemán insiste en la necesidad de un cambio de concepción de los miembros que conformarían ese Estado Universal, indicando que deben superar sus motivaciones individuales para asumir motivaciones democráticas a favor de la defensa de los derechos humanos, y dice: "Si se amplían las preferencias valorativas más allá de la percepción de los intereses nacionales a favor de la puesta en marcha de la democracia y de los derechos humanos, cambian entonces las condiciones bajo las cuales funciona el sistema de potencias."[132]

Consciente de que un órgano Cosmopolita de esta índole puede afectar la soberanía nacional de los Estados que lo compongan, e incluso consciente de que esta es una de las grandes críticas a su propuesta, Habermas señala que será necesario institucionalizar el Estado Cosmopolita para que vincule a todos los gobiernos en una federación con instituciones comunes que regulen el orden jurídico entre sus miembros y controlen su cumplimiento con sistemas legales y judiciales unitarios y coercitivos.

Sin embargo, también reconoce que para ello debe variar la percepción interna actual del mundo: "La revisión de los conceptos fundamentales afecta a la soberanía de los Estados y al carácter cambiante de las relaciones interestatales, a la soberanía interna de los Estados y a las limitaciones normativas de la clásica política de expansión, así como a la estratificación de la sociedad mundial y a una globalización que hacen necesaria una reconceptualización[133] de aquello que entendemos como paz."[134]

---

[132] Jürgen Habermas, *La inclusión del otro, estudios sobre teoría política*, Barcelona, Editorial Paidós, 1999, p.154

[133] A esto es a lo que se refiere cuando habla de la superación de la amenaza recíproca que ha sido una constante entre las relaciones entre estados soberanos

[134] Jürgen Habermas, *op. cit.*, pp.161-162

En lugar de formar una confederación de Estados, se trata de formar una confederación de ciudadanos del mundo regidos bajo las bases de los derechos humanos que les son comunes a todos, construyendo una justicia mundial, un parlamento mundial y un nuevo Consejo de Seguridad.

La concepción de las personas como ciudadanos del mundo, se vería ajustada a las posibilidades reales de participación individual que ofrecen las TIC, mientras que el Estado Universal contribuiría a unificar en una única legislación y bajo un sistema jurídico (legislativo, administrativo y judicial) único, todas las actuaciones derivadas de Internet; procurando la seguridad jurídica de quienes participan como agentes en esa comunicación.

Sin embargo, el Estado Universal, contrarrestado con la diversidad de culturas que conforman el planeta, no es más que una utopía que de diversas formas se ha esgrimido a lo largo de los tiempos. Es una utopía que incluso ha servido para satisfacer desde la justificación teórica de estados totalitarios hasta la noción pacifista de igualdad universal sin fronteras.

2.4.5.2. La Computopía

Dentro de los defensores de una idea de Estado Universal pero bajo una perspectiva ya no político-filosófica sino tecnológica, podemos citar también al profesor Yoneji Masuda, que es uno de los fundadores de la sociedad informatizada japonesa a través de sus investigaciones en el Japan Computer Usage Development Institute. Masuda propone la existencia de la *Computopía*, que consiste en una organización política universal donde toda la problemática de la humanidad está globalizada y en virtud de la cual los individuos estarán organizados a partir de una democracia participativa directa con una base tecnológica de redes de comunicación universal. La organización se hará por un proceso en donde la retroalimentación (feed-back) será la regla de convivencia. Si en el intercambio de información y actividades se llegan a determinar las ventajas y desventajas de las actividades que realicen los individuos, el sistema se irá ajustando mediante un equilibrio natural de intereses derivado del Feed-back.

Pérez Luño ha estudiado sus propuestas, y resume los principios o condiciones necesarias que Masuda advierte para llevar a cabo la Computopía, indicando lo siguiente: “Tales principios o condiciones se refieren a: 1º) el reconocimiento del derecho de todos los ciudadanos, sin ningún tipo de discriminación o excepciones, a participar directamente en la decisión de los asuntos que les afecten; 2º) el espíritu de “sinergia”, es decir, de cooperación y de sacrificio voluntario y

altruista de los intereses egoístas en función del bien común, como exigencia ética que debe presidir todo el sistema social; 3º) la garantía del derecho de las personas y los grupos para conocer y acceder a todas las informaciones que les conciernan; 4º) la distribución equitativa entre los ciudadanos de los beneficios y cargas que comporta la vida social; 5º) búsqueda de las soluciones a través del acuerdo participativa y de la persuasión en los distintos conflictos y tensiones que puedan plantearse; y 6º) la cooperación de los ciudadanos en la puesta en marcha de las soluciones adoptadas sin que, por tanto, sea necesario acudir a la coacción acompañada del castigo por la fuerza de la ley, como sucede en las sociedades actuales."[135]

Tanto la propuesta del Estado Cosmopolita como la propuesta de la Computopía, sugieren la creación de un Estado Universal como germen fundacional de lo que podría ser la regulación unitaria de Internet, como una alternativa para la regularización de la sociedad virtual bajo las normas de un Estado real.

2.4.6. Alternativas territoriales

Finalmente esta propuesta parte de regular Internet a partir del juicio territorial: por Estados que emitan decisiones en virtud de su soberanía, o a partir de conglomerados de Estados adscritos por convención a jurisdicciones territoriales superiores.

2.4.6.1. Estatales

Es una postura que redime la soberanía de los Estados bajo las premisas de un orden jurídico como al que hacía referencia Thomas Hobbes con su *Leviathan*. Efectivamente quienes sostienen este sistema arguyen que el ser humano es por naturaleza antisocial, y de él no puede esperarse que de forma natural defienda los derechos humanos de otros, sino que requiere de un poder que le obligue y lo sancione, que ejerza una autoridad individual sobre su persona.[136]

Estas propuestas estatales también rechazan la teoría del Estado Universal, por cuanto consideran que su autoridad constituiría una violación a la soberanía de los Estados autónomos

[135] Antonio Pérez Luño, *Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las N.T. de la información*, Madrid, Colección editorial Los libros de FUNDESCO, 1987, p. 139

[136] Sus defensores rechazan abiertamente la autorregulación para abogar por un Estado al que el individuo se somete. Claro está, esa soberanía del órgano público debe ir regulada por un sistema de limitaciones y contrapesos que den garantía al administrado de que se defenderán sus intereses de forma objetiva y racional.

que son los que verdaderamente están llamados a coordinar el derecho dentro de su ámbito jurisdiccional.

Bajo ese fundamento teórico-filosófico de un Estado que impone su fuerza jurídica a la voluntad de los ciudadanos, se propone la implementación de normas nacionales para regular los problemas que se deriven de las relaciones de Internet. Sus defensores sostienen que como los problemas son los mismos en el mundo digital que en el mundo analógico (y lo único que cambia es el ámbito de acción del derecho) solo deben reformarse las normas para su aplicación en nuevos ámbitos donde los derechos han adquirido una mayor vulnerabilidad. Por ello, sostienen que hay normas internas que se aplican ya a Internet y por ende cada Estado puede ejercer su soberanía juzgando las actuaciones que se realicen en su jurisdicción. Al efecto dicen: "La existencia de un apreciable acervo normativo creado al margen de los ordenamientos jurídicos estatales no impide que éstos ocupen el lugar más destacado en la regulación de las situaciones jurídicas derivadas de Internet. No sólo porque es en los ordenamientos estatales (en sus normas de fuente interna e internacional) donde se localizan las disposiciones que necesariamente regulan muchas de esas situaciones (tutela de la propiedad intelectual, protección de los consumidores, represión de prácticas ilícitas), sino también porque el empleo de normas extraestatales en la regulación del comercio electrónico encuentra su fundamento en los propios ordenamientos estatales, que típicamente atribuyen un amplio alcance a la autonomía de las partes en la configuración de las transacciones comerciales internacionales. No existe un vacío jurídico, sino más bien al contrario, pues con frecuencia una pluralidad de legislaciones estatales son en principio aplicables a las actividades en Internet."[137]

Es claro que el problema es determinar cuándo le corresponde a cada Estado la jurisdicción dado que esa territorialidad es difícil de precisar en Internet, sobre todo cuando existen agentes que intervienen de forma invisible o cuyas actuaciones repercuten en el ámbito de diversas naciones de forma simultánea; por lo que la aplicación del derecho internacional actual resulta insuficiente.

El principio del tratamiento nacional de la regulación de Internet e incluso el tratamiento nacional de la protección de la propiedad intelectual, puede generar que solo se proteja a los usuarios nacionales (o autores nacionales) y queden por fuera de la protección el resto de agentes que interactúan en la Red, o bien que las empresas nacionales se vean afectadas por trabas que no

[137] Pedro de Miguel Asensio, op. cit., p. 89.

poseen *paraísos informáticos*. En el mismo sentido, genera una inseguridad jurídica en torno a cuál es la legislación aplicable y la determinación inequívoca de las conductas ilícitas.

2.4.6.2. Regionales

Se trata de regular Internet a partir de las decisiones regionales que adopten diversos grupos de naciones agrupadas por criterios de territorialidad que no representan la globalidad, y que sin embargo es la alternativa que han venido asumiendo los Estados desde hace algunos años, desde la Unión Europea, hasta los países de tradición anglosajona (*Common Law*) o sectores como el Parlamento Andino o el Parlamento Centroamericano, por citar algunos.

La tendencia ha sido establecer pautas de un derecho mínimo regional para que cada Estado estipule regulaciones internas que coincidan con esa voluntad común de una zona geográfica a la que esté políticamente adscrito.

De esta manera, se puede afirmar que ninguna de las teorías anteriormente descritas se ha impuesto de manera uniforme y por el contrario las soluciones actuales han correspondido a la incorporación parcial de ciertos aspectos de cada una de las propuestas, conformando una regulación mixta que lo único que ha generado es una discontinuidad de la legislación, una inseguridad jurídica y la inaplicación de muchas de las normas; ya sea por falta de jurisdicción, de medios de coerción o de competencia de quien legisla, o bien por la existencia de los propios medios tecnológicos que permiten la elusión de responsabilidades y de obligaciones acordadas por la comunidad de Internet.

2.5. Seguridad, contenidos y propuestas regulatorias en Internet. El Marco jurídico.

Desde que Internet ha comenzado a ser usado masivamente, existe la preocupación por su regulación. Es bien sabido que Internet es una red que se extiende por todo el planeta y que presenta la peculiaridad de no tener ningún centro de gobierno o control. La existencia de millones de páginas web, o emisores de información supone un reto para la regulación del nuevo medio que presenta características totalmente nuevas que nada tienen que ver con los medios de comunicación tradicionales.

Los efectos de semejante transformación ya se están haciendo sentir en la ciencia, economía, la política, la sociedad, la cultura, la educación y entretenimiento. La forma en que nos

interrelacionamos con los demás está siendo socavada por nuevas prácticas (compras on-line, chats, e-mail, educación a distancia, foros de discusión, etc.) y ya nadie puede ser capaz de predecir exactamente cuán profundos serán los cambios. Los que sí parece ser notorio es que el cambio debe ocurrir simultáneamente en todos los ámbitos a fin de lograr un proceso de transición armónico. En esta era digital o de la informática, infinidad de instituciones, normas, leyes, costumbres, formas de pensar y de relacionarse resultan inadecuadas e inapropiadas y necesitan ser revisadas y actualizadas en forma urgente.

A partir de la existencia de nuevas formas de operar con la tecnología delitos que no son nuevos, y que ya existían desde mucho antes de la aparición de la informática, se han planteado serios interrogantes que nuestro derecho positivo parece no saber cómo resolver.

Cualquiera de nosotros puede ser víctima de delitos,[138] tanto en el mundo "real", por llamarlo de alguna manera, como del "virtual". Sin embargo, parecería que las conductas nocivas realizadas en éste último ámbito gozan de cierta impunidad. Ciertas conductas como la destrucción de base de datos personales, el hurto o el fraude informático pueden resultar impunes en virtud de la falta de adecuación de la normativa vigente a las nuevas situaciones,[139] ya que, en el orden penal la ley debe contener la descripción precisa de las acciones delictuosas, únicas conductas susceptibles de ser penadas.[140]

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

Así pues, la proliferación de conductas nocivas que no encuentran un castigo adecuado demanda una mayor y más rápida actividad por parte de los legisladores. Esta es la mejor solución si queremos contar con un sistema jurídico seguro, que no de lugar a soluciones injustas y castigos no previstos expresamente por la ley. Son precisos y urgentes acuerdos internacionales a fin de armonizar criterios y evitar incompatibilidades entre distintos sistemas legales. El

---

[138] Por mencionar algunos, pueden ser el robo, el espionaje a través de un acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, o el espionaje industrial, el terrorismo mediante la existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo, siendo aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional, el propio narcotráfico ya que se ha utilizado a la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el bloqueo de dinero y para la coordinación de entregas y recogidas; así como más delitos como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

[139] Tal como lo expresa el principio de legalidad de la máxima "nullum crimen nulla poena sine lege" (no hay delito ni pena sin ley penal anterior).

[140] Isern, M, *Ciberespacio y Propiedad Intelectual*, mensaje nº 10, Infonomía, 17 de enero del 2001.

anquilosado ordenamiento jurídico se nos presenta como un aparato demasiado "pesado", lento y obsoleto, como para seguir el desenfrenado e imparable ritmo impuesto por el desarrollo de las tecnologías y hacer frente a los desafíos planteados por la revolución digital.

En un primer término, debe considerarse que en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

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

De esta forma, la OCDE en 1986 publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica, en donde se reseñaban las normas legislativas vigentes y las propuestas de reformas en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.[141]

Una vez desarrollado todo este proceso de elaboración de las normas a escala continental, el Consejo de Europa aprobó la recomendación R (89) sobre delitos informáticos, en la que "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras... y en particular las directrices para los legisladores nacionales."[142]

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

[141] Como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.
[142] Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

Por otra parte, en el ámbito de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.[143]

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal -hasta ese entonces era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En este orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo en 1992, adoptó diversas, recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el derecho penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad). Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación deberá tenerse en cuenta hasta qué punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.[144]

Un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras.

Desde hace aproximadamente doce 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.

Así el Consejo Europeo en su reunión de Corfú del 24 al 25 de junio de 1994, propuso la creación de un marco jurídico comunitario para regular específicamente la sociedad de la

[143] En http:// www.oecd.org/chapter1.htm [consultado el 2 de marzo de 2007]
[144] Además, señala que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

información en Europa dentro de un mercado interior que genere nuevos bienes y servicios. Desde entonces, la Comunidad Europea ha emitido regulaciones que incluyen desde la protección de los consumidores de Internet,[145] hasta materias sobre normalización de las telecomunicaciones o aspectos sobre la seguridad del uso de Internet.

En el ámbito comunitario se ha reconocido al sector de telecomunicaciones (pilar de la sociedad de la información) como un servicio universal[146] y como tal, se debe permitir el acceso general de los usuarios a un conjunto de servicios que derivan de la telemática.

A esa resolución se le suma otra referente a la difusión electrónica del derecho comunitario y de los derechos de acceso y consulta de legislación por medio de mecanismos electrónicos, dando una importancia especial a las facilidades que en esta era han introducido las TIC.[147]

Otro grupo de normas pretende la normalización del ámbito de las TIC en la región[148] o el establecimiento de prioridades políticas en la materia.[149]

Otros documentos se han centrado en la regulación común de los contenidos ilícitos y nocivos de Internet en el ámbito regional. Tal es el caso de la Decisión nº 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999 por la que se aprueba el plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales;[150] o bien la Resolución del Consejo y de los representantes de los Gobiernos de los Estados Miembros reunidos en el seno del Consejo de 17 de febrero de 1997 sobre contenidos ilícitos y nocivos en Internet.[151]

---

[145] Resolución del Consejo de 19 de enero de 1999 sobre la dimensión relativa a los consumidores en la sociedad de la información. Diario Oficial nº C 023 de 28 /01/1999, p. 1-3

[146] Resolución del Consejo, de 7 de febrero de 1994 relativa a los principios del servicio universal en el sector de las telecomunicaciones. Diario Oficial nº C 048 del 16/02/1994

[147] Resolución del Consejo del 20 de junio de 1994 relativa a la difusión electrónica del derecho comunitario y de los Derechos nacionales de ejecución y a la mejora de las condiciones de acceso. Diario Oficial nº C179 de 01/07/1994, p.3-5

[148] Resolución del Consejo del 27 de abril de 1989 relativa a la normalización en el ámbito de las tecnologías de la información y de las telecomunicaciones. Diario oficial nº C117 del 11/05/1989

[149] Resolución del Consejo de 21 de noviembre de 1996 relativa a las nuevas prioridades políticas en materia de sociedad de la información. Diario Oficial nº C 376 del 12/12/1996, p. 1-5

[150] Decisión nº 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999 por la que se aprueba el plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. Diario Oficial nº L 033 de 06/02/1999, p.1-11

[151] Resolución del Consejo y de los representantes de los Gobiernos de los Estados Miembros reunidos en el seno del Consejo de 17 de febrero de 1997 sobre contenidos ilícitos y nocivos en Internet, Diario Oficial nº C070 del 06/03/1997, p.1-2

Sin embargo, regular Internet con base en leyes territoriales es también una alternativa que se constata ya en algunas legislaciones que empiezan a adoptarse en la Unión Europea, de países que pretenden ajustar las acciones que se realicen en Internet a través de su normativa interna.[152]

En el tema de la pornografía infantil, bajo la dirección e incluso el financiamiento de entidades públicas o estatales autónomas, muchos proveedores de servicios han aunado esfuerzos para consolidar mecanismos de denuncia que sirven de control en contra de estos actos ilícitos, y para ello han puesto a disposición de usuarios líneas de denuncia por Internet (páginas web o correos electrónicos).[153]

También existen empresas que han facilitado a los Estados o han implementado en sus servicios privados (en condición de proveedores de servicios) mecanismos tecnológicos de control (conocidas como medidas tecnológicas con sus respectivos controles antielusión) que impiden el acceso a ciertos contenidos,[154] la descarga de ciertas páginas o incluso el seguimiento de visitas de un usuario.[155]

Tanto la Unión Europea como el Consejo de Europa han elaborado documentos que pretenden la vinculación de sus miembros y que incluso los obligan a adaptar su normativa interna para la armonización de las medidas que deben regir en Internet uniformemente para todos los Estados miembros.

El fin es evitar ordenamientos jurídicos fragmentados o contradictorios que dificulten las transacciones en el mercado interior europeo por lo que se aboga por la "armonización".

Por su parte, dentro de esta misma inquietud sobre los contenidos ilícitos de Internet, el Consejo de Europa emitió la denominada Recomendación del Consejo de 25 de junio de 2001

---

[152] Tal es el caso, por ejemplo de la denominada "*Charte de l´Internet*" en Francia, creada el 5 de marzo de 1997 bajo el auspicio del Ministerio de Correos y Telecomunicaciones, en la que se ofrecen reglas de actuación que pueden adoptar los usuarios y los proveedores de servicios de Internet, para utilizar legítimamente este servicio. La intención de la *Carta de Internet* es también crear un órgano compuesto por los diferentes agentes que participan en la Red para que funcione de mecanismo regulador y conciliatorio.

[153] En Inglaterra, entidades públicas han creado un código de conducta denominado *R3 Safety-Net* que pretende precisamente la persecución de la pornografía infantil en Internet que establece controles entre diversos proveedores, mecanismos de denuncia y determina responsabilidades sobre la manipulación, oferta y acceso a este material.

[154] Tal es el caso de software como el Cyberpatrol o el Netnanny

[155] La ventaja es que es el propio usuario quien decide establecer límites de ingreso a Internet para evitar por ejemplo que menores de edad accedan a ciertos contenidos ilícitos o nocivos. La desventaja es cuando esos mecanismos de control son impuestos por terceros que intentan ejercer un control tanto sobre la autodeterminación informativa de los usuarios o bien sobre su intimidad en relación no solo a datos sino a la libertad que ostentan de navegar en Internet, remitirse correos electrónicos personales y mantener comunicaciones privadas (y por ende inviolables) a través de las nuevas tecnologías que facilita la sociedad de la información; o bien cuando palabras claves impiden el acceso a contenidos ilícitos pero también a otros webs de otra índole que se ven afectadas por los metatags incluidos.

sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología,[156] en el cual se pretende la centralización del control en la región bajo las directrices del G8.

Es importante destacar la Resolución del Consejo del 3 de octubre de 2000 sobre la organización y gestión de Internet,[157] como normativa que conmina a los Estados a fomentar políticas regionales para la administración de Internet pues se encarga a una Comisión para que: 1º) fomente la coordinación para la gestión de Internet, 2º) establezca acuerdos entre los Estados para una internacionalización de la gestión de Internet respetando políticas públicas y acuerdos internacionales y 3º) constituya una red europea de competencias científicas, técnicas y jurídicas para la gestión de nombres de dominio, direcciones y protocolos de Internet entre los Estados miembros.

Ese reconocimiento del poder que en Internet ostentan las instancias privadas (proveedores de servicios, proveedores de acceso o empresas privadas) sobre el ámbito de acción individual de los Estados o regional de la comunidad, es una evidencia de que las acciones regionales, pese a su conveniencia, resultan insuficientes sin la incorporación de los agentes que intervienen en Internet (cuyo origen no es territorial).

El 8 de febrero de 2002 el Consejo de Ministros, tras dar por cerrada su labor en el Proyecto de Ley de Internet, remitió al Parlamento el proyecto denominado Ley de Servicios de la sociedad de la información y contratación electrónica.

El Proyecto, pretende dar respuesta normativa a dos aspectos: en primer lugar regular la denominada sociedad de la información, como "realidad" que interconecta a los proveedores de servicios y a los usuarios, y en segundo lugar, regular la contratación electrónica.

En la mayoría 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.

Aunque la preocupación por la presencia de material ilícito y nocivo en la Red es la misma, las soluciones que se están aportando en estos momentos son distintas. Mientras que en la Unión Europea se propician otros métodos combinados, como el uso de filtros o las líneas de

[156] Recomendación del Consejo de 25 de junio de 2001 sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología (2001/C 187/02) publicada en el DOCE C 187 del 3/7/2001

[157] Resolución del Consejo del 3 de octubre de 2000 sobre la organización y gestión de Internet (2000/C 293/02) Publicada en el DOCE C 293 del 14-10-2000

denuncia, en Estados Unidos ha existido un intento regulación y limitación de la libertad de expresión en Internet con la Ley de Decencia en las Telecomunicaciones (Congress Decency Act).

Dentro de esta última inquietud, la *Anti-Terrorism Ac*t de Estados Unidos conocida como USA PATRIOT, aprobada el 26 de octubre del 2001 a raíz de los atentados terroristas del 11 de septiembre en Estados Unidos es una iniciativa estatal autónoma para regular desde una única nación, los flujos de datos y demás información que circula en Internet.[158] Este documento, cuya denominación oficial es "The Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001"[159] fue aprobado solo con un voto en contra en el Senado, pese a la gran oposición interna e internacional por las serias violaciones que podría implicar a los derechos civiles[160] y sobre todo a la injerencia en las actividades extra-territoriales.

Dentro de sus normas, la USA PATRIOT permite a los agentes del FBI y a miembros de la Fiscalía vigilar -por simple sospecha de que se esté ejerciendo una actividad terrorista- las comunicaciones y transacciones financieras por Internet, permite que los datos personales se compartan entre las administraciones internas (como las agencias), permite además aplicar la tecnología *Carnivore* con el uso del *pen registe*r.[161] Los proveedores de servicios de Internet quedan obligados a contribuir a esta intervención, permitiendo a las autoridades capturar información de sus usuarios o facilitar la instalación de la tecnología *Carnivore*. Lo que más preocupa a los opositores de esta ley, sobre todo en el ámbito internacional, es que a partir las amplias prerrogativas de la policía estadounidense se reconduzca el tráfico de Internet hacia servidores centrales, donde autoridades de ese país retendrían los mensajes de correo electrónico para su revisión; en una actividad que atentaría contra la soberanía del resto de naciones que

[158] A raíz de los atentados del 11 de septiembre, todo aquel que delinque a través de Internet ha sido englobado en un mismo grupo, donde caben desde malhechores, terroristas, criminales, traficantes y todos son juzgados de la misma manera**.** Así, hoy, la forma de actuar ante un crimen informático es el mismo ante el robo, la estafa o el hurto, teniendo en cuenta factores como el valor de la pérdida producida para dictaminar sentencia. Ahora se estima un máximo de diez arios de prisión para los criminales informáticos que sean arrestados por primera vez, sin hacer distinción alguna en el tipo de delito.

[159] The Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, (conocido como Anti-terrorism Act). En http://216.110.42.179/docs/usa.act.final.102401.html (12/12/2001)

[160] El polémico documento también amplía el período de detención sujeto al *Hábeas Corpus* de dos a siete días con una opción de renovar la detención indefinidamente por periodos de 6 meses si se considera que el detenido es una amenaza para la seguridad nacional, lo que ha sido criticado por defensores de los derechos civiles en Estados Unidos

[161] Un dispositivo de seguimiento electrónico que se conecta a una línea telefónica para registrar los números marcados y obtener datos sobre la dirección IP de los usuarios y demás datos de la comunicación electrónica.

interactúan en Internet y por supuesto, contra los derechos fundamentales de usuarios ajenos al mundo del terrorismo.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas. Y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico institucional debe proteger.

En la II Reunión de Ministros de Justicia y Procuradores Generales de las Américas, representantes de 24 países de la Organización de los Estados Americanos advirtieron sobre la necesidad de nuevas leyes para controlar los delitos a través de la superautopista de la información, la presencia de software ilegales, el fraude y la pornografía infantil.

En la Resolución 56/183 (21 de diciembre de 2001) de la Asamblea General de las Naciones Unidas se aprobó la celebración de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) en dos fases. La primera se celebró en Ginebra, acogida por el Gobierno de Suiza, del 10 al 12 de diciembre de 2003, y la segunda tuvo lugar en Túnez, del 16 al 18 de noviembre de 2005.[162]

Si, por una parte, la CMSI recomienda la participación de los gobiernos en el más alto nivel, por otra se invita a participar a representantes de todos los organismos competentes de las Naciones Unidas y otras organizaciones internacionales, las organizaciones no gubernamentales, el sector privado, la sociedad civil y los medios de comunicación para establecer un verdadero proceso multiparticipativo. La Cumbre Mundial sobre la Sociedad de la Información incita a la solidaridad y a las alianzas, pero da una gran tarea de ahora en adelante.

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

[162] Tomadas por separado, cada una de las fases de la Cumbre es la culminación de muchos meses de consultas y negociaciones entre los Estados Miembro, expertos de las Naciones Unidas, el sector privado y los representantes no gubernamentales, que estudian una enorme cantidad de información y comparten un cúmulo de experiencias en los temas relacionados con la Sociedad de la Información.

definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, deben mencionarse la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición. Teniendo presente esa situación, consideramos que es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán considerar los diferentes niveles de desarrollo tecnológico caracterizan a los miembros de la comunidad internacional.[163]

La legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

El debate sobre los límites de la regulación de Internet es global, pero las tendencias en Estados Unidos y en los países europeos tendrán, sin duda, una influencia directa tanto en la regulación mexicana como en la de otras naciones.

---

[163] El "Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos" (en http://www.un.org/spanish) señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos: Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos, Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas, Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos, Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos, Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras y Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Frente a la corriente reguladora se levantan los partidarios de que ciertas áreas queden libres del intervencionismo o proteccionismo estatal. Entre los argumentos más utilizados figuran el derecho a la intimidad y la libertad de expresión.[164]

De todo lo anteriormente dicho, y en mi opinión, creo que la libertad de expresión y el derecho a la información deben estar garantizados, independientemente de cualquier medio de manifestación. Por lo tanto, el Internet no debe quedar al margen, siendo ésta la red de redes más importante y con mayor tráfico de información a nivel mundial, el acceso a toda esta información debe facilitarse a todos los interesados a un precio razonable, sin perder de vista los derechos de propiedad intelectual, en particular las leyes internacionales y locales de derechos de autor.[165]

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

[164] Uno de los derechos más defendidos en los países en los que ha habido una gran implantación de los sistemas informáticos en la gestión de los datos de los ciudadanos por parte de la administración, ha sido el derecho a la persona a que su intimidad no sea vulnerada por un abuso de estos medios. La protección de éste derecho ha generado preceptos de rango constitucional en muchos países.

[165] Esa red permite la difusión y el acceso a gran número de documentos, obras multimedia, conciertos, música, base de datos, archivos, información económicas, tecnológica, películas; incluso permite la telefonía a costos de llamadas locales.

CAPÍTULO III

EL TERRORISMO Y EL TERRORISMO INFORMÁTICO. PRECISIONES CONCEPTUALES, TERMINOLÓGICAS Y DE CONTENIDO.

A lo largo de la historia de la humanidad, ha habido muchas amenazas a la seguridad de las naciones. Dichas amenazas han provocado la pérdida de vidas humanas a gran escala, la destrucción de bienes materiales, enfermedades y lesiones generalizadas, el desplazamiento de grandes cantidades de personas y pérdidas económicas devastadoras.

Los recientes adelantos tecnológicos y la constante agitación política en el ámbito internacional son componentes del riesgo cada vez mayor para la seguridad nacional, asimismo, en los últimos años, la sociedad ha sido víctima de uno de los peores flagelos: el terrorismo, que es un hecho expresivo de violencia que se lo puede ver durante toda la historia en sus más variadas formas de expresión y crueldad.

El terrorismo se constituye así tanto en el ámbito interno como en el mundial, como en una vía abierta a todo acto violento, degradante e intimidatorio, y aplicado sin reserva o preocupación moral alguna.

Los fines buscados por esta forma de "guerra" no convencional pueden tener fines políticos, religiosos, culturales y mediáticos. Por dichas causas, el mundo se ve sacudido diariamente con noticias de atentados producidos en la vía pública, donde pierden la vida gente inocente y totalmente ajena a esa "guerra" o intereses diversos.

Este fenómeno es una de las formas de violencia más difíciles de contener debido a que su campo de acción se extiende más allá de las regiones de conflicto. Es un fenómeno que se caracteriza por su violencia indiscriminada, involucrando a víctimas que no tienen nada que ver con el conflicto causante del acto terrorista; su imprevisibilidad, actúa por sorpresa creando incertidumbre, infundiendo terror y paralizando la acción; su inmoralidad, produce sufrimiento innecesario, golpeando las áreas más vulnerables; al ser indirecto el blanco, el instrumento es usado para atraer la atención y para ejercer coerción sobre la audiencia o un blanco primario, a través del efecto multiplicador de los medios de comunicación masivos. A los actos terroristas debe responderse por medio de normas jurídicas que contemplen su prevención y sanción.

Ahora bien, antes de cualquier consideración jurídica, es necesario hacer un balance de la realidad mundial relacionada con el terrorismo durante los últimos años, para así percibir la magnitud del fenómeno.

Se ha calculado que existen aproximadamente 29 organizaciones terroristas a nivel mundial, de las cuales 14 (48%) son de tendencia islámica.

En 1999 se registraron 392 atentados, cuyo número se vio incrementado, en 2000, a 409, y de los cuales, 169, es decir: el 41.3%, fueron contra personas, bienes o intereses de Estados Unidos de América.

En cuanto al número de muertes provocadas por estos actos, puede señalarse que durante 1999 hubo 223 y en 2000 ascendió a 409. En 2000, 19 (4.6%) de esas muertes fueron de nacionales de los EUA, de los cuales 17 resultaron del atentado contra el buque US-Cole, en Yemen.

El número de personas heridas en ataques terroristas en 2001 fue de 1,080, número que ascendió respecto de la cifra del año anterior, que fue de 796. Mención aparte merece 2001. Durante ese año murieron 3547 personas en 346 atentados terroristas, lo que lo coloca como un año particularmente trágico, porque además del considerable daño causado, anuló de manera evidente los avances hasta entonces alcanzados por la comunidad internacional en la lucha contra la práctica asesina de este crimen, toda vez que sus víctimas no son previamente individualizadas por los sujetos activos y no necesariamente tienen una relación con los propósitos ideológicos de los autores de dichos actos.

De las 3547 víctimas por actos terroristas durante 2001, 3192 (90%) resultaron de los atentados perpetrados en los EUA, durante la jornada del 11 de septiembre, y donde murieron nacionales de 78 países diferentes.

Así, se puede observar que el número de ataques terroristas en el mundo ha decrecido (de 426 en 2000 a 346 en 2001, donde 178 ataques con bomba fueron contra multinacionales petroleras en Colombia, lo que constituyó el 51% del total de ataques en 2001. En 2000 fueron 152 ataques con el mismo mecanismo y los mismos objetivos); sin embargo, la eficacia de sus resultados va en aumento, sin considerar aun la posibilidad de que armas de tipo nuclear lleguen a manos de terroristas para efectuar este tipo de actos.[166]

[166] Cfr. U. S. Department of State, Patterns of Global Terrorism 2001, 21 de mayo de 2002, en http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10235.htm

3.1. Concepto de terrorismo

Desde el punto de vista jurídico, los actos de terrorismo presentan un problema técnico, en el sentido de plantear una dificultad en cuanto a poder definir con exactitud los alcances de los vocablos que ciñan la conducta típica, antijurídica y culpable.

El término terrorismo no tiene una definición jurídica formalmente acordada en el ámbito internacional. A pesar de ello, las más variadas definiciones que se han podido identificar (jurídicas o no), tienen como puntos recurrentes la violencia con un propósito político o social, así como el intento de intimidar y dirigir el acto a civiles o no combatientes.[167]

El terrorismo es algo más que la simple violencia en la que podrían quedarse algunas definiciones y análisis simplistas, donde se considera este tipo de acto delictivo como simple expresión de la delincuencia común y donde se requieren sólo dos partes: un agresor y una víctima.

Es de gran importancia resaltar que en el caso del terrorismo se necesita una tercera parte: las personas que pueden ser intimidadas por lo que le pasó a la víctima.[168] Por lo anterior, se puede decir que el terrorismo es un fenómeno social complejo, porque los factores que lo causan, así como la naturaleza, metas e identidad de los terroristas varían en función de las diversas épocas o sociedades que se estudien.[169] No obstante, el proceso de globalización en que se ha visto inmerso el Estado en la actualidad podría hacer aspirar a una definición que involucre los valores predominantes de la época; sobre todo, en cuanto a lo que se entiende por paz entre los Estados y por la adopción de los estatutos convencionales internacionales vigentes que intentan garantizarla. Esto, evidentemente, también presenta un punto débil en cuanto a la homogeneización obligatoria que excluye a las minorías internacionales, aun sin incorporarse al proceso globalizador, y que son precisamente las promotoras de la conducta que se intenta definir y evitar. Dicho en otras palabras, es imposible una definición absoluta o totalizadora mientras existan grupos que no siguen el espíritu de la época.

---

[167] La agencia noticiosa Reuters tiene establecida la política de no utilizar en sus notas el vocablo terrorista para describir a individuos, organizaciones o actos, ya que la definición de quién es o no es un terrorista está sujeta a la interpretación. Cfr. Cason, Jim y Brooks, David, *Decide Reuters no usar la palabra terrorista para describir a individuos, organizaciones o actos*, La Jornada, México, 29 de septiembre de 2001, p. 7.

[168] Cfr. Mkhondo, Rich, *Terrorism*, en Gutman, Roy *et al*., *Crimes of War*, Nueva York, Norton & Co. Ltd., 1999, p. 349.

[169] Cfr. Zanders, Jean Pascal et al., *Risk Assessment of Terrorism with Chemical and Biological Weapons*, en Stockholm International Peace Research Institute, SIPRI Yearbook 2000, Gran Bretaña, Oxford University Press, 2000, pág. 112.

En general, "Una acción puede definirse como terrorista cuando concurren tres elementos: un acto/amenaza de violencia, una reacción psicológica (o psicosociológica) y unos efectos sociales."[170]

La evolución y diversidad de esta clase de violencia, sus métodos y fines planteados pueden percibirse en el tiempo si se hace un recorrido histórico, desde el atentado en Sarajevo en 1914, donde perdió la vida el archiduque Francisco Fernando y desencadenó la Segunda Guerra Mundial, hasta los atentados contra las Torres Gemelas en Nueva York, en septiembre de 2001; ruta que contiene los hechos del Comando Septiembre Negro, durante las trágicas Olimpiadas de Munich 1972, o la bomba que destruyó el vuelo 103 de Pan Am sobre la localidad de Lockerbie, en Escocia; o los sucesos del Achille Lauro, los atentados de ETA en España, del IRA en el Reino Unido, o los palestinos que, solitarios y con bombas atadas a sus cuerpos, se inmolan en lugares concurridos de Israel, en busca de una justicia terrena y divina.[171]

En su sentido más amplio, el terrorismo es la táctica de utilizar un acto o una amenaza de violencia contra individuos o grupos para cambiar el resultado de algún proceso político. Ahora bien, el terrorismo puede ser definido de manera más específica tomando en cuenta diferentes aspectos:

a. Su definición gramatical: que siguiendo el diccionario de la lengua española, editado por la Real Academia Española, lo define así: "(del Latín terror). Dominación por el terror.// Sucesión de actos de violencia ejecutados para infundir terror."[172]
b. Su definición histórica, "época durante la Revolución Francesa en que eran frecuentes las ejecuciones por motivos políticos".
c. Su definición Jurídica, que de acuerdo al diccionario de ciencias jurídicas, políticas y sociales de Manuel Osorio, lo define así: "actos de violencia en contra de personas, la libertad, la propiedad, la seguridad común, la tranquilidad pública, los poderes públicos y el orden constitucional o contra la administración pública."[173]
d. Su definición Militar: " serie de actos de violencia, destinados a infundir terror por medio de la eliminación de personas. Crea un estado físico y espiritual que prepara a la población para su captación y conquista y que facilita su dominación. El terrorismo

[170] Joaquín, Alcaide Fernández, *Las actividades terroristas ante el derecho internacional contemporáneo*, Madrid, Tecnos, 2000, p. 50.
[171] Cfr. Serrano Figueroa, Rafael, *El derecho humanitario frente a la realidad bélica de la globalización*, México, UNAM, Facultad de Derecho, 2002 (tesis doctoral), p. 87.
[172] *Diccionario de la Real Academia Española*, p. 1693.
[173] Manuel Osorio, *Diccionario de las Ciencias Jurídicas, Políticas y Sociales*, Argentina,Ed. Heliasta, 1990, p. 432.

tiene un objetivo aparente y sin mayor sentido en sí mismo, como es la difusión del miedo, pero su finalidad real pasada es, juzgar al pueblo, a través de la aplicación de un metodología activa y esencialmente torturante."[174]

e. Su definición Política: " No existe una definición política concreta sobre el terrorismo, Los países occidentales cuando internamente se ven afectados, (...) lo incluyen dentro de las figuras tipificantes de violaciones, como delitos contra las personas, la libertad (...)."[175]

Externamente, el terrorismo es calificado desde dos puntos de vista, el primero, durante el estado de guerra, dónde los acontecimientos estarán dentro de las violaciones a los tratados suscritos, tales como los Convenios de Ginebra de 1949, o de aspectos particularizados, como aquellos que originaron el Acuerdo y Estatuto de Londres, del 8 de Agosto de 1945, determinantes del Tribunal de Nuremberg.[176]

El segundo se da durante el estado de paz, por la aplicación de las normas previstas en la resolución de la Asamblea General de las Naciones Unidas, en 1974, en la cual se define a la agresión, por la violación de la Declaración Universal de Derechos Humanos.[177]

De esta manera, existen además diferentes definiciones de terrorismo, dentro de las cuáles destaco las siguientes:

"Es el uso calculado de la violencia o de la amenaza de la violencia de inculcar miedo; se prepuso forzar o intimidar a gobiernos o a sociedades en la búsqueda de las metas que son generalmente políticas, religiosas, o ideológicas."[178]

Por su parte Walter Laqueur lo define como "(…) el asesinato sistemático, la mutilación criminal, y amenaza del inocente para crear miedo e intimidación para ganar un acto político o táctico y para ser ventajoso, normalmente para influir a un público."[179]

James M. Poland, dice que "El terrorismo es el uso ilegal o amenaza de violencia contra personas o propiedad. Normalmente se piensa que intimida o coerce a un gobierno, individuo o grupo, o para modificar su conducta o política."

---

[174] En http://www.interpol.com/Public/Terrorism/default.asp [consultado el 18 de diciembre de 2006.]
[175] Joaquín, Alcaide Fernández, *op. cit*., p. 94.
[176] En http://www.un.org/spanish/docs/sc98/scrl98.htm [consultado el 12 de enero de 2007]
[177] *Idem.*
[178] Esta definición fue hecha cuidadosamente por Brian Jenkins para distinguir entre el terrorismo y otras clases de violencia. El acto del terrorismo es independiente definido de la causa que lo motiva. La gente emplea violencia del terrorista en el nombre de muchas causas. La tendencia a etiquetar como terrorismo cualquier acto violento de el cual no aprobemos es errónea. El terrorismo es una clase específica de violencia. El terrorismo es el uso ilegítimo de fuerza para lograr un objetivo político cuando las personas inocentes son los afectados.
[179] Walter, Laqueur, *Una historia del terrorismo*, (trad. Tomás Fernández A), Buenos Aires, Ed. Paidos, 2003, p. 43.

Asimismo, el FBI concluye que el terrorismo "Es uno de los problemas claves con los que históricamente los países de América Latina se han tenido que enfrentar. Las causas sociales y económicas de este fenómeno son ampliamente conocidas. Los gobiernos de América Latina a menudo han respondido al terrorismo con medidas altamente represivas, que no sólo incluyen a los presuntos terroristas, si no que violan los derechos fundamentales de la población en general. La otra respuesta típica, el terrorismo de estado, es la causa mayor de violaciones a los derechos humanos en el continente."[180]

El Título 22 del Código de los Estados Unidos, Sección 2656f(d), define el término terrorismo como "violencia premeditada, políticamente motivada perpetrada contra objetivos no-combatientes[181] por grupos subnacionales o agentes clandestinos, generalmente con la intención de influenciar a una audiencia … El término "terrorismo internacional" significa aquel que involucra a ciudadanos o a territorios de más de un país…El término "grupo terrorista" significa cualquier grupo que practica, o que tiene subgrupos significativos que practican el terrorismo internacional."[182]

El término "actividad terrorista" es definido en el Acta de Antiterrorismo y Pena Capital de 1996 de Estados Unidos de América, como "cualquier actividad que se considere ilegal bajo las leyes del lugar donde se cometa[183] y que involucre cualquiera de los actos siguientes: (I) El secuestro o sabotaje de cualquier medio de transporte.[184] (II) El detener o retener y amenazar con matar, herir o mantener en detención a un individuo, para obligar a una tercera persona[185] a hacer o abstenerse de hacer un acto, como condición implícita o explícita para la liberación del individuo retenido o detenido. (III) Un ataque violento sobre una persona protegida internacionalmente[186]o sobre la libertad de tal persona. (IV) Un asesinato. (V) El uso de cualquiera de lo siguientes - (a) agentes biológicos, agentes químicos, o armas o artefactos

[180] En http://www.fbi.gov [consultado el 19 de diciembre de 2006.]
[181] Para propósitos de esta definición, el término "no-combatiente" se interpreta que incluye, adicionalmente a civiles, personal militar que en el momento del incidente se encuentra desarmado o fuera de servicio. Por ejemplo, los asesinatos del personal militar de los E.U.: Cor. James Rowe, muerto en Manila en abril de 1989; Cap. William Nordeen, agregado de la Defensa de los E.U., muerto en Atenas en junio de 1988; los dos servidores muertos por una bomba en la discoteca Labelle en Berlín Occidental en abril de 1986; y los cuatro marinos adscritos a la embajada de los E.U. en el Salvador, asesinados en un café en junio de 1985. Considera también como actos de terrorismo ataques a instalaciones militares o a personal militar armado cuando no existe en el lugar un estado de hostilidades militares, tales como los bombardeos a bases estadounidenses en Europa, Filipinas, o en cualquier otro lugar.
[182]El gobierno de Estados Unidos ha empleado esta definición de terrorismo para propósitos estadísticos y analíticos desde 1983.
[183] Si es cometido en los Estados Unidos, será ilegal bajo las leyes de los Estados Unidos o cualquier estado.
[184] Incluyendo aeronaves, embarcaciones o vehículos.
[185] Incluyendo a una organización gubernamental.
[186] Definido en la sección 1116(b) (4) del título 18, del Código de los Estados Unidos.

nucleares, o (b) explosivos o armas de fuego,[187] con la intención de poner en peligro, directa o indirectamente, la seguridad de uno o más individuos o causar un daño substancial a la propiedad. (VI) La amenaza, intento o conspiración de realizar cualquiera de los puntos anteriores.”[188]

El Manual de Campo del Ejército de los Estados Unidos define el terrorismo como "el uso ilegal de (o amenaza de usar) la fuerza o violencia contra individuos o propiedades para ejercer coerción o intimidar gobiernos o sociedades, frecuentemente para lograr objetivos políticos, religiosos o ideológicos."[189]

Así, todas las definiciones actuales de terrorismo comparten un elemento común: conducta motivada políticamente. Algunas de estas definiciones incluyen violencia por beneficios económicos o religiosos. Adicionalmente, el rápido crecimiento de las organizaciones criminales transnacionales y el crecimiento del rango y escala de tales operaciones, pueden bien resultar en el uso de violencia para alcanzar objetivos cuya motivación sea la obtención de beneficios financieros.

El término terrorismo implica una acción llevada a cabo por grupos no gubernamentales o por unidades secretas o irregulares, que operan fuera de los parámetros habituales de las guerras y a veces tienen como objetivo fomentar la revolución. El terror de Estado, ejercido por un Estado contra sus propios súbditos o comunidades conquistadas, se considera a veces como una modalidad de terrorismo. Más que la realización de fines militares, el objetivo de los terroristas es la propagación del pánico en la comunidad sobre la que se dirige la violencia. En consecuencia, la comunidad se ve coaccionada a actuar de acuerdo con los deseos de los terroristas. El terrorismo extremo busca a menudo la desestabilización de un Estado causando el mayor caos posible, para posibilitar así una transformación radical del orden existente.

En conclusión se le puede definir como: “Es el uso real o amenaza de recurrir a la violencia con fines políticos, económicos o religiosos ó ideológicos que se dirige no sólo contra víctimas individuales sino contra grupos más amplios y cuyo alcance trasciende con frecuencia los límites nacionales.”[190]

Aun cuando hoy la suposición es que todos los actos terroristas están motivados políticamente, algunos actos están motivados por otros factores, y el número puede crecer a la luz de la expansión de la actividad criminal internacional y en un número creciente de actos

[187] Con cualquier otro propósito que el de obtener ganancias monetarias personales.
[188] Acta de Antiterrorismo y Pena Capital de 1996 de Estados Unidos de América.
[189] Los objetivos religiosos e ideológicos requieren de acción política; en consecuencia, es la violencia para modificar la conducta política, que constituye la preocupación militar primaria.
[190] Definición propia adoptada de las diferentes enunciaciones del presente trabajo.

extremistas llevados a cabo en nombre de causas religiosas y culturales. Lo cierto es que un nuevo enfoque puede centrarse más en definir los actos terroristas, dando menos énfasis a la motivación detrás de los éstos.

3.2. Características del terrorismo

Como se mencionó anteriormente, el terrorismo es el uso de la fuerza o la violencia contra las personas o los bienes materiales en violación de las leyes penales de los Estados con fines de intimidación, coerción o petición de diversos motivos.

Asimismo el término de terrorismo es usado para calificar actos que aterran o atemorizan una sociedad o un subgrupo de ella, pero cuya génesis puede variar de lugar a lugar (rural o urbana), de tiempo en tiempo y de materia a materia (por ejemplo, aérea o marítima) y, en consecuencia, variar su motivación (religiosa, ideológica, en estrategias de guerra de guerrilla, liberación, etcétera) y su regulación (nacional o interna o internacional), por la selección de sus objetivos (puestos de mando de la armada, puentes, telecomunicaciones) y por ello variar los medios de acción (armas de fuego, contaminación de aguas con químicos o como se teme últimamente: el riesgo de que se usen armas biológicas, químicas o hasta el uso de armas nucleares).

Puede entonces inducirse que el terror provocado por una acción con un móvil ideológico es terrorismo, pero esta posición tiene sus riesgos. En una época de globalización hegemónica como la actual, este criterio parecería incluso útil a ciertos propósitos (los terroristas incluidos), al ostentar la carencia de ideologías desde un punto de vista formal o académico; esto es, la ausencia de ideas sistematizadas en un marco teórico que sirvan de guía y apoyo a las razones esgrimidas, lo que no sería difícil encontrar hoy en día y que llevaría a evitar la configuración de la conducta.

Para algunos, es un hecho que a un grupo armado que provoca violencia social o política se le dé la calificación de terrorista; no basta que dicho grupo actúe de manera permanente o estable, sino que también debe ser una entidad o cuerpo consolidado para producir sistemáticamente terror en la sociedad, lo que se traduce en efectos negativos sobre la seguridad ciudadana y sobre el conjunto de la sociedad democrática.

Las situaciones descritas han dificultado poder lograr una definición de estos actos en un solo concepto de terrorismo, por lo que los intentos han sido complicados y los resultados medianamente fructíferos.

En 1972 la Asamblea General de las Naciones Unidas estableció un comité ad hoc para estudiar al terrorismo. Durante las primeras discusiones en busca de un consenso para lograr una definición única se observó que cierto tipo de acciones caracterizadas como terroristas tenían diferentes orígenes y facetas.

Algunos intentos de definición sobre este término enfatizaron la relevancia del "blanco prohibido"; otros apuntaron a los propósitos de la acción, y otros más pensaron que las características del autor eran un factor importante para ser incluidas de manera determinante en la definición.

Por lo anterior, tomar rehenes, piratería en aeronaves, sabotajes, asesinatos, amenazas, bombardeos indiscriminados o tiroteos, han sido vistos por algunos como actos de terrorismo. Pero cabe hacer notar que al mismo tiempo no todos los asesinatos, amenazas o tiroteos, quien quiera que los haya ejecutado, son terrorismo. Parece que mientras estos actos pueden constituir terrorismo, la característica que los podría definir como tales depende de otros factores también, por lo que el terrorismo no puede ser definido sólo por la referencia única de los actos cometidos.[191]

El propósito o el motivo de los actos o agresiones es obviamente un elemento clave para el entendimiento del concepto de terrorismo. Casi todos comparten el sentimiento de que para un terrorista el objetivo es provocar miedo o ansiedad intensa para forzar al objetivo primario a una conducta, en conexión con el poder político demandado.[192]

Los agentes que producen los actos terroristas han tendido en la actualidad a una mayor espectacularidad, por su casi premeditada y segura exhibición de los efectos a través de los medios de comunicación, sin acuerdo previo entre aquéllos y éstos, en usufructo de los valores imperantes en la sociedad y, por ende, en los mismos medios; altamente indiscriminados, porque las víctimas de los actos terroristas son ya generalmente otras personas y los mismos terroristas, en una táctica de guerra total y cuyos efectos alcanzan cada vez a más personas.

Su organización es por células no numerosas, no mayores a tres integrantes que no se conocen entre unas y otras, su organización es altamente difusa y no reivindicatoria, lo que

[191] *Cfr*. Higgins, Rosalyn, *The General International Law of Terrorism*, en Higgins, Rosalyn y Flory, Maurice, Terrorism and International Law, Nueva York, Routledge, 1997, p. 15.
[192] *Cfr. ídem.*

multiplica su efecto atemorizante en la sociedad. Además son grupos cada vez más impotentes frente a las instituciones legalmente constituidas, y por ende sus reacciones son cada vez más circunscritas a los actos fanáticos, donde impera el móvil emocional.

Ciertas características identificadas por los estudiosos del tema han hecho posible discernir cuáles son los actos que pueden ser considerados como terroristas, de otros que no lo son, por ejemplo:

- Los motivos del autor de la agresión han de ser más ideológicos que de beneficio personal, y la selección ideológica de sus objetivos no necesariamente guarda una relación con el propósito último, además de buscar con el hecho la promoción pública de su reclamo, lo que no es así para el caso del criminal común. El daño que resulta a las vidas o propiedades no presenta ningún beneficio personal para el agresor motivado ideológicamente.
- El resultado deseado y buscado por el agresor usualmente es la difusión de una queja a través de un daño causado. El agresor sopesa los riesgos en que incurre al perpetrar ciertos actos que irán contra la meta última que busca lograr, o en contra de otros beneficios políticos o ideológicos que podría obtener por otra vía, y que no son necesariamente inherentes al objetivo primario. En contraste, el criminal común sopesa los riesgos que corre en contra de los beneficios materiales inmediatos que puede obtener del mismo acto.
- El daño resultante de un cierto acto puede tener una importancia menor en el proceso de decisión del agresor, a diferencia del caso del criminal común. Como resultado directo, el terrorista usualmente perpetrará el acto de una manera diseñada para asegurar un efecto máximo con relación a su meta, sin importar la dimensión del daño.[193]

Debe destacarse aquí, el punto de vista de los Estados en los foros internacionales, sobre cómo definir al terrorismo y sus características, lo cual dio como resultado que en 1979, cuando el comité ad hoc de Naciones Unidas reportó a la Asamblea General sus conclusiones,[194] evitara incluir una definición, a pesar de que distintos representantes habían propuesto sus parciales puntos de vista sobre el tema, donde si bien, los líderes de las economías desarrolladas estaban tensos por definir un terrorismo que incluyera el concepto de "Estados terroristas", los

[193] *Cfr*. Bassiouni, M. Cherif, *International Terrorism*, p. 782.
[194] 28 sesión/A/9028, 1973

representantes de los países del tercer mundo estaban inquietos de una definición que pusiera un mayor peso sobre ciertos participantes, no pertenecientes al Estado, sin diferenciar entre el terrorismo, propiamente, y una lucha de clase por la liberación nacional.

Las principales características de los terroristas, así como los actores pertenecientes a estos son:

- Su violencia indiscriminada: extiende sus efectos a la totalidad de la población.
- Su imprevisibilidad: actúa con sorpresa infundiendo terror.
- Su inmoralidad produce sufrimiento innecesario: golpean las áreas más vulnerables.
- Es indirecto: desvía la mirada de la población a un punto, que no es el blanco que se proponen.
- El escape de la religión y en alguna medida del nacionalismo y sus conceptos básicos, producto de la Globalización que desconoce fronteras.
- El auge de la toma de rehenes y escudos humanos.
- El Terrorismo por cuenta propia que tiene como blanco a la población civil.
- Participación creciente de militares, ex – militares, y miembros de los servicios de inteligencia.

De la misma manera, diversos motivos inspiran a los terroristas. Los estudiantes del terrorismo los clasifican en tres categorías: racional, psicológico, y cultural. Un terrorista puede ser formado por una o diversas combinaciones de éstos.

En un primer término tenemos la motivación racional,[195] que es cuando el terrorista piensa con sus metas y opciones, haciendo un análisis de costes y beneficios, intenta determinarse si hay maneras menos costosas y más eficaces de alcanzar su objetivo más que provocar el terrorismo. Para evaluar el riesgo, pesa las capacidades defensivas del blanco contra sus propias capacidades para atacar. Mide las capacidades de su grupo para sostener el esfuerzo. La pregunta esencial es si el terrorismo trabajará para el propósito deseado, dado condiciones sociales en ese entonces. El análisis racional del terrorista es similar al de un comandante militar o de un empresario de negocio que considera líneas de conducta disponibles.

La motivación psicológica[196] para el terrorismo, es otro elemento que inspira a los terroristas y se deriva del descontento personal de este con su vida y las realizaciones, encuentra

[195] Walter Laqueur, *op. cit*., p. 156.
[196] *Ibídem*, p. 158.

su razón en la acción dedicada del fanatismo, no considera que puede ser incorrecto y que su visión puede tener cierto mérito. Los terroristas tienden a crear polarizaciones para proyectar sus propias motivaciones antisociales sobre otras, atribuyen solamente motivos malos a cualquier persona exterior a su propio grupo. Esto permite a los terroristas deshumanizar a sus víctimas y quitar cualquier sentido de la ambigüedad de sus mentes. La claridad que resulta del propósito suprime a las que anhelen violencia para relevar su cólera constante. La otra característica común del terrorista psicológicamente motivado es la necesidad pronunciada de pertenecer a un grupo. Con algunos terroristas, la aceptación del grupo es un motivador más fuerte que los objetivos políticos indicados de la organización. Tales individuos definen su estatus social por la aceptación del grupo.

Los grupos terroristas con motivaciones internas fuertes encuentran necesario la existencia de un grupo, donde, como mínimo, debe cometer actos violentos para mantener autoestima del grupo y legitimidad. Así, los terroristas realizan a veces los ataques que son objetivos no productivos o aún ineficaces a su meta anunciada.

Otro resultado de la motivación psicológica es la intensidad de la dinámica del grupo entre terroristas. Tienden a exigir unanimidad y son intolerantes a la disensión. Con el enemigo claramente identificado e inequívoco mal, la presión de extender la frecuencia y la intensidad de operaciones está siempre presente. La necesidad de pertenecer al grupo desalienta dimisiones, y el miedo del compromiso rechaza su aceptación. Se rechaza el compromiso, y los grupos del terrorista se inclinan hacia posiciones del maximalista. Esto puede explicar porqué los grupos terroristas son propensos a fracturarse.

La motivación cultural[197] deriva de que las culturas forman valores y motivan a gente a las acciones que se parecen no razonables a los observadores no nativos. El tratamiento de la vida general e individual en detalle es una característica cultural que tiene un enorme impacto en el terrorismo. En las sociedades en donde la gente se identifica en términos de la calidad de miembro de grupo (familia, clan, tribu), puede haber una buena voluntad para sacrificarse. Ocasionalmente, los terroristas parecen ser impacientes para dar sus vidas por su organización y causa. Otros factores incluyen la manera en la cual se acanala la agresión y los conceptos de la organización social. Algunos sistemas políticos no tienen ningún medio no violento eficaz para que la sucesión accione.

[197] Walter Laqueur, *op. cit.* p. 161.

Un motivo cultural importante del terrorismo es la opinión y anticipación de una amenaza a la supervivencia étnica del grupo. El miedo de la exterminación cultural conduce a la violencia. Todos los seres humanos son sensibles a las amenazas a los valores por los cuales se identifican, estos incluyen el lenguaje, la religión, la calidad de miembro de grupo, y el territorio del nativo. La posibilidad de perder cualquiera de éstos puede accionar la defensiva.

La religión puede ser la más volátil de identificadores culturales porque abarca los valores llevados a cabo profundamente. Una amenaza para su religión pone no solamente el presente en riesgo sino también su fin cultural y el futuro. Muchas religiones, incluyendo cristianismo e Islam, han utilizado la fuerza para obtener a convertidos. El terrorismo en el nombre de la religión puede ser especialmente violento.

3.3. Tipos de terrorismo

El clasificar algo tan complejo como el terrorismo es una tarea extremadamente difícil y casi imposible, ya que cada definición o tipo es diferente de acuerdo al punto de vista de las diferentes sociedades, religiones y sistemas políticos en el mundo y muchas veces se traslapan. Los tipos de terrorismo pueden ser clasificados de acuerdo a la naturaleza de sus ataques y sus perpetradores y sus victimas, etc.

En general se clasifica al terrorismo en tres grandes grupos:[198]

- Terrorismo Nacionalista
- Terrorismo de Estado y
- Terrorismo Global

Los primeros dos tipos, terrorismo nacionalista y de Estado, son los tipos tradicionales de terrorismo. El tercer tipo, el terrorismo global, se ha vuelto especialmente significativo en tiempos recientes, especialmente después de los sucesos del 11 de septiembre de 2001. Sin embargo, con la cada vez mayor importancia del terrorismo global y las tecnologías que han permitido el surgimiento de varios derivados del terrorismo global, surgen diversas clasificaciones, incluyendo terrorismo bioquímico, ciberterrorismo, narcoterrorismo, terrorismo nuclear, etc.

Así tenemos que el **Terrorismo Nacionalista** es aquel donde los perpetradores son individuos o grupos con fuertes ideas y metas nacionalistas. Ellos desean establecer un estado

[198] *Ibídem*, p. 195.

independiente, o tomar control de cierta región o país y a veces derrocar el gobierno de un país o lograr la completa abolición de un sistema político para reemplazarlo por otro, o simplemente abandonarlo a favor de otro.[199]

Por su parte el **Terrorismo de Estado**[200] es definido como el uso sistemático, por parte del gobierno de un Estado, de amenazas y represalias, considerado a menudo ilegal dentro incluso de su propia legislación, con el fin de imponer obediencia y una colaboración activa a la población. Por su naturaleza es difícil de identificar, y los conceptos varían en función del carácter de las épocas históricas, zonas geográficas y características culturales. Los regímenes despóticos del pasado utilizaban con frecuencia prácticas de este tipo, que las democracias modernas condenarían sin necesidad de realizar una crítica contemporánea rigurosa.[201]

Estos regímenes totalitarios se caracterizaban por un monopolio de los medios de comunicación, la imposición de una ideología monolítica, la exigencia no sólo de obediencia sino de participación activa en las medidas policiales del Estado, y un aparato de policía secreta y de campos de concentración para disciplinar e incluso exterminar a los adversarios y disidentes. Los líderes potenciales de la oposición eran aislados, encarcelados, exiliados o asesinados.

Los componentes de muchas organizaciones nacionales de seguridad e información han utilizado métodos ilegales para hacer frente a los adversarios, tanto dentro como fuera del país. Lo que diferencia estos episodios de un sistema donde se aplica el terrorismo de Estado es la importancia de la operación y el total respaldo de la clase dirigente. En efecto, el aparato de terror, el Estado y el partido en el gobierno suelen estar relacionados de un modo indisociable. El sistema acaba destrozando a menudo a los elementos de su propia cúpula.

En otro plano, algunos regímenes han recurrido a medios extralegales para eliminar a elementos específicos de la población, en especial en lo que a proscritos y presuntos delincuentes se refiere.

---

[199] Tal es el caso de ETA en España o Sendero Luminoso en Sudamérica. En el caso del Ejercito Revolucionario Irlandés (ERI) en el Norte de Irlanda, ellos desean liberar a Irlanda del Norte del dominio británico y son un buen ejemplo de terrorismo nacionalista, así como el grupo de Irlandeses Leales, quienes tienen exactamente metas opuestas a las del ERI. Desafortunadamente, ambos lados de este conflicto han causado, en el pasado, la perdida de numerosas vidas humanas. Los Tigres de la Liberación del Tamil Eelam, quienes desean establecer un estado independiente en Sri Lanka, HAMAS y Euskadi Ta Askatasuna (ETA) en España, son también buenos ejemplos de grupos terroristas nacionalistas activos hoy en día.

[200] También conocido como Terrorismo de Anti-Establecimiento.

[201] Las formas más desarrolladas de terrorismo de Estado, para las que el término fue inventado, han sido los sistemas empleados en el siglo XX bajo el fascismo y el comunismo. Asimismo, la práctica de terror desde el poder se extendió en el siglo XX bajo regímenes militares o militarizados en el seno de democracias formales.

Una variación del Terrorismo de Estado es el Terrorismo Apoyado por el Estado, en el cual grupos terroristas son protegidos o patrocinados por el gobierno y se involucran en ataques violentos y opresión general sobre la población de un país.[202]

En lo referente al Terrorismo Global,[203] comienza a tomar forma en la década de los 90, teniendo su efecto más devastador en Estados Unidos el 11 de septiembre de 2001. Esta forma de terrorismo ha dado lugar a numerosos derivados como el ciberterrorismo, el terrorismo bioquímico, el narcoterrorismo, el terrorismo nuclear, el ecoterrorismo, etc.

Este tipo de terrorismo no conoce fronteras, sus metas son internacionales y los culpables trabajan desde diferentes partes del mundo por una causa común, están íntimamente interconectados, y toman ventaja de los últimos avances tecnológicos en los medios de comunicación.

Ellos atacan indiscriminadamente, utilizando tácticas muy violentas, causando la perdida de muchos miles de vidas inocentes. Los principales blancos no son sus victimas directas, por el contrario, ellos desean intimidar a la población y a los gobiernos al causar daños a sectores vulnerables o al atacar símbolos nacionales o importantes para una nación.

Los terroristas globales atacan de una manera altamente organizada y cuidadosamente planeada, tienen vínculos y son apoyados y patrocinados por muchas organizaciones criminales. Estos grupos internacionales de terroristas buscan causar el impacto mas fuerte posible para capturar la atención de los medios de comunicación y diseminar así el terror en la población.

Este tipo de terrorismo es el mas prominente en tiempos modernos y dentro de el podemos incluir a varios subtipos de terrorismo y clasificarlos a su vez de acuerdo a diferentes criterios, porque aunque todos los tipos comparten ciertas características, difieren en las tácticas que emplean, en sus objetivos, su metas, su creencias religiosas, etc.

A continuación se hará una breve descripción de las nuevas formas de terrorismo:

Terrorismo bioquímico: Los terroristas han utilizado agentes biológicos que se dispersan rápidamente por aire o agua, o que pueden contaminar productos comestibles y causar terribles enfermedades. La diseminación deliberada de agentes biológicos como bacterias o virus que son capaces producir enfermedades graves y a veces la muerte en sus formas naturales, pero mas frecuentemente alterados selectiva o genéticamente, se define como “Bioterrorismo”. Los bioterroristas no solo tienen como blanco a grandes masas poblacionales sino que también atacan

[202] El Reino del Terror en Francia y el Holocausto en Alemania son considerados, por algunos, como buenos ejemplos de Terrorismo de Estado en la historia.
[203] Walter Laqueur, *op. cit.*, p. 199.

grandes e importantes reservas de recursos como agua o productos comestibles, también pueden atacar al ganado o a cultivos, pudiendo causar epidemias incontrolables que también pueden ser transmitidas a los humanos. Asimismo, las Armas Biológicas, pueden ser clasificadas en tres grupos, de acuerdo a su toxicidad:

- **Categoría A:** Este tipo representa el riesgo mas alto para la seguridad pública, porque son organismos que se transmiten fácilmente por tacto o inhalación y requieren atención medica especializada, ya que causan enfermedades graves y casi siempre, la muerte.
- **Categoría B**: Son menos fáciles de diseminar, causan enfermedad moderada y menos muertes.
- **Categoría C**: Estos agentes son mas peligrosos que las dos categorías anteriores, no porque puedan causar un mayor numero de muertes o porque produzcan enfermedades graves, sino por el hecho de que son microorganismos que son fáciles de obtener y son objetos ideales para experimentos de ingeniería genética, que pueden ser producidos masivamente y pueden constituir una gran amenaza para la salud publica.

Algunos de los organismos en las tres categorías son considerados todavía más peligrosos porque la victima no muestra ningún síntoma hasta días después de haber contraído la enfermedad, haciendo más difícil la tarea de salvarle la vida al paciente en etapas muy avanzadas de la infección.

Las enfermedades más importantes causadas por Bioarmas son: viruela, Peste Neumónica, Botulismo, Tularemia y Ántrax.

Otra definición es el **Terrorismo Químico**, que es el uso de substancias químicas como armas por individuos o grupos para amenazar, perjudicar o matar a victimas inocentes en el intento de alcanzar una meta política, ideológica o religiosa.[204] Predecir un ataque tal es casi imposible.

Otra gran preocupación es la de la posibilidad que un grupo terrorista disperse o disemine un agente contaminante en alimentos o reservas de agua, lo cual traería trágicas consecuencias.

[204] En el pasado, han habido varios ejemplos de este tipo de ataque, uno de los más conocidos es el ataque con gas sarín en el metro de Tokio en 1995 que causo una docena de muertes y cientos de personas tuvieron que ser atendidas medicamente.

Este tipo de terrorismo puede ser devastador ya que es muy difícil de controlar y el ataque mismo tiene una mayor duración y efecto que el de un ataque de bomba.[205]

Los terroristas pueden hacer uso de agentes químicos peligrosos que son desarrollados como armas, pero también pueden utilizar químicos mas fácilmente accesibles que se utilizaron en diferentes industrias y laboratorios comerciales.[206]

Entre los principales tipos de Armas Químicas encontramos las siguientes: Cloro, Fosgeno, Gas Mostaza, Tabun,[207] Sarín,[208] Soman,[209] Cianuro de Hidrogeno, Metales Pesados como el arsénico, el plomo y el mercurio. También existen otros compuestos, incluyendo volátiles que son usados como armas, similares al cloro y al fosgeno, por ejemplo el benceno, el cloroformo y algunos trihalometanos. Pesticidas y oxidantes, ácidos corrosivos como los ácidos nítrico y sulfúrico y venenos industriales, tanto en forma liquida como gaseosa, como los cianuros y los nitrilos e incluso combustibles industriales como el propano y el petróleo. Todos han sido exitosamente usados como armas químicas que han causado las muertes de muchas personas.

Nuevas substancias químicas son sintetizadas a un paso acelerado en diferentes países, generalmente con propósitos médicos o industriales, pero que podrían ser potencialmente peligrosas en caso de que caer en manos de los terroristas. Es por esto que las agencias gubernamentales deben monitorear cuidadosamente las actividades de compañías y laboratorios

---

[205] En 1997, la Organización para la Prohibición de Armas Químicas (OPAQ), fue formada para asegurar el cumplimiento de las metas propuestas durante la Convención de Armas Químicas (CAQ). De acuerdo al sitio de Internet de la OPAQ, esta organización esta "Dedicada, por el bien de la humanidad, a excluir completamente la posibilidad de el uso de armas químicas..." En efecto, su principal objetivo es el de controlar y eventualmente prohibir completamente la producción e intercambio de sustancias químicas peligrosas usadas con propósitos industriales y médicos, con el fin de mantenerlas lejos del alcance de grupos terroristas. Esta organización también intenta destruir sustancias químicas existentes, almacenadas como armas o que podrían ser almacenadas como armas. Todo esto apoyado por solidas leyes que deben ser reforzadas en todos los países del mundo.

[206] Para la prevención y ayuda en caso de un ataque químico terrorista, es necesario que todos los gobiernos mantengan infraestructuras fuertes de salud pública y manejo de emergencias para que sea posible ofrecer ayuda rápida a las victimas de un ataque químico terrorista. Todo esto con la cooperación de los departamentos de seguridad e inteligencia del gobierno de cualquier nación.

[207] El Tabun es un agente neurotóxico (etilo-N, N-dimetilfosforamidocianidato) que entra al cuerpo a través del sistema respiratorio y también cutáneamente. Afecta el control muscular, causando la muerte por asfixia. Fue descubierto en 1936 y fue producido masivamente por el ejército Nazi. Mas tarde fue usado por Saddam Hussein contra Irán.

[208] Otro agente neurotóxico (isopropilo metilfosfanofluoridato). Es bastante más potente que el Tabun. El sarín fue descubierto en 1938 y fue producido masivamente por el ejército Nazi. Tiempo después fue utilizado por Saddam Hussein contra Irán y más recientemente, por la secta Aum Shinrikyo, en el ataque químico del metro de Tokio en 1995 que lleno las primeras paginas de los periódicos del mundo entero.

[209] También una substancia neurotóxica (pinacolylo metilo fosfonofluoridato), es aun mas potente que Tabun y sarín. Soman fue descubierto en 1944 por científicos Nazis y fue posteriormente desarrollado como un arma química durante 1952-1956 por químicos de los Estados Unidos y el Reino Unido. Es sin duda alguna el mas letal de todos los agentes neurotóxicos. Fue usado por Saddam Hussein en la guerra contra Irán en la década de 1980.

que desarrollan estas substancias y los sistemas legales de todos los países deben estar preparados para controlar su tráfico y uso.

Otra forma de terrorismo es el **Terrorismo nuclear,**[210] donde invariablemente, la seguridad en todos los países del mundo se vería seriamente amenazada si armas nucleares o aparatos de dispersión radiológica (ADR) cayeran en manos de grupos terroristas violentos. Existe actualmente un mercado negro para materiales radioactivos que podrían ser usados para manufacturar armas peligrosas, también, la información necesaria para construir dichos aparatos como los ADRs es fácilmente accesible en bases de datos en línea que casi cualquier persona puede revisar anónimamente desde la biblioteca de una universidad. Más información puede ser intercambiada en mensajes encriptados por medio de Internet.

Hasta hoy, no existe evidencia de grupos terroristas conocidos adquieran o manufacturen estos materiales o armas, o que tengan en su poder información o armas ya ensambladas. Un ataque terrorista que utilice un ADR, en contraste, causaría una menor perdida de vidas, pero causaría un impacto mucho mayor debido al hecho de que un área mucho mayor es afectada y que puede ser estratégicamente elegida para atraer la mayor atención posible, aunque el daño material sea considerablemente menor.

Otra arma comúnmente usada por terroristas nucleares es el Aparato de Dispersión Radiológica (ADR), el cual esta diseñado para esparcir materiales radioactivos sobre grandes aéreas, no causa danos materiales, pero afecta el medio ambiente y la zona afectada se vuelve inhabitable, siendo necesario llevar a cabo un operativo de limpieza masivo, que puede costar desde miles a millones de dólares dependiendo del tamaño de la zona afectada.

La construcción de un ADR es considerablemente mas sencilla que la construcción de un AEN, y en algunos casos, es un arma mas efectiva para atraer la atención de las autoridades y ejercer presión sobre ellas, ya que el resultado de un ataque radiológico es mas difícil de predecir y contamina grandes aéreas. Los terroristas tienen fácil acceso a radioisótopos que pueden encontrarse en muchos objetos caseros y crear dispositivos radiológicos que pueden causar serios danos en aéreas urbanas y todos los efectos son muy difíciles de predecir y controlar ya que están influenciados por factores ambientales como el viento, la temperatura, la humedad, etc. En este caso los atacantes buscan crear un fuerte impacto psicológico en la población y llamar la atención de los medios y el gobierno, para alcanzar sus metas, las cuales pueden ser de varios tipos:

[210] Walter Laqueur, *op. cit.*, p. 201.

derrocar a un gobierno, iniciar una Guerra civil y atacar o destruir un sistema percibido como contrario a las creencias de los terroristas.

El **Ecoterrorismo** ha ocupado un lugar prominente en los medios de comunicación en años recientes. Además de historias de incendios y bombardeos perpetrados por reconocidos terroristas que aparecen en los principales periódicos en todos los países del mundo, han aparecido muchos libros sobre el tema. Existen muchas definiciones de ecoterrorismo, y la mayoría de ellas tiende a ser controversial, por ejemplo: "Amenazas y actos de violencia en contra de personas y propiedades, vandalismo, sabotaje e intimidación, cometidos en el nombre del ambientalismo",[211] por su parte el FBI lo define como "El uso o amenaza de uso de violencia de naturaleza criminal en contra de victimas inocentes o en contra de propiedades, por un grupo orientado al ambientalismo."[212]

Los blancos de los ecoterroristas son variados e incluyen: compañías automovilísticas, compañías madereras, laboratorios de investigación medica tanto privados como de universidades, peleteros, cazadores y pescadores deportivos, incluso granjeros y pescadores comerciales, deportistas extremos, circos, zoológicos, rodeos y en general consumidores de animales como alimento, vestimenta, medicina u otros servicios, incluyendo el entretenimiento.

Por otro lado el término **Narcoterrorismo** es usado para describir las actividades de conocidas organizaciones terroristas, las cuales obtienen fondos a través del narcotráfico, pero el termino tuvo sus orígenes a principios de la década de 1980, cuando el entonces presidente de Perú Belaunde Terry lo utilizo por primera vez para describir los ataques devastadores en contra de su policía de narcóticos por traficantes Peruanos y de otros países Latinoamericanos vecinos.

Algunas veces las organizaciones terroristas son apoyadas y patrocinadas por grupos narcotraficantes que pueden perpetrar ataques y otros crímenes y en general causar perjuicio a civiles y llamar la atención de las autoridades y grupos protectores de la ley.[213]

La utilización del tráfico de drogas para alcanzar ciertas metas por organizaciones o grupos terroristas. El Narcoterrorismo es un crimen que afecta a los derechos humanos y a la paz

[211] En http://attila.inbio.ac.cr:7777/pls/portal30/ [consultado el 17 de enero de 2007]
[212] En http://www.fbi.gov Sección de Terrorismo Domestico del FBI
[213] Para mediados de la década de los 80s, el narcoterrorismo ya estaba siendo activamente combatido por los Estados Unidos, quienes iniciaron una serie de operaciones militares para intentar ejercer control sobre el fuerte cartel de cocaína Colombiano Medellín, dirigido por Pablo Emilio Escobar, conocido en los medios de comunicación como "El Rey Coca". Este grupo de narcotraficantes, proveía fondos para terroristas Colombianos que a su vez causaron innumerables muertes a través de cierto número de ataques dirigidos por Escobar, quien se rindió ante las autoridades Colombianas en 1991.

mundial entre otros importantes valores humanos. Las porciones más jóvenes de la población son las más afectadas por el uso de las drogas, lo cual los lleva a la violencia y al crimen. Organizaciones narcoterroristas, en consecuencia, utilizan a personas jóvenes como un arma.

3.4. Los medios de comunicación como factor que facilita el terrorismo.

La violencia mediática es hoy tan frecuente que cualquier atrocidad imposible de soportar en nuestra vida cotidiana se hace tolerable e incluso indiferente si llega a nosotros a través de los medios de comunicación. Esta aparente paradoja solo es concebible en una sociedad como la nuestra, una sociedad del espectáculo en la que apenas nada puede sorprendernos y, al mismo tiempo, cualquier sorpresa sólo puede llegar desde los medios.

Es aquí donde se inserta un nuevo terrorismo; nuevo no en cuanto a su origen, postrero y harto experimentado, sino en su forma de actuar, que aprovecha las oportunidades que le brinda la red mediática para rentabilizar al máximo sus acciones.

Sus dos pilares fundamentales de actuación son su nueva estructura en red y el aprovechamiento de la fuerza de la representación que le ofrecen los canales de comunicación. En el primer caso, la estructura en red, le brinda a la organización terrorista la posibilidad física de llevar a cabo un atentado de grandes dimensiones. En segundo lugar la representación mediática ha traído consigo una nueva configuración de la realidad que es ahora un híbrido de elementos efectivos y ficticios al mismo tiempo; los terroristas aprovechan el enorme potencial de los medios para dar a sus acciones un carácter de inmediatez y universalidad como nunca se había conocido antes.

La propagación de las estructuras en red y sus tecnologías acarrea algunos riesgos y peligros debido a que están utilizándose para crear amenazas a la libertad y a la intimidad. En una guerra en red arquetípica, las unidades se asemejarán a una variedad de *nodos* (células terroristas) dispersos e interconectados preparados para actuar como una red multicanal. Esta nueva forma de estructuración permite al terrorismo organizado actuar cada vez más a través de fluidas redes en lugar de hacerlo a través de jerarquías más formales. Las organizaciones terroristas presentan estructuras más fragmentadas y más caóticas que incluyen también redes de influencia. Un nuevo sistema bélico que aporta muchos beneficios a organizaciones pequeñas unidas por un mismo objetivo o ideal común.

Las redes no son exclusivas de las organizaciones terroristas; son una de las formas de organización social más comunes. Se caracterizan por no ser un tipo de organización exclusivo, y con frecuencia existen en el interior de estructuras jerárquicas más tradicionales. Aportan a las organizaciones una sensación de omnipresencia y son capaces de coexistir dentro y fuera de jerarquías aumentando así su eficacia. Las redes pueden variar en tamaño, forma, pertenencia, cohesión y propósito. Facilitan los flujos de información, conocimiento y comunicación, así como los de productos más tangibles. Pero en la actualidad, a medida que las comunicaciones se han abaratado y simplificado, las redes han sufrido una rápida expansión como forma de organización ya que; "las redes tecnológicas facilitan la actuación de redes sociales mayores y más dispersas y pueden incluso servir como un multiplicador de fuerzas decisivo para ciertas clases de redes sociales."[214]

En un momento histórico donde la supremacía militar de las Naciones Unidas no ofrece opciones a una confrontación bélica convencional, las redes proporcionan a los terroristas diversidad, flexibilidad, poca visibilidad y pervivencia, actuando de forma clandestina y no mostrando centros de poder obvios. Los terroristas pueden trasladarse con facilidad en áreas de alto riesgo frente a las fuerzas del orden. Del mismo modo ofrecen oportunidades para la redundancia y la resistencia de forma que incluso si se destruye una parte de ella, la red puede seguir actuando. Las redes, como organizaciones, son muy resistentes y pueden reconstruirse fácilmente de modo que la degradación de una red no conduce necesariamente a su defunción. Lo cual permite a las células terroristas permanecer dormidas despistando la sospecha policial sin reducir por ello su capacidad de actuación. La velocidad, comodidad y anonimato de las formas de comunicación que ofrecen las nuevas tecnologías les posibilita una reactivación de la red en un tiempo reducido.

Aunque es evidente que el aprovechamiento de las tecnologías de la información no es prerrogativa única de las organizaciones en red las redes se encuentran extraordinariamente bien situadas para aprovechar las nuevas oportunidades tecnológicas. La realidad es que muchas organizaciones criminales han utilizado la tecnología como fuerza multiplicadora para desarrollar sus actividades emprendedoras con mayor eficiencia a menor costo.[215]

Ahora bien, en el caso de los medios de comunicación se sustituye la percepción sensorial directa de los acontecimientos por parte de la población por una percepción "dirigida", sesgada y

[214] P. Williams, *Redes transnacionales de delincuencia* en Arquilla, J. y Ronfeldt, D., *Redes y guerras en red. El futuro del terrorismo, el crimen organizado y el activismo político*, Madrid, Alianza editorial. 2003, p. 92
[215] *Ibidem*, p. 94.

seleccionada por uno o más grupos de poder, aquellos que controlan los medios, que trasladan la realidad como tal a un constructo homogéneo que ha de ser consumido por todos por igual.

Esta mediación es en cierto modo inevitable ya que una razón meramente física (el hombre no puede asistir in presentia a todos los acontecimientos mundiales por razones lógicas) es la culpable de que deban existir medios de canalización que hagan llegar la información al máximo número de puntos del planeta. El problema no se localiza en la existencia de esas vías, sino en el uso que se hace de ellas. En este sentido, la mejor forma de entender la mediación es como un proceso que permite dar sentido al mundo a través de diversos medios de expresión e interacción y que tiene el potencial de configurar y transformar la actividad social.[216]

En los medios de comunicación la imagen sustituye a la imaginación y el imaginario del medio al imaginario del individuo. Tras lo dicho puede advertirse que la representación actual en los medios de comunicación lleva consigo un proceso de "vacio" de lo que podría suceder en la representación de individuos actualizados en la realidad efectiva. La principal divergencia entre la representación de estos y de los individuos ficticios radica en el hecho de que en el primer caso los receptores del discurso mediático aceptan la posibilidad de que los individuos que forman parte de ese discurso puedan integrarse en su modo de percepción externa, mientras que en el segundo caso el individuo ficticio no es concebido como parte de ese modo de percepción.

Por lo tanto, en este nuevo discurso mediatizado el receptor deposita su confianza en lo que se le está contando, que sustituye como hemos comentado su propia percepción directa de los hechos por una simple imposibilidad física, y esto tiene una consecuencia de crucial importancia: el receptor modifica su conducta en función de esta percepción mediatizada, debido a que

Ya no es el mundo que se hace imagen (sociedad mediatizada) sino el imaginario que se hace mundo (sociedad mediática). Un imaginario que, mezclando ficción y realidad, se incorpora al funcionamiento interno de las organizaciones y modifica en profundidad todas las relaciones interpersonales, se acaba por crearlo y prolongarlo.

Estas capacidades de los medios de comunicación se traducen en ciertos factores. Por un lado, el tiempo real puesto que las tecnologías de la comunicación lo vuelven todo presente. Se inaugura el reino de lo inmediatico, donde la representación se impone como referencia inmediata; se establece de esta forma una nueva relación con la realidad, más próxima, en la que

[216] R. Mansell, *La revolución de la comunicación. Modelos de interacción social y técnica*, Madrid, Alianza editorial, 2003, p. 156.

esta última está al alcance de la mano. Los mass media están asumiendo hoy la realidad social; el efecto de directo, la realidad inmediatica que sustituye a la realidad misma y puede tener más efectos que un acontecimiento real.

Esta situación nos desvela que vivimos en una era de riesgo que es global, individualista y más moral de lo que suponemos. La globalización y la extensión de las redes de comunicación instantáneas implican el debilitamiento de las estructuras estatales; de la autonomía y del poder del estado.

Allí donde las antiguas distancias de tiempo producían, hasta la revolución de los transportes del siglo pasado, el alejamiento propicio entre las distintas sociedades, en la era actual de la revolución de las transmisiones, el incesante feed-back de las actividades humanas engendra la amenaza invisible de un accidente.

El marco de la sociedad del riesgo conecta áreas que hasta hoy habían sido inconexas. Sigue siendo muy difícil predecir exactamente cómo se desbordarán en cada país en concreto los nuevos riesgos sociales y políticos. Pero muchos sostienen ahora que el riesgo de una reacción contra Occidente que se manifiesta ahora a través del terrorismo internacional, sobre todo el islámico.

Los riesgos se han convertido para los estados en una de las principales fuerzas de movilización política, y las organizaciones terroristas lo saben, por este motivo utilizan sus redes de células terroristas y las dinámicas de representación de la sociedad del espectáculo como armas de riesgo en su lucha armada.

En la sociedad del riesgo, áreas de intervención y acción política que aparentemente carecen de importancia están cobrando extraordinaria relevancia, y cambios menores están induciendo transformaciones básicas en el juego de poder de la política del riesgo global. Por este motivo, el concepto de “sociedad del riesgo global”, llama la atención sobre la controlabilidad limitada de los peligros que nos hemos creado.

Esta encrucijada que vincula y distancia a la vez a los medios de comunicación con el terrorismo plantea condicionamientos inseparables de su condición de organismos libres en medio de una sociedad democrática que se enfrenta a una de sus peores lacras, posiblemente uno de los problemas más graves de las futuras décadas para todos los países, los países desarrollados y los países en vías de desarrollo, ya que el terrorismo no distingue muchas veces de condiciones económicas sino de condiciones sociales.

3.5. Terrorismo informático. Antecedentes, conceptos y características.

Con el surgimiento de las tecnologías de información también se abrió una compuerta para la comisión de delitos a través de las mismas. Históricamente las leyes penales surgen como una respuesta a las actividades que producen daño a la sociedad y con la aparición de los computadores, comenzaron nuevos delitos y la preocupación por castigar ciertas conductas, recibiendo el nombre de Delitos Informáticos.

El desarrollo de la Informática y la incorporación de la misma a nuestra vida cotidiana, ratifica su presencia en la mayoría de los países incluyendo hasta los del tercer mundo a nivel gubernamental. Las telecomunicaciones se están moviendo rápidamente hacia la Internet como canal preferencial. La globalización ha encontrado un mecanismo de facilitación en la Internet y el comercio se orienta hacia la conexión directa con los consumidores gracias a ella. En la administración de empresas es una meta llegar a la oficina sin papeles y el trabajo telemático desde casa se hace una clara opción para la reducción de costos.

El desarrollo de las nuevas tecnologías informáticas ha cambiado los medios de registro y archivo de la actividad humana. Las computadoras son los cuadernos y agendas de esta nueva era de la información. Gran cantidad de documentos son elaborados digitalmente en computadores para ser posteriormente impresos.

El correo convencional está siendo sustituido a pasos agigantados por el correo electrónico. Las redes de informática permiten nuevos tipos de publicaciones virtuales sin tinta. Las tecnologías de información están ganando cada día preponderancia en las operaciones de control de sistemas administrativos, de seguridad y vigilancia. La tecnología militar en la actualidad depende en gran parte de la informática, así como los mecanismos de preservación y análisis de información de seguridad. Internet, la Red de redes nació de la idea y de la necesidad de establecer múltiples canales de telecomunicación entre computadores.

En caso de un ataque nuclear que eliminara líneas de conexión existentes, se utilizarían medios alternos de conexión informática in importar la ruptura de otras líneas o canales de conexión.

En el ciberespacio, se desarrollan nuevas formas de transmisión y recuperación de la información, que permiten al menos en teoría, que el terror ejercido por fanáticos de todo tipo pero con talento informático, se pueda ejercer con una eficacia y profundidad nunca vista antes.

Es posible, que el horror desencadenado por atentados explosivos puedan parecernos en un futuro no muy lejano, un incidente menor (en cuanto a su espectacularidad, no en el dramatismo de su costo en vidas humanas), si consideramos las posibilidades que el uso de ciertas tecnologías de la era cibernética y su disponibilidad en medios masivos de recuperación de la información como la Internet, puedan brindar a los grupos terroristas de la era de la información.

El mundo físico y el mundo virtual tienen puntos en común, los cuales pueden y serán usados como blancos por una nueva generación de violentos, los ciberterroristas. A medida que nuestras sociedades se vuelvan más y más dependientes del proceso de integración informático que se da en forma global, más posibilidades habrá para que esta infraestructura de la información y el conocimiento se vuelvan un blanco apetecible de grupos o individuos que a través del terror quieran lograr sus fines, cualesquiera estos sean. A través del uso de las armas de la Infoguerra, los ciberterroristas serán capaces de causar graves daños a la infraestructura de un país, o de infligir una interdicción profunda al normal desenvolvimiento de una sociedad. Estas nuevas armas son totalmente diferentes de las armas convencionales pero son capaces de producir tan o más daño que ellas.

a) Antecedentes y conceptualización de Terrorismo Informático (Ciberterrorismo).

Todos los sistemas informáticos dependen del factor humano y por ende, este podrá ser el eslabón débil en la cadena de seguridad. Una de las leyes de la Seguridad Informática establece que la tecnología no es una panacea y otra que ningún sistema informático es 100% seguro. Partiendo de estas premisas y sabiendo que los sistemas militares de ataque y de defensa, los de información públicos y muchos otros de control de sistemas de sanidad, energía y servicios públicos dependen casi en su totalidad de la informática, podemos decir que el terrorismo vía tecnologías de información es un codiciado terreno para los terroristas.

La proliferación de computadoras conectadas a módems telefónicos que se inició a principios de los años 80 aumentó la vulnerabilidad de los sistemas informáticos y permitió el nacimiento de los hackers.

Esa vulnerabilidad hizo que los organismos de inteligencia de Estados Unidos comenzaran especular con la posibilidad de que algún grupo terrorista pueda cometer atentados o actos de sabotaje de gran envergadura empleando medios telemáticos, sin necesidad siquiera de que el agresor se encuentre dentro del territorio estadounidense. Para designar a esa eventual categoría de actos terroristas, se acuñó el término ciberterrorismo.

El temor ante hipotéticos ataques ciberterroristas se acentuó durante los años 90 debido a varios factores, como son:

a) El surgimiento de Internet y su masiva penetración en la sociedad. Eso multiplicó la cantidad de módems existentes; aumentó la vulnerabilidad de muchas redes privadas (ya que las mismas pasaron a estar conectadas a Internet, que es una red de acceso público) y fomentó la proliferación de hackers, debido a que penetrar una red ilegalmente o fabricar virus capaces de infectar miles de computadoras, pasó a ser cada vez más sencillo, como se describe en el capítulo II de esta tesis.

b) La sensación de vulnerabilidad generada por la proximidad del *millenium bug* (*la falla del milenio*), también conocido como Y2K. La incapacidad de muchas computadoras para registrar fechas posteriores a 1999 hizo temer un "apocalipsis informático" en la transición al 2000, que finalmente no se produjo gracias a la masiva inversión en prevención y adecuación de los sistemas computacionales a nivel oficial y privado.[217]

c) La proliferación masiva de noticias sobre el accionar de los hackers, cuyas capacidades aparecen en muchos casos exageradas.

Estos factores hicieron que durante la administración de Bill Clinton se adoptaran una serie de medidas preventivas en relación al ciberterrorismo.

La raíz Ciber está relacionada a lo tecnológico. La Cibernética, como término que utiliza esta raíz, se refiere al estudio de las conexiones nerviosas de los seres vivos y su aplicación a sistemas electrónicos o mecánicos. El término Ciberespacio fue introducido por William Gibson en su novela de Ciencia-Ficción "Necromancer", definiéndola como una alucinación consensual y una representación grafica de los datos extraídos de los bancos de información de computadoras.

El Ciberespacio, es un concepto abstracto que sirve para representar hechos informáticos producidos a través de redes públicas interconectadas conocidas comúnmente como Internet. Se dice que algo ha ocurrido en el ciberespacio cuando se ha verificado vía Internet. En base a estos esquemas podemos decir metafóricamente, que las páginas Web se encuentran en el ciberespacio.

[217] Al analizar los artículos de la prensa estadounidense publicados en los años inmediatamente anteriores al 2000, se evidencia el temor existente entre los organismos de inteligencia de que entre los técnicos contratados para las tareas de reconversión informática, se infiltraran terroristas con el objeto de colocar virus, robar contraseñas o alterar los sistemas computacionales de tal forma de dejarles una "puerta trasera" que posteriormente les permitiera ingresar en forma ilegal para cometer un atentado.

El vocablo "*terror*" proviene del francés antiguo "*terrere*", que significa asustar. Se trata del miedo intenso producido por la violencia o la amenaza de violencia con fines políticos. El terrorismo es la creación deliberada y la explotación del miedo para buscar un cambio político. El Terrorismo abarca cualquier acción que produzca miedo a un grupo determinado de personas. El terrorismo es también definido como la dominación por el terror. Se trata de actos de violencia o maldad, ejecutados para amedrentar ciertos sectores sociales o de una población o para desorganizar su estructura económica, social o política.

En Estados Unidos la definición usada por el FBI describe al terrorismo como el uso ilegal de la fuerza y de la violencia contra personas o la intimidación para forzar un gobierno, población civil, o cualquier segmento con a cambios políticos o sociales.[218]

Vistos los conceptos anteriores, podemos establecer que el Ciberterrorismo, ó Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

En los ataques a medios informáticos, a diferencia de muchos tipos de ataques terroristas, no existe necesidad de la presencia física del atacante. En caso de fallo del plan, el ciberterrorista aprende y se prepara para un nuevo ataque sin poner en riesgo su vida. La cobardía es también una de las características del ciberterrorista quien logra fácilmente su seguridad temporal cuando el ataque es informático.

Mientras hay realmente algún grado de similitud y superposición entre el terrorismo informático y el crimen cibernético, fundamentalmente son diferentes actividades. Desafortunadamente, la tendencia a agrupar los diferentes tipos de conflicto de la información junta produce efectos de inestabilidad local sobre el intento de tratar con estos fenómenos. En la mayoría de los estados avanzados, tres mecanismos intentan tratar con el problema del conflicto informático: a) El establecimiento de seguridad nacional, b) Autoridades de coacción legal y c) El sistema de justicia criminal. Aún, en la mayoría de estos países, el estado de preparación para el conflicto de la información, en general, y el terrorismo informático y el crimen cibernético, en particular, es insuficiente.

[218] En http://fbi.gov/Terrorism.htm, [consultado el 13 de febrero de 2007.]

Ciberterroristas están realizando extorsión a grupos financieros para recaudar fondos a cambio de no ser ciberatacados. El anonimato es una de las ventajas de las telecomunicaciones informáticas. La planificación de ataques, y la comunicación entre miembros de células terroristas puede establecerse desde cualquier cibercafé de forma asíncrona vía correo electrónico o en vivo vía Chat.[219]

b) Características del Terrorismo Informático

Actualmente la amenaza del ciberterrorismo no es inmediata. Sin embargo, la amenaza potencial del ciberterrorismo no puede ser sobre-enfatizada. El potencial para causar caos y desacomodo a las personas, a los gobiernos y a los sistemas globales ha aumentado a medida que el mundo se ha globalizado.

La perdida económica causada por un ciberataque puede causar desastre en sistemas financieros mundiales, apagones nacionales y el colapso de infraestructuras clave de información tecnológicas que apoyan muchos departamentos gubernamentales. Más que eso, la habilidad de los individuos de alcanzar a una amplia audiencia por medio del reclutamiento, movilización y propaganda anónimos utilizando el ciberespacio es preocupante. El ciberespacio permite la distribución de ideas teóricas, militares, de enseñanzas teológicas y propaganda, y también reclutar y mantener la comunicación entre organizaciones.

El ciberterrorismo puede ser definido como el ataque ilícito o amenaza de ataque en contra de redes de computadoras y la información guardada en ellas, con la intención de intimidar o extorsionar.

Uno de los principales blancos de los ciberterroristas son las redes computacionales que proveen servicios públicos, tales como sistemas de control de energía eléctrica, aeropuertos, redes de trenes, redes satelitales, sistemas financieros y de emergencia, etc. Para lograr esto, inundan el sistema con mensajes de correo electrónico para paralizarlo. Esta forma de ataque se conoce como bomba de correo electrónico.[220]

---

[219] La propaganda de los grupos catalogados como terroristas se ha hecho común en Internet. El Ejercito de Liberación Nacional colombiano (ELN), las FARC, Sendero luminoso, ETA, Hezbollah y hasta el Ku Klux Klan tienen presencia en la Web lo cual hace evidente la utilización de tecnología por parte de estos grupos.

[220] Un buen ejemplo de bombardeo por correo electrónico sucedió en 1997, cuando defensores del grupo ETA crearon un sitio web para el Periódico del País Vasco en un proveedor de servicios de Internet llamado Instituto de Comunicaciones Globales. Un grupo de personas quisieron obligar al ICG a quitar el sitio de ETA de la red, y para esto enviaron miles de correos electrónicos al proveedor de servicios de Internet, paralizándolo y eventualmente el ICG desistió y quito el sitio de la red.

En algunas ocasiones, los ataques ciberterroristas son acompañados de bombardeos suicida o ataques químicos simultáneos, con el propósito de llamar mas la atención sobre estos actos y causar mayor confusión y paralizar los medios de comunicación.

Otro uso que los terroristas le pueden dar al Internet es para el intercambio de mensajes electrónicos encriptados que contienen información crucial acerca de sus propuestas victimas, direcciones, fotografías, itinerarios, tácticas, etc. También pueden enviar mensajes intimidantes a sus victimas, reclutar mas seguidores y en general, mantener todo tipo de información peligrosa disponible para otros terroristas por medio de sus propios sitios de Internet.[221]

Así, los ciberterroristas tienen varias ventajas sobre otros tipos de terroristas: tienen mas anonimidad, entrando a cuentas electrónicas utilizando diferentes nombres de usuario, son muy difíciles de rastrear y pueden operar desde cualquier parte del mundo, sus actividades son baratas y sus blancos potenciales son numerosos. No necesitan de mucho entrenamiento y no necesitan trasladarse a largas distancias, corriendo en general, menores riesgos.

Entre mas complejo sea un sistema de computo, mas fácil es entrar a el ilegalmente, aunque algunos expertos piensan que el ciberterrorismo es una exageración.[222]

Lo cierto es que un ciberterrorista puede acceder remotamente a un sistema de control de procesamiento de cualquier lugar y cambiar las indicaciones de un procesador, ya que estar en la obra para ejecutar esos actos. Un ciberterrorista ubicara un número de bombas computarizadas alrededor de una ciudad, todas simultáneamente transmitiendo diseños numéricos únicos, cada bomba recibe el diseño de otra. Si una de las bombas deja de transmitir, todas las bombas explotan simultáneamente. Un ciberterrorista desorganizara los bancos, las transacciones financieras internacionales, la bolsa de valores.

En efecto, el ciberterrorista hará que la población de una nación no estuviera capacitada para comer, para beber, para moverse o para vivir. En suma, la gente cargo con la protección de su nación, no se alarmaran, ni estarán capacitados para sacar a los terroristas, desde que el

[221] Ha sido reportado que los miembros de al-Qaeda, por ejemplo, se preparan para un ataque intercambiando paquetes encriptados de información, fotografías e instrucciones. En Kabul, Afganistán, soldados del ejército de los Estados Unidos encontraron modelos en AutoCAD de una presa, supuestamente siendo usados para planear el bombardeo y colapso de esa estructura.

[222] En 1997 la Agencia de Seguridad Nacional (ASN) de los Estados Unidos condujo un ejercicio para probar la medida de seguridad de los sistemas nacionales de ese país. Un equipo de 35 hackers, llamado “Equipo Rojo” fue instruido para actuar como si hubieran sido contratados por un servicio de inteligencia extranjero y para que intentaran entrar en los sistemas nacionales de seguridad. Sus únicas herramientas podían ser programas que hubieran escrito ellos mismos o que fueran fácilmente accesibles en Internet. Los hackers entraron a la red y comenzaron a encontrar claves de acceso por el método de búsqueda y error o pidiéndolos a oficiales distraídos. Pronto estuvieron en total control del sistema, con el poder de deshabilitarlo si así lo hubieran querido. Este ejercicio fue conocido como el “Recipiente Elegible”

ciberterrorista es más probable que este al otro lado del mundo. Todos estos escenarios pueden ser ejecutados hoy.

Esta nueva amenaza, es una faceta de una novedosa forma de conducir la guerra, conocida como guerra infraestructural (Infraestructural Warfare), la cual probablemente será la forma dominante de los conflictos en el Siglo XXI.

3.6. Acuerdos, acciones y legislación en materia de regulación del Terrorismo Informático e Internet.

Internet y las redes y tecnologías relacionadas se han convertido en instrumentos indispensables para todos los Estados, ya que ha impulsado un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el Hemisferio. Individuos, empresas y gobiernos cada vez utilizan más las redes de información que integran Internet para hacer negocios; organizar y planificar actividades personales, empresariales y gubernamentales; transmitir comunicaciones; y realizar investigaciones.

Lamentablemente, Internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial de usuarios de ésta red. La información que transita por Internet puede ser malversada y manipulada para invadir la privacidad de los usuarios y defraudar a los negocios. La destrucción de los datos que residen en las computadoras conectadas por Internet puede obstaculizar las funciones del gobierno e interrumpir el servicio público de telecomunicaciones y otras infraestructuras críticas.

Estas amenazas a los ciudadanos, economías y servicios esenciales, tales como las redes de electricidad, aeropuertos o suministro de agua, no pueden ser abordadas por un solo gobierno ni tampoco pueden combatirse utilizando una sola disciplina o práctica.

El terrorismo informático es uno de los problemas claves con los que los diferentes países se han tenido que enfrentar. Las causas sociales y económicas de este fenómeno son ampliamente conocidas. Los gobiernos a menudo han respondido al terrorismo con medidas altamente represivas, que no sólo incluyen a los presuntos terroristas, si no que violan los derechos fundamentales de la población en general.

No obstante lo expuesto en el presente capítulo, no existe una tipificación exacta de Ciberterrorismo en los diversos ordenamientos jurídicos, pero no dudo que se incluyan como delitos independientes o como agravantes, con penas más severas que las de los delitos

informáticos ordinarios cuando cualquier tipo de delito informático se realice con fines políticos. A continuación se enunciaran algunos acuerdos, leyes y legislaciones ya aprobadas en materia de Terrorismo y Ciberterrorismo, empezando por la Organización de Naciones Unidas.

Las Naciones Unidas han estado activas en la lucha contra el terrorismo internacional, reflejando la determinación de la comunidad internacional para eliminar esta amenaza. La Organización y sus agencias han desarrollado una amplia gama de acuerdos legales internacionales, que permiten a la comunidad internacional tomar acción para suprimir el terrorismo y poner a los responsables a la justicia.

Desde 1963, estos acuerdos proporcionan las herramientas legales básicas para combatir el terrorismo internacional en todas sus. Dichos acuerdos, han sido ratificados por la mayoría de los países alrededor del mundo. Tales acuerdos han sido desarrollados por la Asamblea General, la Organización Internacional de la Aviación Civil (OACI), la Organización Marítima internacional (OMI), y el Organismo Internacional de Energía Atómica (la OIEA).[223]

De esta manera tenemos:

a. Resoluciones adoptadas por la Asamblea general:

- **49/60.** Medidas para eliminar el terrorismo internacional
- **50/53.** Medidas para eliminar el terrorismo internacional
- **51/210.** Medidas para eliminar el terrorismo internacional
- **52/165.** Medidas para eliminar el terrorismo internacional
- **53/108.** Medidas para eliminar el terrorismo internacional
- **54/110.** Medidas para eliminar el terrorismo internacional
- **55/158.** Medidas para eliminar el terrorismo internacional

b. El Consejo de Seguridad

Cómo órgano principal encargado de las cuestiones relativas a la paz y seguridad internacionales ha estado en continua lucha en contra del terrorismo. El 28 de septiembre, el Consejo adoptó la resolución 1373 (2001), sobre las amenazas a la paz y la seguridad internacionales creadas por actos de terrorismo. Inmediatamente después del ataque del 11 de septiembre en Nueva York y Washington, D.C., a través de la resolución 1368 (2001), el Consejo condenó inequívocamente en los términos más enérgicos los horrendos ataques terroristas en contra de los Estados Unidos de América, e instó a todos los Estados a que colaboren con urgencia para someter bajo justicia a los autores.

[223] En http://www.un.org, [consultado el 21 de enero de 2007]

Mediante resolución 1333 (2000), se exige a las autoridades de los talibanes que procedan rápidamente a la clausura de todos los campamentos en que se entrene a terroristas.

En la resolución 1269 (1999), se condena inequívocamente todos los actos, métodos y prácticas terroristas por considerarlos criminales e injustificables, y llama a los Estados para que apliquen plenamente las convenciones internacionales contra el terrorismo en las que son partes.

De igual manera, en la resolución 1267 (1999), se exige que los talibanes entreguen sin más demora a Usama bin Laden a las autoridades competentes para ser enjuiciado.

c. Otras Convenciones

Además de estas convenciones, la Asamblea General ha adoptado la Declaración sobre medidas para eliminar el terrorismo internacional (1994) y la Declaración complementaria de la Declaración de 1994 sobre medidas para eliminar el terrorismo internacional (1996), condenando todos los actos, métodos y prácticas terroristas por considerarlos criminales e injustificables, dondequiera y por quienquiera sean cometidos y se urge a los Estados a tomar medidas al nivel internacional y nacional para eliminar el terrorismo.

El Centro de las Naciones Unidas para la Prevención Internacional del Crimen, con oficinas en Viena, investiga las diferentes tendencias del terrorismo y asiste a los países en la capacitación y sobre todo en la prevención de actos terroristas. Esta oficina pertenece a la Dirección de las Naciones Unidas para el Control de las Drogas y la Prevención del Crimen.

Además, actualmente existen 21 tratados mundiales o regionales relativos al tema del terrorismo internacional.

- Convenio sobre las infracciones y ciertos otros actos cometidos a bordo de las aeronaves, firmado en Tokio el 14 de septiembre de 1963 (entró en vigor el 4 de diciembre de 1969)
- Convenio para la represión del apoderamiento ilícito de aeronaves, firmado en La Haya el 16 de diciembre de 1970 (entró en vigor el 14 de octubre de 1971)
- Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil, firmado en Montreal el 23 de septiembre de 1971 (entró en vigor el 26 de enero de 1973)
- Convención sobre la prevención y el castigo de los delitos contra personas internacionalmente protegidas, inclusive los agentes diplomáticos, aprobada por la Asamblea General de las Naciones Unidas el 14 de diciembre de 1973 (entró en vigor el 20 de febrero de 1977)

- Convención internacional contra la toma de rehenes, aprobada por la Asamblea General de las Naciones Unidas el 17 de diciembre de 1979 (entró en vigor el 3 de junio de 1983)
- Convención sobre la Protección Física de los Materiales Nucleares, firmada en Viena el 3 de marzo de 1980 (entró en vigor el 8 de febrero de 1987)
- Protocolo para la represión de los actos ilícitos de violencia en los aeropuertos que presten servicio a la aviación civil internacional, complementario del Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil internacional, firmado en Montreal el 24 de febrero de 1988 (entró en vigor el 6 de agosto de 1989)
- Convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima, hecho en Roma el 10 de marzo de 1988 (entró en vigor el 1° de marzo de 1992)
- Protocolo para la represión de actos ilícitos contra la seguridad de las plataformas fijas emplazadas en la plataforma continental, hecho en Roma el 10 de marzo de 1988 (entró en vigor el 1° de marzo de 1992)
- Convenio sobre la marcación de explosivos plásticos para los fines de detección, firmado en Montreal el 1° de marzo de 1991 (entró en vigor el 21 de junio de 1998)
- Convenio internacional para la represión de los atentados terroristas cometidos con bombas, aprobado por la Asamblea General de las Naciones Unidas el 15 de diciembre de 1997 (entró en vigor el 23 de mayo de 2001)
- Convenio internacional para la represión de la financiación del terrorismo, aprobado por la Asamblea General de las Naciones Unidas el 9 de diciembre de 1999 (entró en vigor el 10 de abril de 2002)
- Convención árabe sobre la represión del terrorismo, firmada en una reunión celebrada en la Secretaría General de la Liga de los Estados Árabes en El Cairo el 22 de abril de 1998 (entró en vigor el 7 de mayo de 1999)
- Convención de la Organización de la Conferencia Islámica sobre la lucha contra el terrorismo internacional, aprobada en Uagadugú el 1° de julio de 1999
- Convención Europea para la Represión del Terrorismo, concertada en Estrasburgo el 27 de enero de 1977 (entró en vigor el 4 de agosto de 1978)

- Convención de la Organización de los Estados Americanos (OEA) para la prevención y represión de los actos de terrorismo encuadrados como delito contra las personas y actos conexos de extorsión de alcance internacional, concertada en Washington, D.C. el 2 de febrero de 1971 (entró en vigor el 16 de octubre de 1973)
- Convención de la Organización de la Unidad Africana (OUA) sobre la prevención y la lucha contra el terrorismo, aprobada en Argel el 14 de julio de 1999 (entró en vigor el 6 de diciembre de 2002)
- Convención regional sobre la eliminación del terrorismo de la Asociación del Asia Meridional para la Cooperación Regional, firmada en Katmandú el 4 de noviembre de 1987 (entró en vigor el 22 de agosto de 1988)
- Tratado de Cooperación entre los Estados miembros de la Comunidad de Estados Independientes para Combatir el Terrorismo, hecho en Minsk el 4 de junio de 1999.
- Convención Interamericana contra el Terrorismo, aprobada en Bridgetown el 3 de junio de 2002.
- Protocolo por el que se enmienda el Convenio Europeo para la Represión del Terrorismo, aprobado en Estrasburgo el 15 de mayo de 2003.

Por su parte la Comisión Interamericana de Derechos Humanos ha condenado en numerosas oportunidades el terrorismo y señalado que no hay causa o pretexto que pueda invocarse para justificar, ataques contra civiles y otros actos proscritos por el derecho internacional.

Los diferentes ataques terroristas han resultado en un vigoroso debate para la adopción de normas antiterroristas que incluyen, entre otras cosas, comisiones militares y otras medidas.

La doctrina de la CIDH ha sido que tribunales militares no pueden juzgar civiles, salvo ante la inexistencia material de cortes civiles, cuando tal juzgamiento es de hecho imposible. Incluso y en tal caso, la Comisión ha señalado que el juzgamiento debe reconocer las garantías mínimas establecidas en el derecho internacional, que incluyen la no discriminación entre ciudadanos y quienes se encuentren bajo la jurisdicción de un Estado, juez independiente, derecho de defensa, libre elección, y acceso a las pruebas y posibilidad de contradecirlas.

En el marco de las atribuciones establecidas en el artículo 18 de su estatuto, la CIDH elaboró un Informe sobre Terrorismo y Derechos Humanos, dirigido a asistir a los Estados en la adopción de normas adecuadas en el marco del Derecho Internacional.

Entre las resoluciones de la OEA en condena y prevención del terrorismo, tenemos las siguientes;[224]

- Resolución 1399 en el Periodo XXIV Ordinario de Sesiones 1996.Cooperación hemisférica para prevenir, combatir y eliminar el terrorismo
- Resolución 1492 en el Periodo XXVII Ordinario de Sesiones 1997.Cooperación hemisférica para prevenir, combatir y eliminar el terrorismo
- Resolución 1553 en el Periodo XXVIII Ordinario de Sesiones 1998.Cooperación hemisférica para prevenir, combatir y eliminar el terrorismo
- Resolución 1650 en el Periodo XXIX Ordinario de Sesiones 1999.Cooperación hemisférica para prevenir, combatir y eliminar el terrorismo

Del mismo modo la Interpol fomenta la cooperación policial en todos los asuntos de delincuencia internacional salvo los que revisten un carácter político, militar, religioso o racial. Los actos terroristas que son de tipo delictivo constituyen una grave amenaza para la vida y la libertad de las personas y la seguridad nacional de los Estados miembros.

El papel de Interpol es doble, consiste en prevenir los actos de terrorismo internacional y, en el caso en que lleguen a cometerse, asegurarse de que sus autores sean localizados, detenidos y llevados ante los tribunales.

Interpol recoge, registra, analiza y difunde información sobre personas y grupos sospechosos, y sobre sus actividades. La información proviene de los países miembros, así como de fuentes públicas de información, que también consulta. Es importante destacar que toda la información relacionada con el terrorismo se tiene que comunicar de forma sistemática, rápida y precisa. La veracidad y la rapidez de la información suele ser directamente proporcional a su utilidad para los funcionarios especializados que trabajan en la Subdirección de Seguridad Pública y Terrorismo de Interpol, que se encargan de evaluar las amenazas y publicar avisos y alertas usando herramientas específicas de Interpol, como las difusiones rojas y azules.

En 2002 la Secretaría General de Interpol creó el Grupo Mixto Especializado de Interpol[225] con miras a diseñar y aplicar una metodología multidisciplinar para ayudar a los países miembros en sus investigaciones vinculadas con el terrorismo. A menudo resulta difícil determinar las relaciones exactas entre la delincuencia organizada y las organizaciones terroristas. Se sospecha que muchos de los atentados terroristas realizados en todo el mundo están

[224] En http://www.oas.org, [consultado el 14 de febrero de 2007]
[225] En http://interpol.int, [consultado el 23 de febrero de 2007.]

financiados mediante actividades de delincuencia organizada, entre las que figuran el tráfico de drogas, el blanqueo de capitales y otras formas de delincuencia económica y financiera, la extorsión, el robo a mano armada, los secuestros, el cobro de impuestos revolucionarios y el tráfico de armas. El Grupo Mixto Especializado se ha creado para desarrollar la capacidad de Interpol en este terreno con objeto de mejorar y ampliar el papel de la Organización en materia de detección y desarticulación de organizaciones delictivas y terroristas.

En la Conferencia Regional Asiática de 2002, celebrada en Sri Lanka, los países miembros apoyaron enérgicamente la creación de un nuevo proyecto sobre el terrorismo en el Sureste asiático. El proyecto Pacific [226]tiene fines y objetivos de carácter preventivo y operativo, y reúne a especialistas muy importantes para que intercambien información relacionada con el terrorismo, introduzcan esta información en la base de datos de Interpol a fin de analizarla y utilizarla, y asimismo para animar a los países miembros a que soliciten la publicación de difusiones rojas y de mensajes de difusión que den lugar a detenciones y extradiciones.

De la misma manera El Grupo G-8, acordó por unanimidad la creación del Grupo de Acción contra el Terrorismo (GACT).

El GACT "reforzará las capacidades de lucha contra esta grave amenaza a escala internacional",[227] el grupo de acción contra una de las peores plagas que existe en el mundo, según la declaración del G-8, "estará encargado de reforzar la voluntad política y coordinar la ayuda al fortalecimiento de las capacidades institucionales."[228] También acordó que otros Estados, principalmente donantes, serán invitados para asociarse al GACT. Los países miembros del GACT aportarán financiamiento, asesoramiento técnico y posibilidades de formación para que el Grupo pueda cumplir adecuadamente con sus objetivos. Este grupo de acción nacerá con un buen apoyo, pues en la Cumbre de Sharm el Sheij (Egipto), se respaldó la lucha mundial contra el terrorismo[229] y, además, servirá para establecer la paz en el Medio Oriente, una de las regiones más afectadas por la acción terrorista.

Durante la cumbre que tuvo lugar en París en 1989, surge el Grupo de Acción Financiera Internacional sobre el Blanqueo de Capitales (GAFI)[230] creado por el Grupo de los Siete Países más Industrializados (G-7). El principal objetivo del GAFI es el estudio y la búsqueda de medidas destinadas a combatir el blanqueo de capitales.

---

[226] *Ídem.*
[227] En http://en.g8russia.ru [consultado el 11 de marzo de 2007]
[228] *Ídem*.
[229] Con la aprobación de Israel y la Autoridad Nacional Palestina
[230] En http://www.g7.utoronto.ca/, [consultado el 25 de marzo de 2007]

En el Pleno extraordinario, el GAFI aprobó un conjunto de Recomendaciones Especiales sobre Financiación del Terrorismo que compromete a sus miembros a:

- Tomar inmediatos recaudos para ratificar e implantar los pertinentes instrumentos emitidos por la Organización de Naciones Unidas.
- Sancionar penalmente la financiación del terrorismo, los actos terroristas y las organizaciones terroristas.
- Congelar y confiscar los activos de los terroristas.
- Informar las transacciones que se sospeche estén relacionadas con el terrorismo.
- Proporcionar el más amplio rango posible de asistencia a las autoridades regulatorias y de cumplimiento de la ley de otros países para investigaciones sobre financiación del terrorismo.
- Imponer requisitos contra el lavado de dinero sobre sistemas alternativos de remesas de dinero.
- Hacer más severas las normas sobre identificación del cliente en las transferencias telegráficas de dinero internacionales y domésticas.
- Asegurarse que las entidades, en particular las organizaciones sin fines de lucro, no puedan ser utilizadas indebidamente para financiar el terrorismo.

Asimismo, emitió algunas recomendaciones Especiales acerca de la Financiación del Terrorismo:

- Ratificación e implantación de los instrumentos de la ONU
- Penalizar la Financiación del terrorismo y el lavado de dinero asociado a ello.
- Congelación y confiscación de activos terroristas
- Informe de transacciones sospechosas relacionadas con el terrorismo
- Cooperación Internacional
- Remesas de dinero alternativas
- Transferencias telegráficas
- Organizaciones sin fines de lucro

Los países deberán adecuar las leyes y normas concernientes a las entidades, que puedan ser violadas para financiar el terrorismo. Las organizaciones sin fines de lucro son particularmente vulnerables; los países deberán asegurarse de que ellas no puedan ser utilizadas en forma impropia:

- Por organizaciones terroristas disimuladas como entidades legítimas,

- Para explotar entidades legítimas como vía de financiación terrorista o con el propósito de evadir medidas de congelación de bienes y
- Para ocultar o disimular el desvío clandestino, a organizaciones terroristas, de fondos destinados a propósitos legítimos.

Lo que se constata al nivel de la legislación interna de los Estados no es muy distinto, como puede intuirse, a la situación en el ámbito internacional; esto es, existe también una incapacidad técnica para definir autónomamente al terrorismo.

Cabe destacar una situación particular, que es el hecho de que los gobiernos agredidos por este tipo de conducta optan en general por medidas de fuerza que les garantice presencia frente a sus electores, a través de una imagen de reacción punitiva inmediata, independientemente de las violaciones que dichas conductas instrumentadas desde el poder puedan implicar, desde el punto de vista de la violación de los derechos individuales. Huelga decir que la preservación del Estado de derecho es más importante incluso que la necesidad misma de eliminar al terrorismo, porque erosionar las garantías de que gozan legítimamente los ciudadanos puede traducirse en una erosión de la seguridad jurídica y de todas las instituciones del Estado, aunque en ocasiones estos criterios queden identificados como meros argumentos técnicos que no trascienden al interés político.

Estados Unidos ofrece un ejemplo reciente de una reacción legal frente a actos terroristas, con la Ley Antiterrorista, del 26 de octubre de 2001, donde se da un catálogo de acciones a instrumentar desde la autoridad, como detenciones, intervenciones telefónicas o de correos electrónicos, sin orden de juez competente, como actos preventivos de posibles actos terroristas.

En cuanto a una definición en el derecho interno, se encuentra en el Código de Estados Unidos de América, sección 2656f (d), en los siguientes términos: "Violencia premeditada y políticamente motivada, perpetrada contra objetivos no combatientes, por grupos subnacionales (identidades criminales), o agentes clandestinos, con la intención de influir en una audiencia."[231]

En la anterior definición cabe destacar la idea de identidades criminales, que por extensión se podría traducir al concepto de nacionalismos criminales, sin que se trate de una analogía.

Asimismo, Estados Unidos cuenta con la **Benjamin Franklin True Patriot Act,** referente a las libertades civiles de los terroristas, del 9 de abril de 2003, la **Anti-Terrorism**

[231] En http:// www.whitehouse.gov/infocus/nationalsecurity/index.es.html, [consultado el 8 de abril de 2007]

Intelligence Tools Improvement Act of 2003, la cual refuerza las herramientas de investigación antiterroristas y promueve compartir la información.

Cuenta también con un programa llamado Carnívoro, que es un paquete de presentaciones de computadora muy sofisticado desarrollado por expertos del FBI como continuación de un proyecto anterior llamado "Omnívoro" que se implemento a mediados de la década de los noventas. Después de cierta publicidad negativa en la prensa, el FBI decidió cambiar el nombre de Carnívoro por el de "SCD1000" o "Sistema de Colección Digital 1000". Este fue uno de los primeros programas de vigilancia en ser usados por agencias de protección legal para monitorear actividad sospechosa en Internet. Es caza de grabar todos los mensajes recibidos por personas utilizando un determinado proveedor de servicios de Internet.[232]

El programa en si mismo es lo suficientemente ligero para ser instalado en una computadora portátil y funciona de acuerdo al mismo principio que otros programas 'rastreadores' y programas de diagnostico de redes que son utilizados rutinariamente en proveedores de servicios de Internet y que funcionan con la mayoría de las aplicaciones mas populares para correo y mensajería electrónico.

Lo cierto es que la mayoría de las organizaciones de otros gobiernos han también formado algún tipo de grupo para tratar con los terroristas informáticos. La CIA creó su propio grupo, el Centro de Conflicto de Información, provisto con 1000 personas y un equipo de respuesta las 24 horas. El FBI investiga a hackers y a grupos similares. El Servicio Secreto persigue a los casos de comercio del banco, de fraude y de interceptación de líneas telefónicas. La Air Force creó su propio grupo, Equipos de Ingenieros en Seguridad Electrónica, (ESETs). Los equipos de dos o tres miembros casualmente van en los lugares del Air Force y tratan de mejorar en el control de sus computadoras. Los equipos han tenido un exitoso promedio de 30% en la completa mejora del control de los sistemas.[233]

---

[232] Los defensores de los derechos civiles han protestado fuertemente contra el uso de este programa, declarando que viola los derechos de las personas, y hasta el 11 de septiembre de 2001, Carnívoro nunca había sido usado sin el permiso de un juez. Sin embargo, el 13 de septiembre de ese mismo año, el Senado aprobó el Acto de Combate al Terrorismo, el cual daba a los oficiales del FBI el permiso de usar el programa sin una orden judicial o el consentimiento de un juez. Sin embargo, de acuerdo al Director Asistente del FBI, Donald Kerr, Carnívoro, o DCS1000 tiene la habilidad de seleccionar entre todas las comunicaciones de Internet, aquellas que son sospechosas y las que no lo son, de acuerdo a los criterios que se den en una corte judicial. Por ejemplo, el programa puede buscar entre numerosos mensajes y seleccionar solo aquellos originados de un determinado individuo, o aquellos que vienen de un determinado individuo y que están relacionados con una cierta cuenta bancaria.

[233] Según expertos en la materia, se maneja que serán objetivos primordiales de los ataques, las redes de Gobierno y fuerzas militares, centrales telefónicas digitales, medios de comunicación, centros de investigación científica, centros satelitales, represas, centrales eléctricas o de distribución. La táctica de ataque por excelencia será la interrupción y/o disminuir la efectividad de los sistemas de información.

Recientemente ha habido esfuerzos renovados para prevenir el cibercrimen y monitorear cualquier actividad sospechosa que pudiera estar relacionada con el terrorismo. Por ejemplo, hace algunos años, los gobiernos de Francia y el Reino Unido requirieron que todos los proveedores de servicios de Internet firmaran un acuerdo de auto-censura y que retuvieran, al menos por un año, las bitácoras de correo electrónico, conversaciones electrónicas y otros datos similares, en caso de que contuvieran información que pudiera ser usada como evidencia de actividad terrorista. Otros países Europeos, como Suecia y Dinamarca, han hecho lo mismo al permitir que la policía pueda acceder rápidamente las bitácoras, inmediatamente después de un ataque, sin una orden judicial, y que puedan instalar programas “rastreadores” en los proveedores de servicios de Internet para interceptar correos electrónicos y mensajes, similares al programa Carnívoro desarrollado por el FBI en los Estados Unidos.

El gobierno de China ha tratado de controlar el crecimiento de cibercafés cerrando miles de ellos en un esfuerzo para atrapar a disidentes y criminales que utilizan el Internet para planear e infringir daño a grandes compañías entre otros blancos.

En México, por su parte, en el artículo 139 del Código Penal Federal se tipifica al terrorismo como los "actos contra personas, cosas o servicios que produzcan alarma, temor, terror en la población o en un grupo o sector de ella, o tratar de menoscabar la autoridad del Estado o presionar a la autoridad para que tome una determinación".

Lo cierto es que ha sido práctica común observar en otros casos que todo acto terrorista, en cuanto a sus implicaciones legales, es referido a los estatutos legales que regulan, en particular, la materia o actividad involucrada.

Existen dos importantes problemas jurisdiccionales que valen resaltarse. El primero atañe a los actos terroristas que han ocurrido regularmente en sitios donde la jurisdicción para la aplicación de las normas legales es en muchas ocasiones incierta, por ejemplo: un avión sobre aguas internacionales. El segundo es que si bien ha sido claro quién puede argumentar jurisdicción, no siempre está claro la conveniencia política de hacerlo, por el miedo a las represalias.

Las leyes internacionales contienen reglas de la jurisdicción que operan sobre personas y eventos, ya sea dentro o fuera del territorio de un Estado. Regularmente los Estados pueden extender su jurisdicción a los nacionales que están en otro país, pero esto no es obligatorio, y pueden en cualquier evento referirse a la competencia territorial.[234] Por ello, la jurisdicción en

[234] *Cfr*. Higgins, Rosalyn, *op. cit*., pp. 23 y 24.

relación con agresiones específicas devino elemento central en los subsecuentes "tratados aéreos".

No sólo fue necesario definir la jurisdicción y el territorio nacional cuando varios intereses concurrían. Rápidamente apareció que frecuentemente todos los Estados deseaban no ejercer la jurisdicción por miedo a las represalias. Las nuevas convenciones se encaminaron entonces a asegurar que aquéllos con competencia jurisdiccional primaria (esto es, aquéllos donde el avión había llegado y donde se encontraba el secuestrador presente) se daba la procedencia del ejercicio de la jurisdicción penal local o el deseo de extraditar al agresor a una competencia jurisdiccional permitida.

En general, el legislador, interno y/o internacional, parece preferir el acogerse a la solución básica de incluir los denominados delitos de terrorismo como delitos comunes, a los que se atribuyen especiales consecuencias como es la agravación de las penas.

A la hora de definir se opta por la caracterización de la autoría -banda armada, organización o grupo terrorista-, a la que se añade el elemento teleológico o intencional.

Como alternativa a los problemas que plantea el tratamiento jurídico del terrorismo, especialmente en derecho internacional, la doctrina ha propuesto la desaparición de esta categoría específica y su sustitución por la noción de delitos contra el derecho humanitario.[235]

En opinión de otros juristas, lograr una definición de terrorismo no sería un trabajo más complejo que lograr cualquier otro concepto jurídico, pero, en general, en los documentos internacionales se ha preferido referir "manifestaciones de terrorismo", como en la Convención de Nueva York de 1997.

Como era de esperarse, los trabajos en busca de un concepto definitorio -que no definitivo- de este tipo de conducta se han intensificado a partir de los acontecimientos del 11 de septiembre de 2001.

No obstante el problema de la subjetividad implicada en el tema de la definición, puede afirmarse que la tendencia general es el de una homogeneización de criterios, donde parece imperar que todo acto de terrorismo es internacional[236] porque representa una amenaza a la paz y seguridad internacionales.

Sólo de manera enunciativa se puede referir la posibilidad de que el tema del terrorismo es estructuralmente de dominio internacional, para lograr un frente común que asegure eficacia más

[235] *Cfr*. Ramón Chanet, Consuelo, *Terrorismo y respuesta de fuerza en el marco del derecho internacional*, España, Editorial Tirant lo Blanch Alternativa, 1993, pp. 106 y 107.
[236] Aun si se presenta en la jurisdicción interna de un Estado

que violaciones a los derechos individuales. Ejemplo de ello lo encontramos incipientemente en el Comité Europeo del Consejo de Europa sobre Actos Criminales, donde se ha establecido que cualquier Estado tiene jurisdicción sobre ciertos crímenes.

En la Convención Europea para la Represión del Terrorismo se listan las conductas consideradas como terroristas; nunca pueden ser consideradas delitos políticos, con el fin de rehusar la extradición; todo Estado debe, en su jurisdicción, adoptar medidas contra el sospechoso si no lo extradita.

En opinión de Rosalyn Higgins, es en el tratamiento jurisdiccional que la Convención Europea sobre la supresión del terrorismo hace sobre la persecución y condena de esta conducta, donde se puede identificar cercano al concepto de jurisdicción universal.[237]

La jurisdicción universal ha tenido un impulso derivado de las lagunas que, en materia de aplicación de justicia y falta de determinación de responsabilidad individual, ha venido presentando el entorno internacional; sin embargo, su proliferación puede representar un serio problema para la estabilidad del sistema en su conjunto y tal vez provocar "...la tiranía de los justos."[238] Por esto, la creación de la Corte Penal Internacional puede resultar una respuesta a las acciones de denegación de justicia por crímenes de guerra, ante la máxima de que nadie puede estar por encima de la ley.

La ambigüedad de los elementos que integran el tipo, podría hacer posible afirmar que el terrorismo es un fenómeno que preocupa a todos los Estados, aunque todos los Estados no están preocupados por el mismo fenómeno.

[237] *Cfr*. Higgins, Rosalyn, *op. cit*., p. 65.
[238] Kissinger, Henry, *Does America need a Foreign Policy?,* Estados Unidos de América, Ed. Simon & Schuster, 2001, p. 273.

CAPÍTULO IV

LEGISLACIÓN COMPARADA.

Durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales. Aunque la preocupación por la presencia de material ilícito y nocivo en la Red es la misma, las soluciones que se están aportando en estos momentos son distintas. Mientras que en Estados Unidos ha existido un intento regulación y limitación de la libertad de expresión en Internet desde la Unión Europea se propician otros métodos combinados, como el uso de filtros o las líneas de denuncia.[239]

En el mismo sentido, se puede decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

El desarrollo de la Internet, como un nuevo medio de difusión masiva de contenidos se erige como una realidad incontestable, con todos los visos de seguir experimentando un crecimiento exponencial en los próximos años. Este crecimiento no se encuentra exento de fuertes tensiones derivadas de las potencialidades que encierra el uso de la tecnología digital, y de las facilidades intrínsecas del sistema para acceder y transmitir datos de una máquina a otra, sin que las fronteras políticas supongan barrea efectiva para ello.

La legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

[239] Lo mencionado en el primer párrafo, se estudió de manera profunda en el Capítulo II, apartado 2.5 “Seguridad, contenidos y propuestas regulatorias en la Internet. El Marco jurídico”, del presente trabajo.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, provisionales y de identificación de las personas. Y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje. No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

Por lo anterior, se procederá a realizar un análisis comparado y detallado de las diferentes propuestas y legislaciones en diferentes países de la Unión Europea, América del Norte y Centro y Sur América, para terminar con nuestro país.[240]

4.1 Unión Europea

Cuando el legislador comunitario, en los últimos años de los ochenta, acometía la tarea de intentar generar un marco homogéneo para el medio audiovisual europeo y en concreto todo aquello relacionado con lo que conocemos como sus contenidos, todavía, seguro, no conocía de una nueva posibilidad de transmisión de datos, información y contenidos como es Internet.

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 la mayoría de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma

[240] La elección de los países que se analizaran durante el desarrollo de este apartado, fue seleccionado de acuerdo a los adelantos jurídicos nacionales que presentan en referencia a la regulación de Internet, la piratería, delitos y terrorismo informáticos, de la misma manera, la información bibliográfica resulto un impedimento, ya que, debido a la poca o nula información sobre esta temática, se dificultó el poder realizar un análisis más amplio, donde se incluyeran la mayoría de las naciones.

preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

De esta manera, la Unión Europea sostienen que "el desarrollo de las nuevas tecnologías de la información y la comunicación dan lugar a profundos cambios en la economía y en la sociedad. El éxito de la sociedad de la información es decisivo para el crecimiento, la competitividad y la creación de empleos en Europa."[241]

Esta es la razón por la que la Comisión lanzó la Iniciativa eEuropa en diciembre de 1999, cuyo objetivo era permitir a la UE utilizar todas las posibilidades. El plan de acción global sobre esta Iniciativa, aprobado por el Consejo Europeo de Feira en junio de 2000, destaca la importancia de la seguridad de las redes y de la lucha contra los delitos informáticos.

La Unión Europea ya lanzó una serie de medidas para luchar contra el contenido ilícito y perjudicial en Internet con el fin de proteger los derechos de la propiedad intelectual y los datos de carácter personal, promover el comercio electrónico y reforzar la seguridad en las transacciones, a saber:

- El programa de acción relativo a la delincuencia organizada, adoptado por el Consejo JAI en mayo de 1997 y aprobado por el Consejo Europeo de Ámsterdam, que invitaba a la Comisión a realizar un estudio sobre la delincuencia informática. La Comisión presentó en abril de 1998 este estudio, conocido por su título abreviado como "estudio COMCRIME;"[242]
- El Consejo Europeo de Tampere reconoció que los esfuerzos para llegar a un acuerdo sobre definiciones y sanciones comunes de una serie de actos delictivos deben también referirse a la delincuencia que utiliza las nuevas tecnologías y;
- La aprobación de una serie de medidas iniciales en el marco de la estrategia de la Unión en materia de lucha contra la delincuencia que se sirve de las altas tecnologías.

En esta línea, debe mencionarse que el interés por regular acciones delictivas informáticas en la Unión Europea, surge a raíz de los intereses comerciales de este grupo, también es importante apuntar que hoy en día, este bloque está inmerso en la aprobación de multitud convenios transnacionales de actividad comercial.

A continuación se detallará el marco jurídico propio de algunos Estados miembros de la Unión Europea, destacándose los más avanzados en la regulación de los delitos informáticos:

[241] En europa.eu/scadplus/leg/es/lvb/l33193b.htm [consultado el 14 de marzo de 2007]
[242] Olivier Hance, *Leyes y negocios en Internet* (Trad. de Yazmín Juárez Parra), México, McGraw Hill, 1996, p. 137.

4.1.1 España

En el contexto de la sociedad de la información, y con el uso imprescindible de la informática en el desarrollo de las actividades profesionales y personales, todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes, tiene una ley aplicable a su comisión, esto es el principio de territorialidad, es decir, se aplica la ley del lugar de comisión del delito.

Así, la legislación sobre delitos informáticos en España se encuentra en el Código Penal,[243] en sus artículos siguientes:

a. Delitos contra la libertad: (Art. 169- 172 Código Penal)

Artículo 169. "El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado…"[244]

Artículo 170. "Si las amenazas de un mal que constituyere delito fuesen dirigidas a atemorizar a los habitantes de una población, grupo étnico, cultural o religioso, o colectivo social o profesional, o a cualquier otro grupo de personas, y tuvieran la gravedad necesaria para conseguirlo, se impondrán respectivamente las penas superiores en grado a las previstas en el Artículo anterior."[245]

Artículo 171. "…Si alguien exigiere de otro una cantidad o recompensa bajo la amenaza de revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés, será castigado con la pena de prisión de dos a cuatro años, si ha conseguido la entrega de todo o parte de lo exigido, y con la de cuatro meses a dos años, si no lo consiguiere…Coacciones a través de medios electrónicos: Los elementos necesarios para que exista son: Conducta violenta de contenido material o intimidatorio, que pueda ejercerse directa o indirectamente (en este último caso, a través de cosas o terceras personas) contra la víctima, se busca impedir lo que la Ley no prohíbe, o efectuar lo que no se quiera, sea justo o injusto, intensidad de la violencia necesaria para ser delito y no una

[243] Ley-Orgánica 10/1995, de 23 de Noviembre/BOE número 281, del 24 de Noviembre de 1995.
[244] Joan Queralt, *Código Penal de España*, p. 89.
[245] *Ídem*.

mera falta por coacción de carácter leve, el autor debe actuar movido por el ánimo de restringir la libertad ajena, el acto debe ser considerado social y jurídicamente ilícito.[246]

b. Pornografía Infantil: En el Artículo 189 se trata a los delitos de prostitución y corrupción de menores. En este caso se incluye la expresión "el que por cualquier medio" con el fin de incluir Internet como medio para cometer este delito. Se trata de delitos tradicionales existentes hasta ahora en el código penal y que son de perfecta aplicación a los cometidos por medios informáticos, de la misma manera, la difusión y exhibición de material pornográfico a menores, está consignada en el artículo 186, donde se castiga el hecho de exhibir material pornográfico a menores a través de cualquier medio, por ejemplo el correo electrónico.

c. Calumnias e injurias: se define por calumnia a la "Imputación de un delito,"[247] y por injuria al "Insulto, que cabe con publicidad si se propaga el insulto."[248] Asimismo se dice que es posible llevar a cabo estos delitos a través del correo electrónico o incluso a través de terminales móviles.

d. Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio: Todos estos delitos necesitan denuncia de la persona agraviada, salvo el caso de los menores de edad o incapaces. Esto se encuentra consignado en el Artículo 197.1, donde el primer inciso perseguiría las conductas de: Apoderamiento memorizando el contenido sin desplazamiento físico y obtención de e-mails impresos en formato papel fuera del sistema informático. El segundo inciso perseguiría conductas de: Interceptar, reproducir, grabar sin consentimiento correos electrónicos de un tercero (por ejemplo, quebrantando "passwords"). En la era de Internet es habitual la conducta de rastrear información ubicada en los discos duros de los ordenadores conectados a la Red mediante programas rastreadores o sniffers, lo que facilita el control por personas ajenas, entre otros datos, de los correos electrónicos, así como la lectura de los mismos. Este atentado contra las comunicaciones electrónicas y telecomunicaciones encuentra ubicación punitiva en este segundo inciso del artículo 197.1.

e. Delitos contra el Patrimonio: aquí de encuentra el denominado "hurto electrónico", que es el "acto de tomar cosas muebles ajenas sin la voluntad de su dueño, por medios informáticos, electrónicos o telemáticos."[249] Asimismo, se considera que la estafa informática es la transferencia no consentida de cualquier activo mediante manipulación informática o artificio

[246] *Código Penal de España*, p. 92.
[247] Artículos 205 y 206
[248] Artículo 208 y 209 del Código Penal de España.
[249] Artículo 234 del Código Penal de España.

semejante, actuando el autor con ánimo de lucro. En los artículos 238 y 239 del Código, se menciona la utilización de llaves falsas, mencionando que: "A los efectos del presente Artículo, se consideran llaves, las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia."[250] Del artículo 248 al 264 se aborda la estafa informática, considerando reos de estafa a "los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero."[251]

f. Delitos contra la Propiedad Intelectual: Artículo 270: "…Será castigado también con la misma pena quien fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo."[252]

g. Delitos contra el mercado: en el artículo 278, se habla sobre el apoderamiento y revelación de secretos empresariales, incluyendo documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo. Por su parte el artículo 282 se refiere a la publicidad engañosa a través de Internet.

4.1.2 Francia

Las disposiciones penales sobre estos delitos, están contempladas en sus numerales del 41 al 44 del Código Penal, los cuales contemplan lo siguiente: Artículo 41" El que hubiere procedido o mandado proceder a la realización de tratamientos automatizados de información nominativa sin que hubieran sido publicados los actos reglamentarios previstos en el artículo 15 o formuladas las denuncias previstas en el artículo 16, supra, será castigado con pena de privación de libertad de seis meses a tres años y con pena de multa de 2 000 a 200 000 francos, o con una sola de estas dos penas. Asimismo, el tribunal podrá ordenar la inserción de la sentencia, literalmente o en extracto, en uno o varios periódicos diarios, así como su fijación en tablón de edictos, en las condiciones que determinare y a expensas del condenado."[253]

[250] Código Penal de España, p. 106.
[251] *Ibidem*, pp. 121-127.
[252] *Ibidem*, pp. 129.
[253] *Código Penal de Francia*, Parte legislativa, p. 29.

Artículo 43. "El que habiendo reunido, con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento, informaciones nominativas cuya divulgación tuviere como efecto atentar contra la reputación o la consideración de la persona o la intimidad de la vida privada; hubiere, sin autorización del interesado y a sabiendas, puesto tales informaciones en conocimiento de una persona que no estuviere habilitada para recibirlas a tenor de las disposiciones de la presente ley o de otras disposiciones legales, será castigado con pena de privación de libertad de dos a seis meses y con pena de multa de 2 000 a 20 000 francos, o con una de las dos penas."[254]

Artículo 44 "El que, disponiendo de informaciones nominativas con ocasión de su registro, de su clasificación, de su transmisión o de otra forma de tratamiento las hubiere desviado de su finalidad, según la misma hubiera sido definida, bien en el acto reglamentario previsto en el artículo 15, supra, o en las denuncias formuladas en aplicación de los artículos 16 y 17, bien en una disposición legal, será castigado con pena de privación de libertad de uno a cinco años y con multa de 20 000 a 2000 000 francos."[255]

4.1.3 Austria

La Ley de reforma del Código Penal del 22 de diciembre de 1987, contempla los siguientes delitos:

Destrucción de Datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.

Estafa Informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos.[256]

4.1.4 Alemania

Para hacer frente a la delincuencia relacionado con la informática y con sus efectos, a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo

[254] *Ibidem*, p. 30.
[255] *Ibidem*, p. 31.
[256] J. Castañeda. "La fiebre de los dominios", p. 156.

de 1986 en la que se contemplan los siguientes delitos: Espionaje de datos, Estafa Informática, Falsificación de datos probatorios, Alteración de Datos, Sabotaje Informático, Utilización abusiva de cheques o tarjetas de crédito.

Cabe mencionar que esta solución fue también adoptada en los Países Escandinavos y en Austria. Alemania también cuenta con una Ley de Protección de Datos, promulgada el 27 de enero de 1977, en la cual, en su numeral primero menciona que "el cometido de la protección de datos es evitar el detrimento de los intereses dignos de protección de los afectados, mediante la protección de los datos personales contra el abuso producido con ocasión del almacenamiento, comunicación, modificación y cancelación (proceso) de tales datos. La presente ley protege los datos personales que fueren almacenados en registros informatizados, modificados, cancelados o comunidades a partir de registros informatizados".

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos.[257]

Lo anterior es sólo una muestra de los contenidos en materia legislativa que se tienen en algunos países de la Unión Europea referentes a los Delitos Informáticos, no se puede dejar de mencionar que también cuentan con cuerpos especiales de investigación en el seno de la policía, como es la Unidad de Investigación de Delincuencia en Tecnologías de la Información, y en el seno de la Guardia Civil, con el Grupo de Delitos Tecnológicos, así como la utilización por éstos de medios técnicos cada vez más innovadores, y los esfuerzos legislativos llevados a cabo por los demás miembros en conjunto en su lucha contra el cibercrimen, los cuáles están obteniendo frutos.

De esta manera, los principales delitos tratados por la legislación existente a nivel europeo así como a nivel nacional son los siguientes: delitos contra la intimidad: recogida, almacenamiento, modificación, revelación o difusión ilegales de datos personales; delitos relativos al contenido: difusión, especialmente por Internet, de pornografía, y en especial de pornografía infantil, declaraciones racistas e información que incita a la violencia; delitos económicos, acceso no autorizado y sabotaje: muchos países han aprobado leyes que abordan los delitos económicos perpetrados por ordenador y tipifican nuevos delitos relacionados con el

[257] Ignacio Garrote Fernández-Díez, *El Derecho de Autor en Internet. La directiva sobre derechos de autor y derechos afines en la sociedad de la información*, Granada, Editorial Comares, 2001, p. 93.

acceso no autorizado a sistemas informáticos (por ejemplo, la piratería, el sabotaje informático y la distribución de virus, el espionaje informático, y la falsificación y el fraude informáticos); delitos contra la propiedad intelectual: delitos contra la protección jurídica de programas de ordenador y la protección jurídica de las bases de datos, los derechos de autor y derechos afines.

Asimismo, la Comisión Europea presentará posteriormente propuestas legislativas en los siguientes ámbitos: armonización de las legislaciones de los Estados miembros en el ámbito de los delitos relativos a la pornografía infantil; de los sistemas de derecho penal material en el ámbito de la delincuencia que se sirve de las altas tecnologías y sobre aplicación del principio de reconocimiento mutuo relativo a las medidas cautelares previas a los pleitos vinculados a las investigaciones en materia de delincuencia informática que implican a más que un Estado miembro.

Además de las legislativas, se han previsto otras medidas, en particular: la creación de un foro europeo que reúne a las autoridades encargadas de la aplicación de las leyes, a los proveedores de servicio, operadores de redes, asociaciones de consumidores y autoridades encargadas de la protección de los datos con el fin de intensificar la cooperación a escala comunitaria; la continuación de las acciones en favor de la seguridad y la confianza en el marco de la iniciativa eEuropa, del plan de acción Internet y del programa en el ámbito de las tecnologías de la sociedad de la información (IST); puesta en marcha de otros proyectos en el marco de programas existentes sobre formación del personal; financiación de medidas destinadas a mejorar el contenido y la utilización de la base de datos de las legislaciones nacionales proporcionada por el estudio COMCRIME.

4.2 América del Norte

Los delitos informáticos, la piratería informática y los problemas derivados del mal uso de las computadoras y de la Informática, hacen que América del Norte, en particular Estados Unidos, sea el principal Estado donde se cometen dichos quebrantamientos de la ley. De esta manera, trataré de abordar las principales leyes que se han aprobado o que están en vías de aprobación, tanto en Canadá como en el país anteriormente señalado.

4.2.1 Canadá

Como respuesta al debate sobre el ciberespacio, el gobierno canadiense formó la Junta Consultiva sobre la Autopista de la Información o " Information Highway Advisory Council" (IHAC) en 1994, con el objeto de estudiar y preparar una declaración oficial que se refiera a la determinación de las direcciones que debe tomar Internet en Canadá.

Como uno de los puntos más importantes tratados en el primer reporte de dicha Junta, en septiembre de 1995, se encuentra el relativo a la naturaleza del contenido de la información que puede viajar a través de Internet. Respecto a este punto se estableció el exigir un control sobre dos asuntos fundamentales:

- Obscenidad y Racismo.
- Material promotor del odio y la violencia.

Asimismo, cuenta con legislación referente a nuestra materia de estudio, entre las cuales destacan:

- Ley de acceso a los documentos de los Organismos Públicos y de protección de datos personales de 12 junio 1982 de Québec, modificada en 1 de marzo de 1987.[258]
- Adhesion en 1984 a las Guidelines on the Protection of Privacy and Transborder Flows of Personal Data de 1980
- Criminal Law Amendement Act de 20 de junio de 1985.
- Ley de la Provincia de *Ontario* de 1987**.**
- The Privacy Act, 1991. Privacy Commissioner of Canada. *Ottawa.*
- Ley sobre la protección de datos personales para el sector privado.[259]
- Uniform Electronic Evidence Act. Adoptada por la Conferencia de Ley Uniforme de Canadá en Agosto de 1998.
- The Uniform Electronic Commerce Act.[260]
- Electronic Information, Documents and Payments, Bill 70, 2000. Ontario Province.

El Gobierno canadiense dio un plazo hasta el año 2000 para ejecutar la legislación federal por lo que atañe al sector privado, aunque las provincias (excepto Québec) todavía tienen que

[258] Loi sur l´accès aux documents des organismes publics et sur la protection des renseignements personnels. *Quebec* 1982.
[259] Loi sur la protection des renseignements personnels dans le secteur privé (sanctionné le 15 juin 1993).
[260] Adoptada por la Conferencia de Ley Uniforme de Canadá el 30 de septiembre de 1999.

mostrar una voluntad mayor para seguir su ejemplo, en lo que se refiere a aquellos sectores económicos privados para los cuales tienen competencia.

Por otra parte las leyes que ya están en vigor son las siguientes:

- Ley sobre la protección de datos personales y documentos electrónicos.[261]
- Acta sobre Protección de información personal y documentos electrónicos del 1º de mayo de 2000.
- Acta de Comercio Electrónico del 16 de octubre de 2000.
- Acta de Comercio Electrónico e Información del 16 de octubre de 2000.
- Acta sobre Información personal y documentos electrónicos.
- Acta sobre documentos e información electrónica del 1º de noviembre de 2000.
- Acta de transacciones electrónicas del 5 de abril de 2001.

En términos generales podríamos decir, que el gobierno canadiense, eventualmente ha ido buscando la manera de regular aquellos temas que puedan constituir un atentado contra las buenas costumbres y el orden público de la sociedad (racismo, obscenidad, terrorismo, etc.). Sin embargo, hasta ahora no se han propuesto nuevas leyes que se apliquen específicamente a Internet y a los delitos que de este se derivan.

4.2.2 Estados Unidos

Por su parte en Estados Unidos de América se adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986, con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya, etcétera, y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

Es interesante también señalar que el Estado de California, en 1992 adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta ley de 1994.[262]

---

[261] Loi sur la protection des renseignements personnels et les documents électroniques

[262] The Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, (conocido como Anti-terrorism Act). En http://216.110.42.179/docs/usa.act.final.102401.html (12/12/2001)

Las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10000 por cada persona afectada y hasta $50000 el acceso imprudencial a una base de datos, etc. Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus[263] conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

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

Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, estas leyes son un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

El aumento en la cantidad de casos de hacking y la sensación de inseguridad permanente que generaron,[264] cambiaron la percepción de las autoridades con respecto a los hackers y sus ataques, así, surge el FCIC (Federal Computers Investigation Commitee), que es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente.[265]

Además existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias. Sus integrantes son "forenses de las computadoras" y trabajan, además de los Estados Unidos, en el Canadá, Taiwán e Irlanda.

---

[263] Conocidos como computer contaminant

[264] Fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas

[265] El FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

Así, en la mayoría de los Códigos Penales de los Estados Unidos se ha tipificado una figura de destrucción de datos y sistemas informáticos, como se muestra a continuación:

- **Fair Credit Reporting Act**, **del 26 de octubre de 1970**, no menciona en ningún momento los sistemas de tratamiento automatizado de datos, sus previsiones sobre la recogida, conservación y transmisión a terceros de informes sobre la solvencia personal, profesional o económica de las personas y los derechos que a los afectados reconocía para su protección, inauguran una técnica que, posteriormente, se aplicará también a la tutela de las informaciones personales introducidas y tratadas en computadoras.
- **The Family Education Rights Act**, de 1974 sobre los expedientes académicos.
- **The Freedom of Information Act, de 1974** (U.S. Code.) También conocida como FOI Act o FOIA, que exime al gobierno de hacer públicos sus archivos cuando esto suponga una injustificada invasión de la intimidad de las personas.
- **Public Law 93-579 del 31 de diciembre de 1974** llamada Privacy Act of 1974, modificada varias veces, por última vez en 1988 (Computer matching act).[266]

Además existen leyes de alcance sectorial, unas tendentes a regular la protección de los datos en contextos específicos (servicios postales, comunicaciones electrónicas, datos médicos, crédito, servicios financieros, uso de grabaciones magnetoscópicas, etc.).

Varias leyes contienen preceptos que inciden en la protección de datos en el respectivo contexto: ley federal de Procedimiento Administrativo, ley de Comunicación por Cable, ley de Reforma Tributaria, ley de Interferencias de las Telecomunicaciones y casi todos los estados cuentas con leyes de alcance sectorial, tales son:

- **The Tax Reform Act**, **de 1978** sobre la confidencialidad de los datos bancarios.
- **The Electronic Fund Transfer Act, de 1978** sobre la obligación de las instituciones financieras que efectúen transferencias electrónicas u otros servicios bancarios por ese procedimiento, de informar a sus clientes del acceso de terceras personas a sus bancos de datos.
- **The Privacy Protection Act, de 1980** sobre la tutela especial que se establece en favor de periodistas o informadores limitando las facultades de los agentes públicos

[266] En su exposición de motivos indicaba que "El Congreso estima que la privacidad de un individuo es afectada directamente por entes y órganos federales... el creciente uso de ordenadores y de una tecnología compleja de la información si bien es esencial para el eficiente funcionamiento de las Administraciones Públicas, ha aumentado grandemente el detrimento que para la privacidad individual puede derivarse de cualquier captación, conservación, uso y difusión de información personal"

dedicados a la persecución de los delitos en relación con el registro de sus materiales de trabajo.

- **Counterfeit Access Device and Computer Fraud and Abuse Act de 1984** que trata sobre el acceso a los datos, su utilización y destrucción que recortaba las competencias federales en esta materia.
- **The Cable Communications Policy Act de 1984** que prohibía los servicios de divulgación de información por cable, salvo que hubiese consentimiento por parte de la persona de la que se mandaban los datos.
- **Electronic Communication Privacy Act de 1986** que respondía a las necesidades de defensa de la privacidad en las nuevas formas de comunicación. Prohíbe la interceptación de mensajes mandados por medio de esta tecnología, define todo lo relativo a comunicaciones electrónicas,[267] establece las sanciones civiles y penales por infringir la normativa, etc.
- **The Computer Security Act of 1987.** Información sobre las leyes que regulan y protegen los sistemas de computación y desarrollan la criptografía en el Gobierno de Estados.
- **The Computer Matching and Privacy Act de 1988** para prevenir el excesivo desarrollo que se estaba produciendo en la elaboración de dossiers automatizados, y por lo tanto el más que probable intercambio de datos personales entre las compañías sobre todo del sector privado.[268]

Asimismo, en 1997 el Presidente de Estados Unidos, William Clinton, presentó un documento denominado **"Marco para el Comercio global Electrónico"**, para evitar toda imposición por parte del Gobierno Federal de impuestos especiales para las transacciones comerciales y las prestaciones de servicios efectuados por y a través de Internet.

[267] Correo electrónico, transmisiones vía satélite, telefonía celular, etc.

[268] También se encuentran la The Telephone Consumer Protection Act of 1991, la Ley de Privacidad del Estado California de 1992, la ABA, Resolution concerning the CyberNotary, la Driver´s Privacy Protection Act of 1994, la Communication Decency Act de 1996, la The Electronic Signature Act Florida, de mayo de 1996 que reconoce la equivalencia probatoria de la firma digital con la firma manual, la Ley de referencia de la firma digital, para los legisladores de los Estados Unidos, de1 de agosto de 1996.The Massachusetts Electronic Records and Signature Act de 1996 que recoge todo mecanismo capaz de proporcionar las funciones de la firma manuscrita sin ceñirse a un tipo concreto de tecnología, la Georgia Electronic Records and Signatures Act, del 22 de abril de 1997, The Electronic Commerce Act de 30 de mayo de 1997, que hace referencia al cybernotary, la Consumer Internet Privacy Protection Act of 1997, la Fair health Information Practices Act of 1997, la Children´s Privacy Protection and Parental Empowerment Act of 1997 que prohíbe la venta de información personal acerca de los niños sin el consentimiento de sus padres, la Social Security ON-line Privacy Protection Act of 1997, la Personal Information Privacy Act of 1997 y la American Family Privacy Act of 1997

Por otra parte, el vicepresidente Al Gore, envió un Comunicado sobre intimidad en julio de 1998, el cual se refiere a un conjunto de medidas que representan el próximo gran paso a la materialización de la "Declaración de derechos electrónicos" en cuatro áreas amplias y esenciales: información personal comprometida, suplantación de identidad, protección de la intimidad de los niños e iniciativas voluntarias del sector privado.

Las leyes y proyectos de ley presentados en la Casa de Representantes en 1998 y 1999, tienen que ver en su mayoría con derechos financieros y comerciales, es decir, dan seguridad a estos aspectos, tal es el caso de la **Digital millenium copyright Act**, del 8 de octubre de 1998, la **Financial Services Act of 1999** y la **Financial Information Privacy Act of 1999.**

Del mismo modo se crearon leyes para la protección de información personal, ya sea referente a cuestiones de salud, de comercio o de derechos sociales, en este rubro están:

- **Personal Privacy Protection Act**,
- **Integrity in Voter Registration Act of 1999**,
- **Social Security Integrity Act,**
- **Freedom and Privacy Restoration Act of 1999**,
- **Federal Employment Applicant Drug Testing Act,**
- **Genetic Information Nondiscrimination in Health Insurance Act of 1999,**
- **Maintenence of Protected Health Information**,
- **Consumer Internet Privacy Protection Act of 1999**,
- **Drug-Free Ports Act,**
- **Collections of Information Antipiraty Act,**
- **Patients´ Bill of Rights Act of 1999**,
- **Social Security On-line Privacy Protection Act of 1999,**
- **Safe Schools Internet Act of 1999**,
- **Children´s Privacy Protection and Parental Empowerment Act of 1999,**
- **Wireless Communications and Public Safety Act of 1999,**
- **Patient Protection Act of 1999,**
- **Wireless Privacy Enhancement Act of 1999,**
- **Know your Customer´ Sunset Act**,
- **FinCen Public Accountability Act,**
- **Bank Secrety Sunset Act,**

- **Parent-Child Privilege Act of 1999,**
- **American Financial Instituions´ Privacy Act**,
- **Childrens´ Internet Protection Act**,
- **Fraud Prevention Act of 1999**,
- **Know your Customer regulations Termination Act,**
- **Know your Customer programa abolishement Act,**
- **Prohibition of "Know your Customer" Regulations**,
- **Privacy Promotion Act,**
- **Congressional Research Accessibility Act,**
- **Security and freedom through Encryption (SAFE) Act**,
- **Freedom to E-file Act**,
- **Childrens´ Internet Protection Act,**
- **Consumer Credit Report Accuracy and Privacy Act of 1999**,
- **Medical information Privacy and Security Act,**
- **Protection of Children from On-line Predators and Exploitation Act of 1999,**
- **Personal Information Privacy Act of 1999**,
- **Electronic Signatures in Global and National Commerce Act of 1999,**
- **Personal Data Privacy Act of 1999**,
- **Electronic Privacy Bill of Rights Act of 1999,**
- **Uniform Electronic Transactions Act** del 29 de Julio de 1999 y
- **Uniform Computer Information Transactions Act,** de la misma fecha.[269]

A partir del año 2000, las leyes se enfocan hacia la protección de los niños, las transacciones en línea, la seguridad en Internet, la privacidad personal, la identificación de crackers, hackers, gurus, etc, y la protección de datos de salud en referencia a los archivos médicos y razones sociales, así la **Department of Transportation and Related Agencies Appropriations Act 2000**, eliminó los proyectos federales que se tenían para licitar la

[269]A lo largo de 1999, se fueron incrementando las leyes referente al tema tratatado, tal es el caso de la Commerce Comittee of U.S., el Proyecto para proteger las direcciones en Internet del 28 de octubre de 1999, con el que se busca combatir la especulación cibernética que se da con la adquisición de dominios en Internet, la Government Secretary Reform Act of 1999, la Financial Information Privacy Acto of 1999, la Federal Comisión o Statistical Policy Act of 1999, la .Patinets´ Bill of Right Act of 1999, la Patients´ Bill of Rights Plus Act, la Congressional Openness Act, la Clone Pager Authorization Act of 1999, la American Financial Institutions Privacy Act of 1999, la Genetic Information Nondiscrimination in Health Insurance Act of 1999, la Medical Information Privacy and Security Act y la Financial Services Modernization Act of 1999.

construcción de carreteras, con lo cual se evitó que se obtuvieran datos de las licencias de conducir, los registros de motores de vehículos o fotografías provenientes de los archivos de los conductors; surgió también la **Children´s Online Privacy Protection Act,** la **Secure Online Communication Enforcement Act of 2000**, la **Privacy Commission Act,** la **Online Privacy and Disclosure Act,** la **Identity theft Protection Act of 2000,** la **Child Support Distribution Act of 2000,** la **Medical Financial Privacy Protection Act,** la **Social Security Number Protection Act of 2000**, la **Privacy and Identy Protection Act of 2000,** la **Notice of Electronic Monitoring Act,** la **Digital Privacy Act of 2000**, la **Electronic Communications Privacy Act of 2000**, la **Freedom from Behavioral Profiling Act of 2000**, la **Amy Boyer´s Law**, la **Consumer Privacy Protection Act,** la **Privacy Policy Enforcement in Bankruptcy Act of 2000**, la **Consumer Internet Privacy Enhancement Act** y la **Electronic Signatures in Global and National Commerce Act.**

He de destacar que el 29 de Septiembre de 2000, el estado de California, aprueba una **ley contra los delitos informáticos.**

Paralelamente, el parlamentario demócrata Rick Boucher presentó al Congreso estadounidense un proyecto de ley denominado "Ley de 2000 sobre Derechos del Propietario de Música", el cual se buscaba dar legalidad a la creación de bases de datos con audio, que hagan posible compartir archivos musicales entre personas que hayan comprado la música previamente.[270]

Siguiendo con la línea anterior, en 2001, a raíz de los ataques del 11 de septiembre,[271] se toman medidas más a fondo para evitar ataques posteriores, o por lo menos para tratar de localizar puntos débiles de los sistemas informáticos, con penas mucho más severas, se empieza por controlar el Spyware, a proteger más los datos personales, etc., por lo tanto surgen la **Spyware Control and Privacy Protection Act of 2001**, la **Federal Employee Protection Act of 2001,** la **Wireless Privacy Protection Act of 2001,** la **Consumer Online Privacy and Disclosure Act,** la **Student Privacy Protection Act y la Privacy Commission Act.**

[270] Explicando su iniciativa, el congresista señaló que "Un consumidor que legalmente es dueño de un trabajo musical, tal como un CD, podrá almacenarlo en Internet y utilizarlo para fines personales en el momento y lugar que lo desee". De acuerdo a Boucher, esto no afectaría las regalías y los derechos de autor ya que los consumidores deben probar que son dueños de la música que van a descargar. Esta ley tiene relevancia para futuros juicios como los que han enfrentado a la industria discográfica estadounidense, representada por la asociación RIAA y los sitios de intercambio de música Napster, MP3.com y otros. En cualquier caso, la ley llegó demasiado tarde para MP3.com, que ya ha pagado 20 millones de dólares para llegar a un acuerdo extrajudicial con cuatro sellos discográficos y 118 millones de dólares sólo para evitar un juicio con Universal Music.

[271] Ver capítulo III, del presente trabajo.

Es hasta 2003, cuando Estados Unidos, preocupado por su seguridad nacional, enfatiza las reglas sobre Internet, preocupándose esta vez, desde la seguridad de la información personal, hasta de la seguridad en aeropuertos, teléfonos, seguridad doméstica, terrorismo internacional, seguridad social, telemarketing, genoma humano, beneficios federales, etc. Se empieza con la **Global Internet Freedom Act,** que desarrolla y aplica tecnologías sobre sensores de Internet y probables conflictos en torno a éste, con fecha del 7 de enero de 2003, le siguió la **Online Privacy Protection Act of 2003**, en la cual se estipula que se requiere de la Comisión Federal para prescribir regulaciones a la protección de la información personal, lo que provee un mayor control de la información, la **Digital Media Consumers' Rights Act of 2003,** contiene información relativa a la venta o transferencia de música por Internet, la **Aviation Biometric Badge Act,** maneja cuestiones referentes a la seguridad en Aeropuertos, usando bandas de seguridad biométricas, la **Comprehensive Homeland Security Act of 2003**, contiene los fundamentos para la implementación de seguridad doméstica, entre otras cosa, la **Equal Rights and Equal Dignity for Americans Act of 2003**, protege los derechos civiles de todos los estadounidenses, la **Justice Enhancement and Domestic Security Act of 2003**, provee de seguridad doméstica, el Acta denominada **To exclude United States persons from the definition of `foreign power' under the Foreign Intelligence Surveillance Act of 1978,** relacionada con el terrorismo internacional, la **Data-Mining Moratorium Act of 2003,** impone una moratoria sobre los datos totales que posee el Departamento de Defensa y el programa para la Seguridad Nacional, con fecha del 16 de enero de 2003, la **Illicit Drug Anti-Proliferation Act of 2003,** prohíbe el mantenimiento, control, renta, traspaso, manufactura o distribución de droga, ya sea para consumo o venta.

La **Do-Not-Call Implementation Act**, autoriza a la Comisión Federal para colectar entradas para la implementación y aseguramiento de las llamadas privadas y sus registros, la **Domestic Consumer Safety Act of 2003**, creada para la seguridad de las personas que necesitan trabajadores en sus hogares, es un sistema en el cual se revisa un archivo de los trabajadores autorizados por las mismas compañías de mantenimiento, la **Telemarketing Relief Act of 2003**, aborda una lista de números telefónicos de las personas que no requieren o quieren recibir llamadas telefónicas con propósitos de telemarketing, la **DNA Database Completion Act of 2003**, autoriza un programa para la eliminación de la red nacional de registros y obtención del ADN, asimismo, se hizo una simple copia de los registros de ADN de los presos calificados como altamente ofensivos, la **Child Sex Crimes Wiretapping Act of 2003**, la cual dice que

ciertos delitos sexuales contra los menores, se deben a la intercepción de comunicaciones, la **Family Dinnertime Protection Act of 2003**, la cual contiene limitaciones a las llamadas de telemarketing de las 5:30 p.m. a las 7:30 p.m., la **Foreign Intelligence Collection Improvement Act of 2003,** establece la Agencia de Inteligencia de la Nación, la **Clear Your Good Name Act:** es una ley que requiere agencias federales para impugnar los registros de arresto ciudadanos.

La **Prevent Bank Fraud by Terrorists Act of 2003**: para prevenir que los terroristas y lavadores de dinero, establezcan cuentas bancarias para transferencias bancarias usando falsos números de seguro social falso o números de identificación al pagar impuestos, la : **Benefit Authors without Limiting Advancement or Net Consumer Expectations (BALANCE) Act of 2003**: salvaguarda los derechos y expectativas de los consumidores que adquirieron legalmente entretenimiento digital, la **Computer Owners Bill of Rights:** protege a los dueños de las computadoras, la **Product Safety Notification and Recall Effectiveness Act of 2003**: es una ley que lleva directamente la Comisión de Productos seguros para el Consumidor, la cual promulgó una regla que requiere un certificado de ciertos productos para la estabilidad y mantenimiento de un sistema computacional.

La **Child Obscenity and Pornography Prevention Act of 2003**: la cual previene el tráfico de pornografía y obscenidad infantil, la **Iris Scan Security Act of 2003:** Establece garantías para las agencias federales para utilizar la tecnología de escaneo del iris, lo que lleva a un expediente judicial de las personas, es utilizado para aquellas que deseen comprar un arma, la **Economic Opportunity Protection Act of 2003:** extiende las limitaciones de ciertas provisiones de la Ley del Estado, sobre el Acta del Reporte de crédito de 2003, la **Federal Courts Improvement Act of 2003:** esta ley hace mejoras a la operación y administración de las Cortes Federales, la **United States Commission on an Open Society with Security Act:** establece la Comisión de los Estados Unidos sobre Sociedad Abierta con Seguridad, la **Privacy Act of 2003:** la cual menciona que se requiere del consentimiento individual de la personal para vender ó promover su información personal de identificación.

La ley llamada **Private Security Officer Employment Authorization Act of 2003**: permite obtener un resumen de los registros criminales de las personas que aplican a un puesto de empleo en las oficinas de seguridad privada, la **Second Chance for Ex-Offenders Act of 2003:** permite impugnar los registros de ciertos actos no violentos, la **CAN-SPAM Act:** regula el comercio interestatal, imponiendo limitaciones y penalizaciones en la transmisión de correos comerciales no solicitados vía Internet, la **Stop Taking Our Health Privacy (STOHP) Act of**

2003: restaura la protección de las cédulas de identificación de salud personal que fueron debilitados en agosto de 2002, la **Student Privacy Protection Act of 2003:** logra que los estudiantes y los padres, tengas derechos sobre la violación de sus derechos de privacidad bajo la Provisión de Educación General.

En cuestiones de seguridad personal, surge la **Genetic Nondiscrimination in Health Insurance and Employment Act,** que prohíbe la discriminación sobre las bases de la información genética con respecto a la seguridad social, la ley **To reduce unsolicited commercial electronic mail and to protect children from sexually oriented advertisements:** la cual regula y protege a los niños de la pornografía infantil vía mail, la **Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003**: la cual asegura que los correos electrónicos con contenido comercial no solicitados, pueden ser revisados para identificar a la persona o compañía que lo envió.

En lo relativo a seguridad aérea y portuaria, surgen la **Aviation Security Technical Corrections and Improvements Act of 2003,** la cual hace correcciones técnicas en cuestiones de seguridad aérea, y la **Port Security Improvements Act of 2003,** que previene de ataques en Puertos.

Asimismo, surge la **Antiterrorism Tools Enhancement Act of 2003,** con el fin de fortalecer las herramientas de investigación antiterrorista,[272] de igual forma se aprueba la **Government Network Security Act of 2003,** para asegurar las agencias federales en el desarrollo e implementación de protección de la seguridad y privacidad de los sistemas computacionales del gobierno y de los riesgos de compartir archivos, la **Database and Collections of Information Misappropriation Act,** la cual prohíbe la apropiación de ciertas bases de datos, la **Gun Show Loophole Closing Act of 2003:** la cual contiene estadísticas de los criminales que se dedican a las transacciones ó venta de armas de fuego.

Como se puede observar, es en este país, donde la legislación contempla varios de los delitos informáticos mencionados en el Capítulo II de este trabajo, no está por demás mencionar que, uno de cada tres ataques informáticos que suceden en el mundo proceden de ordenadores o servidores estadounidenses,[273] Estados Unidos es el país del mundo que genera más actividad delictiva en Internet, además, es el punto de encuentro de los hackers más sofisticados del

[272] Ver capítulo III, del presente trabajo.

[273] Según un estudio sobre seguridad en Internet hecho por la empresa Symantec. El informe señala también que China, con un 10% de todos los ataques, y Alemania, con un 7%, también son focos importantes de agresiones. Symantec asegura que el delito que más prolifera en la red es la sustracción de datos personales y bancarios, y que el spam supone ya el 59% del tráfico mundial de e-mails.

mundo,[274] los cuales en estos últimos 2 años han creado códigos pensados para robar datos e información confidencial que puede ser utilizada para obtener un ganancia económica. Los cibercriminales siguen haciendo herramientas cada vez más perfectas para que sus ataques no sean detectados y, al mismo tiempo, crear una red de colaboración que permite el crecimiento continuado de este tipo de delitos.[275]

Estados Unidos también lidera lo que se llama "bots network activity",[276] en donde el dueño del ordenador normalmente no sabe que su máquina está siendo atacada y en este fenómeno tiene un papel muy importante el correo "basura", que inunda todos los días nuestros mails, el cuál no deja de crecer año con año.[277]

Los Estados Unidos también es el centro de operaciones de más de la mitad de la economía de servidores clandestinos. Estos servidores son usados para facilitar transacciones fuera de la ley de datos robados.

4.3 Centroamérica y Sudamérica

La difusión de la informática ha llegado a todos los ámbitos de la actividad humana. La reglamentación que busca una forma de convivencia más armónica dentro de las sociedades, tratando de prevenir o castigar las conductas que riñen con el bienestar de la mayoría, no está exenta de los efectos de este nuevo medio.

Algunos países de Centro y Sudamérica, han estado legislando sobre temas relativos a la comisión de delitos vinculados a la informática, ya sea porque utilizan herramientas informáticas para realizarlos, o porque el blanco de la infracción es de índole informática[278].

[274]Symantec hace este estudio cada seis meses, pero es la primera vez que identifica el país de origen de los ataques informáticos. Para llevarlo a cabo, el informe se ha centrado en la actividad de los 120 millones de ordenadores que tienen instalado sus antivirus en los últimos seis meses.
[275]Los informáticos de Symantec han descubierto también que la fuerte competencia en este "inframundo" criminal está haciendo caer los precios de información financiera robada. Así, los criminales ofrecen números de tarjeta de crédito verificados por un dólar, y es posible adquirir una identidad completa (fecha de nacimiento, número de cuenta bancaria, número de tarjeta de crédito y número de carné de identidad) por sólo catorce dólares.
[276]Es decir, ordenadores comprimidos controlados remotamente que operan para producir grandes cantidades de spam y otros ataques dañinos.
[277]Según Symantec, en el segundo semestre del año pasado el 59% de todo el tráfico de e-mail en el mundo es spam. Este supone un 5% más que el periodo anterior.
[278] En este apartado se verán las legislaciones de El Salvador, Costa Rica, Venezuela, Chile, Argentina y Ecuador.

4.3.1 El Salvador

El Salvador es uno de los países que se encuentra en este momento presentando y discutiendo una ley acerca de delitos informáticos. La propuesta de ley tipifica los delitos informáticos, y contempla en la categoría de delitos contra los sistemas que utilizan tecnologías de información los siguientes: el Acceso indebido; el Sabotaje o daño a sistemas; el Sabotaje o daño culposos, es decir, cometido por imprudencia, negligencia, impericia o inobservancia de las normas establecidas; el Acceso indebido o sabotaje a sistemas protegidos; la Posesión de equipos o prestación de servicios de sabotaje; el Espionaje informático; y la Falsificación de documentos.

En la categoría de delitos contra la propiedad, se incluyen: el Hurto; el Fraude; la Obtención indebida de bienes o servicios; el Manejo fraudulento de tarjetas inteligentes o instrumentos análogos; la Apropiación de tarjetas inteligentes o instrumentos análogos; la Provisión indebida de bienes o servicios; y la Posesión de equipo para falsificaciones.

Entre los delitos contra la privacidad de las personas y de las comunicaciones, se hallan: la Violación de la privacidad de la data o información de carácter personal; la Violación de la privacidad de las comunicaciones; y la Revelación indebida de data o información de carácter personal.

En la clase de los delitos contra niños o adolescentes, se incluyen: la Difusión o exhibición de material pornográfico; y la Exhibición pornográfica de niños o adolescentes.

Finalmente, en cuanto a los delitos contra el orden económico, se consideran como tales: la Apropiación de propiedad intelectual; y la Oferta engañosa. La ley contempla las penas que se aplicarán en cada uno de los delitos incluidos, así como los agravantes que pueden suceder en estos delitos.

Del mismo modo se aplican algunos artículos del Código Penal de la República del Salvador a algunos delitos informáticos mencionados anteriormente, tal es el caso del Artículo 154, que dice: “El que amenazare a otro con producirle a él o a su familia, un daño que constituyere delito, en sus personas, libertad, libertad sexual, honor o en su patrimonio, será sancionado con prisión de uno a tres años.”[279]

[279] Se refiere a las amenazas que atentaren contra la seguridad de la persona y su familia a través de medios electrónicos y/o que pudiesen ser anónimos. Por ejemplo: amenazas de muerte a profesores universitarios a través de correo electrónico.

La promoción de pornografía infantil, exhibiciones obscenas a través de Internet y correo electrónico, por ejemplo la promoción de pornografía a través de páginas web, así como el envío de imágenes por medio de correo electrónico, la inducción, promoción, favorecimiento y determinación de la prostitución a través de Internet y correo electrónico, por ejemplo: el envío de correos electrónicos a distintas personas para que accedan a un sitio pornográfico, se encuentran regulados en el Artículo 155 del Código Penal.

También se encuentran tipificados los siguientes delitos:

- Intercepción de mensajes electrónicos y otra información.
- Obtención de claves de acceso y/o información electrónica.
- Divulgación de secretos profesionales.
- Violación de comunicaciones privadas
- Violación agravada de comunicaciones
- Captación de comunicaciones
- Revelación De Secreto Profesional
- Robo de hardware
- Robo de títulos valores a través de transacciones electrónicas
- Robo de capital por medio de infiltración electrónica a cuentas varias, personales, comerciales y estatal.
- Estafa electrónica para beneficio propio y terceros. Por ejemplo: los empleados pueden modificar los balances de las cuentas bancarias para su beneficio.
- La reproducción de software, con fines de lucro.
- La reproducción de música y video, con fines de lucro.
- Comercialización de sistemas sin autorización previa del programador.
- Adjudicarse una obra electrónica.
- Violación de distintivos.
- Violación de Derechos de Autor y Derechos Conexos

4.3.2 Costa Rica

Este país adicionó los artículos 196 bis, 217 bis y 229 bis al Código Penal, para reprimir y sancionar los delitos informáticos, quedando de la siguiente manera:

- Artículo 196 bis: Violación de comunicaciones electrónicas. “Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."[280]
- Artículo 217 bis: Fraude informático. “Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.”[281]
- Artículo 229 bis: Alteración de datos y sabotaje informático. “Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años."[282]

4.3.3 Venezuela

Recientemente se publicó la Ley sobre Delitos Informáticos, cuyo objetivo es proteger los sistemas que utilicen tecnologías de información, así como prevenir y sancionar los delitos cometidos contra o mediante el uso de tales tecnologías.

Se trata de una ley especial que descodifica el Código Penal y profundiza aún más la incoherencia y falta de sistematicidad de la legislación penal, con el consecuente deterioro de la seguridad jurídica.

---

[280] *Código Penal de Costa Rica*, consultado en: http://www.unifr.ch/derechopenal/legislacion/cr/index.htm el 14 de marzo de 2007, 15:37 hrs.
[281] *Ídem*
[282] *Idem*.

La Ley define los términos tecnología de la información, sistema, data, documento, computadora, hardware, firmware, software, programa, procesamiento de datos o de información, seguridad, virus, tarjeta inteligente, contraseña y mensaje de datos.

Pretende ser un Código Penal en miniatura, elabora cinco clases de delitos:

- Contra los sistemas que utilizan tecnologías de información;
- Contra la propiedad;
- Contra la privacidad de las personas y de las comunicaciones;
- Contra niños y adolescentes y;
- Contra el orden económico.

Asimismo, castiga los delitos contra los sistemas que utilizan tecnología de información quedando los siguientes:

- El acceso indebido a un sistema;
- El sabotaje o daño a sistemas, incluyendo cualquier acto que altere su funcionamiento;[283]
- La posesión de equipos o prestación de servicios para actividades de sabotaje;
- El espionaje informático, que incluye la obtención, difusión y revelación de información, hechos o conceptos contenidos en un sistema;[284] y
- La falsificación de documentos mediante el uso de tecnologías de información o la creación, modificación o alteración de datos en un documento.[285]

Asimismo los delitos contra niños y adolescentes son los siguientes:

- La difusión o exhibición de material pornográfico sin la debida advertencia para que se restrinja el acceso a menores de edad;[286] y
- La exhibición pornográfica de niños o adolescentes, penado con prisión de cuatro a ocho años y multa de 400 a 800 UT.

El último capítulo contempla los delitos contra el orden económico, que son los siguientes:

---

[283] Si se trata de sabotaje o daño culposo, la pena se reduce entre la mitad y dos tercios. Si se trata de sabotaje o acceso indebido a sistemas protegidos, la pena aumenta entre la tercera parte y la mitad.

[284] Penado con prisión de tres a seis años y multa de 300 a 600 UT. Si el delito se comete para procurar un beneficio para sí o para otro, la pena aumenta entre un tercio y la mitad. El aumento será de la mitad a dos tercios si se pone en peligro la seguridad del Estado, la confiabilidad de la operación de las personas afectadas o si como resultado de la revelación alguna persona sufre un daño

[285] Si el delito se comete para procurar un beneficio para sí o para otro, la pena aumenta entre un tercio y la mitad. Si el hecho resulta en un perjuicio para otro, el aumento será de la mitad a dos tercios.

[286] Penado con prisión de dos a seis años y multa de 200 a 600 UT.

- La apropiación indebida de propiedad intelectual mediante la reproducción, divulgación, modificación o copia de un software, penado con prisión de uno a cinco años y multa de 100 a 500 UT; y
- La oferta engañosa de bienes o servicios mediante la utilización de tecnologías de la información, penado con prisión de uno a cinco años y multa de 100 a 500 UT, sin perjuicio de la comisión de un delito más grave.

Además de las penas principales indicadas anteriormente, se impondrán, sin perjuicio de las establecidas en el Código Penal, las siguientes penas accesorias:

- El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos previstos en los artículos 10 y 19 de la Ley.[287]
- Trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos los artículos 6 y 8 de la Ley.[288]
- La inhabilitación para el ejercicio de funciones o empleos públicos; para el ejercicio de la profesión, arte o industria; o para laborar en instituciones o empresas del ramo por un período de hasta tres años después de cumplida o conmutada la sanción principal, cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función público, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privada.
- La suspensión del permiso, registro o autorización para operar o para ejercer cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información, hasta por el período de tres años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se valió de o hizo figurar a una persona jurídica.
- Además, el tribunal podrá disponer la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Lo cierto es que a pesar del intento por legislar en esta materia, la Ley llena parcialmente un vacío legislativo en una materia de mucha importancia, ya que presenta, además, varias deficiencias y problemas, entre los que se puede mencionar los siguientes:

[287] Posesión de equipos o prestación de servicios de sabotaje y posesión de equipos para falsificaciones.
[288] Acceso indebido y favorecimiento culposo del sabotaje o daño.

- Utiliza términos en el idioma inglés, cuando la Constitución de la República Bolivariana de Venezuela solo autoriza el uso del castellano o lenguas indígenas en documentos oficiales;
- No tipifica delito alguno relativo a la seguridad e integridad de la firma electrónica y a su registro;
- La terminología utilizada es diferente a la de la Ley de Mensaje de Datos y Firmas Electrónicas, tal como se observa en la definición que hace del mensaje de datos con lo que se propicia un desorden conceptual de la legislación en materia electrónica;
- Repite delitos ya existentes en el Código Penal y en otras leyes penales, a los cuales les agrega el medio empleado y la naturaleza intangible del bien afectado;
- Tutela los sistemas de información sin referirse a su contenido ni sus aplicaciones;
- No tutela el uso debido de Internet; y
- Establece principios generales diferentes a los establecidos en el libro primero del Código Penal, con lo cual empeora la descodificación.

4.3.4 Chile

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La Ley 19223 publicada en el Diario Oficial el 7 de junio de 1993 señala que la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco.[289]

Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años.[290]

El hacking, definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito.

[289]Artículo 1° "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo".

[290]Artículo 2° " El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años.[291]

En su Artículo 3° la Ley nos dice: "El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."[292]

Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.

4.3.5 Argentina

Tiene una Ley de Delitos Informáticos con fecha del 21 de noviembre de 2001, la cual, maneja el Acceso Ilegítimo Informático en su Artículo 1º, el daño informático en el 2º y el Fraude Informático, en el Artículo 5º, también, define al sistema informático como "todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio."[293]

Asimismo se busca, de alguna manera, cubrir las lagunas legales que fueron quedando luego de la incorporación de cierta protección a determinados intangibles en su derecho positivo nacional. Es importante aclara que, como política de legislación criminal, se ha optado por incluir estos delitos en una ley especial y no mediante la introducción de enmiendas al Código Penal, fundamentalmente para no romper el equilibrio de su sistemática y por tratarse de un bien jurídico novedoso que amerita una especial protección jurídico-penal.

Asimismo, se ha optado por incorporar el acceso ilegítimo informático, en la que por acceso se entiende todo ingreso no consentido, ilegítimo y a un sistema o dato informático. Esto representa una figura base porque su aplicación se restringe a aquellos supuestos en que no media intención fraudulenta ni voluntad de dañar, limitándose la acción a acceder a un sistema o dato informático que se sabe privado o público de acceso restringido, y del cual no se posee autorización así se concluye que están excluidos de la figura aquellos accesos permitidos por el

[291] Artículo 4° "El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado"
[292] Pedro De Miguel Asensio, *op. cit.*, p. 123.
[293] Artículo 6º de la *Ley de Delitos Informáticos*.

propietario u otro tenedor legítimo del sistema, además se consideró apropiada, la fijación de una pena de multa, ya que se trata de una figura básica que generalmente opera como antesala de conductas más graves, por lo que no amerita pena privativa de la libertad.

Se añade también la configuración del tipo, que es la intencionalidad de acceder a un sistema de carácter restringido, es decir, sin consentimiento expreso o presunto de su titular, se contempla la pena de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información, como modalidad más gravosa de afectación del bien jurídico tutelado por la circunstancia que supone la efectiva pérdida de la exclusividad de la información.[294]

Por último, se contempla como agravante de ambas modalidades de esta figura delictiva, la circunstancia que los sistemas o datos informáticos sean concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos, en cuyo caso la pena prevista va desde los seis meses hasta los seis años de prisión.[295]

El daño o sabotaje informático se contempla en el artículo 183 del Código Penal, aunque que sólo contempla las cosas muebles. La jurisprudencia de Argentina, sostuvo que el borrado o destrucción de un programa de computación no es una conducta aprehendida por el delito de daño,[296] pues el concepto de cosa es sólo aplicable al soporte y no a su contenido, dicha solución es aplicable también a los datos o información almacenada en un soporte magnético.

Lo importante aquí es que, al incluir los sistemas y datos informáticos como objeto de delito de daño se busca penalizar todo ataque, borrado, destrucción o alteración intencional de dichos bienes intangibles. Asimismo, la incriminación tiende también a proteger a los usuarios contra los virus informáticos, caballos de troya, gusanos, cáncer routines, bombas lógicas y otras amenazas similares. Asimismo, la ley prevé figuras gravadas, previendo especialmente las consecuencias del daño como, por ejemplo, el producido en un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos.

Se protege la información de valor científico, artístico, cultural o financiero de las Universidades, colegios, museos y de toda administración publica, establecimiento público o de uso público de todo género.

---

[294] Penalidad concordante con la descripción típica introducida por la ley 25326, la que incorpora al código penal el artículo 157 bis.

[295] En esta hipótesis resulta notorio el fundamento de la agravante por la importancia que los sistemas e información comprometida involucran para el correcto funcionamiento de servicios vitales para la Nación, sin los cuales se pondría en jaque la convivencia común, en especial en los núcleos urbanos.

[296] Artículo 183 del Código Penal de Argentina.

El fraude informático se ha pensado como un delito de tipo autónomo y no como una figura especial, en este sentido, se entendió que en el fraude informático, la conducta disvaliosa del autor está signada por la conjunción de dos elementos típicos ausentes en los tipos tradicionales de fraude previstos en Código: el ánimo de lucro y el perjuicio patrimonial fruto de una transferencia patrimonial no consentida sin que medie engaño ni voluntad humana viciada. El ánimo de lucro es el elemento subjetivo del tipo que distingue el fraude informático de las figuras de acceso ilegítimo informático y daño informático en los casos en que la comisión de las conductas descriptas en estos tipos trae aparejado un perjuicio patrimonial.

El medio comisivo del delito de fraude informático consiste en la manipulación o despliegue de cualquier artificio semejante sobre un sistema o dato informático. Se ha optado por definir la conducta que caracteriza este delito como una "manipulación" o "artificio tecnológico semejante" en el entendimiento de que dichos términos comprenden tanto la acción de supresión, modificación, adulteración o ingreso de información falsa en un sistema o dato informático. El hecho se agrava cuando el fraude informático recae en alguna Administración Pública Nacional o Provincial, o entidad financiera.

Común a las disposiciones de acceso ilegítimo, daño y fraude informáticos, se ha entendido que el delito se ve agravado cuando quien realiza las conductas delictivas es aquél que tiene a su cargo la custodia u operación del sistema en razón de las responsabilidades y deberes que le incumben, puesto que usa sus conocimientos, status laboral o situación personal para cometer cualesquiera de los delitos tipificados por la ley anteriormente citada.

En cuanto a la escala penal, se le otorga al juez una amplia discrecionalidad para graduar el aumento de la pena en estos casos, pero le pone un límite, y es que la sanción no podrá superar los veinticinco años de prisión.

Independientemente de lo manifestado, se debe tener presente que sí bien el dato informático o información, tal cual está definido en esta ley especial, se trata sin duda como intangible, y que puede revestir cierto valor económico o de otra índole, no debe, por ello, caerse en el error de asociarlo a lo que en los términos del Derecho de la Propiedad Intelectual se entiende por obra protegida.[297] Si bien una obra protegida por el régimen de la Propiedad Intelectual, puede almacenarse o transmitirle a través de red o de un sistema informático y ser objeto de una conducta de las descripta por esta ley, no toda información es una obra de

[297] Por ejemplo el software.

propiedad intelectual y por ende goza del resguardo legal que otorga de dicho régimen de protección especial.

4.3.6 Ecuador

Desde 1999 en Ecuador se puso a discusión el proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, se conformaron comisiones para la discusión de la Ley y para que formularan observaciones a la misma por parte de los organismos directamente interesados en el tema.

Cuando la ley se presento en un principio, tenía una serie de carencias, que con el tiempo se fueron puliendo, una de ellas era la parte penal ya que, las infracciones a la misma, es decir los llamados Delitos Informáticos, se sancionarían de conformidad a lo dispuesto en el Código Penal, situación un tanto forzada, si tomamos en cuenta los 65 años de dicho Código, en resumen los tipos penales ahí existentes, no tomaban en cuenta los novísimos adelantos de la informática y la telemática por tanto les hacía inútiles por decirlo menos, para dar seguridad ante el posible asedio de la criminalidad informática.

En abril del 2002 y luego de largas discusiones los diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos.

De acuerdo a la Constitución Política de la República, en su Art. 219 inciso primero señala que: "El Ministerio Público prevendrá en el conocimiento de las causas, dirigirá y promoverá la investigación pre-procesal y procesal penal."[298]

Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "el ejercicio de la acción pública corresponde exclusivamente al fiscal".

De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto preprocesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal. Es por tanto el Fiscal quien deberá llevar la voz cantante dentro de la investigación de esta clase de infracciones de tipo informático para lo cual contara como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control Ministerio Público, en tal virtud cualquier resultado de

[298] *Constitución Política de la República de Ecuador*, Título X, Capitulo III

dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante del Ministerio Público a emitir su dictamen correspondiente.

En consecuencia, el Ministerio Público del Ecuador está trabajando en la creación de la Unidad de Delitos Informáticos del Ministerio Público, (UDIMP), esta unidad, tiene como misión fundamental investigar, perseguir y prevenir todo lo relacionado con la llamada criminalidad informática en todos sus aspectos y ámbitos, en especial:

- Amenazas, injurias, calumnias. Por correo electrónico, SMS, tablones de anuncios, foros, newsgroups, Web.
- Pornografía infantil. Protección al menor en el uso de las nuevas tecnologías.
- Fraudes en el uso de las comunicaciones: By Pass.
- Fraudes en Internet. Fraude Informático, Uso fraudulento de tarjetas de crédito, Fraudes en subastas. Comercio electrónico.
- Seguridad Lógica. Virus. Ataques de denegación de servicio. Sustracción de datos. Terrorismo Informático
- Hacking. Descubrimiento y revelación de secreto. Suplantación de personalidad.
- Sustracción de cuentas de correo electrónico.

4.4 El caso de México

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. Los primeros enlaces de Internet en el país, que tuvieron fines exclusivamente académicos, por cierto, 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.

En este periodo el uso internacional del Internet origina una normativa no escrita, seguida por los usuarios de nuestro país, la cual se basaba en usos, sin reglas formales, fundada más bien en consideraciones de tipo ético entre la comunidad académica. En 1994 se incorporan instituciones comerciales en nuestro país, dando lugar a una visión diferente del fenómeno de Internet.

La "era de la información", impone en nuestro país, al igual que en el mundo globalizado, nuevas formas de organización, en los negocios, el mundo de la academia, los gobiernos y, cada vez más, en todas las actividades habituales a pesar de que la cultura de la informática y de la información en México se encuentran aún en sus inicios, hoy en día la tecnología de la información constituye para muchas empresas y universidades nacionales un instrumento insustituible para la realización de trabajos específicos. El uso de la computadora como instrumento o herramienta de trabajo, según datos del INEGI, es incipiente, en 1994 sólo existían 2.2 computadoras personales por cada cien habitantes, lo que ubica a nuestro país en el lugar numero veintiocho a nivel mundial en este aspecto, en el año 2000, según el censo realizado, existían 9.3 computadoras por cada 100 habitantes. En 2006 se llegó a 20.5 computadoras por cada 100 habitantes.[299]

Es previsible que el mundo virtual traiga consigo cambios de importancia en las instituciones jurídicas existentes, así como el desarrollo de instituciones jurídicas nuevas que regulen nuevos intereses y nuevas relaciones.

En México, Internet no se ha regulado de manera expresa, como tampoco en el resto de los países latinoamericanos. Su uso gira en torno a cierto Código Ético y la tendencia Institucional es que será un fenómeno "autorregulable".

A pesar de los índices de crecimiento del uso de la computadora y de Internet, México enfrenta un problema social consistente en lo que se puede denominar “analfabetismo informático", del cual el Poder Legislativo no está exento, por lo que muchos congresistas no entienden el concepto y la estructura de Internet. Asimismo, me atrevo a afirmar que tanto los jueces como los magistrados que forman parte del Poder Judicial tienen hoy día la misma carencia. Es difícil prever el pronunciamiento de los tribunales federales o de la Suprema Corte de Justicia Mexicanos en un caso cuya resolución se base esencialmente en un conflicto por el uso de Internet, por lo cual no se tiene conocimiento de la existencia de tesis ni jurisprudencia algunas que se refieran a los medios electrónicos en general y a Internet en especial.

Como se mencionó es un Código Ético el que puede regular la conducta de los usuarios, mas sin embargo, existe en nuestro país una regulación administrativa sobre las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos, en este sentido, se considera pertinente recurrir a aquellos tratados internaciones de los que el Gobierno de México es parte en virtud de que el artículo 133 Constitucional establece que todos

[299] En http://www.inegi.gob.mx/est/contenidos/espanol/rutinas/ept.asp?t=tinf000&c=6672

los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

a) Código Penal Del Estado De Sinaloa

El único estado de la República que contempla en su legislación los delitos informáticos es el Estado de Sinaloa. Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos informáticos, considero pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Artículo 217.- "Comete delito informático, la persona que dolosamente y sin derecho: "1.- Use o entre a una base de datos, sistemas de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; ó II.- Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistemas o red. Al responsable del delito informático se le impondrá una pena de seis meses a dos años de prisión o de noventa a trescientos días de multa".[300]

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. Considero que se ubicó el delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícito, 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.

Por lo anterior, es necesario que en el Estado, también exista una conciencia sobre la necesidad de legislar en este aspecto, creando el tipo penal adecuado a estas conductas antisociales, lo cual sería, un freno eficaz para su comisión. Tal vez porque aún no se han visto en gran escala los estragos que pueden ocasionar estos tipos de conductas, y porque mucha gente aún no se ha incorporado al mundo de la telecomunicación, nuestros legisladores se han quedado al margen en cuanto a este aspecto.

[300] Título Décimo. "Delitos contra el Patrimonio" Capítulo V. Delito Informático.

Es pertinente recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte, ya que nuestra legislación regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero aún no contempla en sí los delitos informáticos.

b) Tratado de Libre Comercio de América del Norte (TLCAN)

Este instrumento internacional contiene un apartado sobre propiedad intelectual, a saber la 6a. parte capítulo XVII en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución. En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.[301]

c) Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio, incluso el comercio de mercancías falsificadas

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 en el marco regulatorio de la OMC. 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.

Como se observa, el tratamiento que los dos instrumentos internacionales comentados 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.

[301] Tratado de Libre Comercio (TLC). 6a. parte capítulo XVII.

d) Ley Federal del derecho de Autor y Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República 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.

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, etc.

En este sentido, es importante detenernos en los artículos 102 y 231 de la presente Ley. 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.

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 del que se infiere la sanción al uso de programas de virus.

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.

El artículo 231, fracción II y VII contemplan dentro de las infracciones de comercio el "producir, fabricar, almacenar, distribuir, transportar o comercializar copias Ilícitas de obras protegidas por esta Ley" y "Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular". La redacción de estas fracciones 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.

Cabe destacar que 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.

El manejo y el uso de la información en la red de redes, tiene muchas aristas por explorar. Existen vacíos en los sistemas de seguridad informática, así como en la aplicación y formulación de leyes; dicha situación convierte a Internet en un espacio propicio para la ejecución de delitos cibernéticos.

Por otra parte, según una iniciativa de ley propuesta el 22 de marzo de 2000 ante el pleno de la Cámara de Senadores, están considerados como delitos informáticos "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen referencia al uso indebido de cualquier medio informático."[302]

El robo o alteración de información, sabotaje, pedofilia, tráfico de menores, fraude, clonación de señales satelitales, de tarjetas de crédito y el ciberterrorismo son actividades consideradas por las autoridades de los tres niveles (federal, estatal y municipal) como una muestra de estos ilícitos, los cuales día con día muestran un incremento en nuestro país, expandiéndose de manera considerablemente rápida.

La Secretaría de Seguridad Pública (SSP), a través de su División de Policía Cibernética, ha detectado a 397 comunidades o sitios Web con pornografía infantil, de las cuales 197 son mexicanas.

Asimismo, esta corporación tiene conocimiento de la existencia de cuatro millones de sitios Web que explotan la pornografía, 60% de ellos son lucrativos, es decir, el sitio exige el pago del "servicio" por medio de la tarjeta de crédito del usuario; el 40% restante son intercambios de fotos y videos persona a persona.

En relación con el fraude, otro ilícito con alto índice de incidencia, la PFP ha documentado una serie de patrones que son resultado de sus extensos patrullajes en la red.[303]

---

[302] En http: //www.senado.gob.mx, consultado el 18 de marzo de 2007, 09:32 hrs.

[303] "Sabemos que los delincuentes actúan entre las 12 del día y las tres de la tarde para subir las 'ofertas'; utilizan cuentas bancarias donde realizan sus depósitos las víctimas, la mayoría de ellas se encuentran en un rango entre los 18 y 30 años, además de que los usuarios afectados son primordialmente hombres. En el mapa geográfico, el mayor número de delitos se localizan en los estados de Jalisco, Estado de México, Morelos, Yucatán, Sonora y Sinaloa."

Uno de los problemas más importantes para la persecución de estos delitos tiene que ver con la rapidez que ofrece la publicación electrónica para poner y quitar información de cualquier tipo y formato en Web.

Para contrarrestar éstos y otros delitos cibernéticos de creciente expansión, el gobierno mexicano conformó un equipo especializado llamado DC México (Delitos Cibernéticos México).

Este grupo lo integran todas las corporaciones policíacas estatales y federales, así como los proveedores de servicio de Internet, (ISPs) y todas las compañías privadas o públicas que ofrecen seguridad informática en el país.

DC México tiene como tareas fundamentales la identificación, el monitoreo y el rastreo de cualquier manifestación delictiva que se cometa mediante computadoras conectadas en territorio mexicano o fuera de él y que tenga afectaciones en nuestro país.[304]

A su vez, DC México tiene varias divisiones que ejecutan distintas funciones, entre ellas se encuentran el subgrupo de contingencias informáticas, el subgrupo de capacitación y el subgrupo de gobierno.[305] DC México trabaja conjuntamente con el servicio de aduanas de los Estados Unidos, además de que establece vínculos cercanos con el Servicio Secreto y la Brigada Tecnológica de España.

Hay que resaltar que Internet no es un vínculo que desarrolle o propicie la ejecución de actividades delictivas. En este sentido, las policías cibernéticas son una herramienta innovadora de las corporaciones de procuración de justicia para la seguridad de todos los usuarios que navegan en Internet, sea cual fuere su región geográfica en el mundo.

México se encuentra rezagado legalmente frente a los demás países del mundo pese al trabajo ya realizado en las reformas de mayo del año 2000, por lo que el Poder Legislativo aún tiene la tarea pendiente de regular en materia informática y de telecomunicaciones.

Hoy en día, la influencia de la tecnología en la comunidad se refleja en todos sus sectores. Asimismo, la trascendencia de los medios masivos de comunicación, apoyándose en los avances tecnológicos, ha tomado uno de los roles principales en la sociedad. La importancia de la información ha llegado al punto en que su recolección, proceso, y distribución, son en definitiva, de las actividades prioritarias en todos los ámbitos de la sociedad.

[304] La Universidad Nacional Autónoma de México participa en este grupo con UNAM-CERT, que es un organismo importante por las contribuciones que ha realizado en materia de prevención del delito.

[305] Dentro de esta corporación se encuentra la división Nuevas tecnologías e investigación académica y desarrollo, que preside la UNAM, y en la cual este grupo tiene la tarea de ver todo lo relacionado con capacitación y desarrollo de innovaciones tecnológicas.

En el área de los negocios específicamente, la información ocupa uno de los puestos más importantes, y es considerada como un elemento altamente valioso e indispensable para el buen funcionamiento de las empresas y los comercios y, consiguientemente, de los mercados.

De aquí que una de las prioridades de los países industrializados, así como los principales foros internacionales, es regular adecuadamente el uso de Internet y el Comercio Electrónico más seguro. La idea es enmarcar legalmente a la informática, de forma que cuente con una columna vertebral jurídica para lograr un mayor grado de desarrollo.

En México no existe una ley específica que regule el comercio electrónico, pero sí un conjunto de observaciones en diversas leyes y códigos que integran más bien una Miscelánea que no han sido suficientes para el pleno desarrollo del Comercio Electrónico.[306]

El consentimiento es uno de los elementos reformados que se refiere más bien a la manifestación de la voluntad a través de los medios electrónicos, ópticos o por cualquier otra tecnología entre personas no presentes, aquí los legisladores de manera muy acertada abren la posibilidad a la aparición de nuevas tecnologías y no solamente al Internet y al Correo Electrónico.

En la fase probatoria el Código de Procedimientos Civiles se reformó para aceptar al mensaje de datos como medio probatorio en los procedimientos procesales y también se habla de la forma de valorar la prueba conforme a la fiabilidad método, por una parte los legisladores se adelantan a los tiempos que estamos viviendo pero al tratar la forma de valorar las pruebas electrónicas de una forma difusa redactan esta reforma.

La fiabilidad del método en este caso es difícil de interpretar que la concepción de este término es de forma genérica, lo que se ha mostrado en el personal judicial al verificar las pruebas electrónicas estos la rechazan por no estar capacitados para poder valorarlas sin embargo no es culpa del Poder Judicial sino de una mala redacción al no ser más clara la ley respecto de la forma de valorar las pruebas.

En el Código de Comercio se abre las puertas al comercio electrónico por Internet ante posibilidad de ofertar bienes y servicios a través de medios electrónicos, con la salvedad de conservar los archivos electrónicos que por ley deban conservar los comerciantes, a los legisladores les falto tratar el soporte electrónico en los que conservará esta información.

[306] El 29 de mayo de 2000, fue publicado en el Diario Oficial de la Federación un decreto para reformar y adicionar el Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, el Código Federal de Procedimientos Civiles, el Código de Comercio y la Ley Federal de Protección al Consumidor, dando paso a la primera etapa de un intento de regular el comercio electrónico en México.

Pese a estos avances, en la legislación vigente no se incluyó expresamente lo referente a firma electrónica y comprobante fiscal electrónico, aspectos que si bien están contemplados para el futuro, de momento limitan, de alguna manera, el desarrollo de las transacciones en línea[307].

Dentro de la Nueva Hacienda Pública Distributiva se ha considerado lo referente al comprobante fiscal electrónico, aspecto en que las autoridades federales vienen trabajando desde hace dos años como parte de los trabajos integrales para impulsar el programa e-México.

El 16 de noviembre de 2001, fue publicado en el Diario Oficial de la Federación, el proyecto de Norma Oficial Mexicana PROY-NOM-151-SCFI-2001. Así pues la Norma Oficial Mexicana por sus características es muy técnica, pero para la conservación de mensajes de datos es de vital importancia.

Esta NOM viene a clarificar las reformas más precisamente las que hacen referencia a la conservación de los mensajes de datos.

Se establece la obligación de los comerciantes de conservar por un plazo de 10 años los originales de aquellos documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta.[308]

Por otro lado, aunque la firma electrónica en México no tiene un apartado especial en donde sea regulada, se puede mencionar que hay varias leyes donde ya se habla de ellas, por ejemplo el Código Fiscal de la Federación, Ley aduanera, etc.

De la misma manera, la Ley Federal de Protección de Datos Personales se presentó al Congreso de la Unión, la cual, tiene por objeto, regular el derecho del consumidor a solicitar información sobre bases de datos que contenga información sobre su persona.[309]

El sistema financiero mexicano se apoya en una infraestructura de Números de Identificación Personal (NIP), siendo estos superados por la tecnología de la criptografía de clave

[307] La omisión de la figura de firma electrónica no fue por irresponsabilidad o falta de visión, sino porque se estaba a la espera de la Ley Modelo sobre firmas electrónicas por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL).

[308] Una de las nuevas implementaciones de esta NOM son la mecánica de atribución de un mensaje de datos a una persona a través de la firma electrónica y cumplir con los elementos de autenticidad, confidencialidad e integridad.

[309] Esto obligaría a las empresas y a las instituciones de crédito a destinar recursos para crear la infraestructura necesaria para cumplir con esta ley y de alguna forma sería necesario unificar las informaciones de las diferentes bases de datos. Esta ley incluiría a los Buró de crédito y a las empresas dedicadas en México a la venta de bases de datos.

pública y privada, así pues la normatividad del sistema financiero mexicano deberá ser revisada para incorporar la autentificación biométrica.

Es así como a través de la reforma a la ley de Adquisiciones nace el proyecto de e-México, el cual incorpora a dos sistemas, Comprante (el cual se encuentra en funcionamiento actualmente) y TramitaNet, para poder realizar cualquier operación ya sea en CompraNet para licitar a través de Internet o de realizar algún tramite a través de TramitaNet o para hacer declaraciones fiscales a través del SAT, cada una otorga una firma electrónica y expide un certificado de firma electrónica por cada sistema, lo que ocasiona dos problemas principales:

- Al ciudadano se le proporcionará multiplicidad de certificados para diversos propósitos, ya sean públicos o privados, a nivel federal o local.
- Se deberá trabajar en la unificación de la firma electrónica del ciudadano para que funja como la firma manuscrita que es única, es en su defecto de una sola firma electrónica para propósitos con la Federación o los Estados.

Así pues México nuevamente se prepara para actualizar su legislación e impulsar el Comercio Electrónico y esperamos que nuestros legisladores alcancen a percibir que México necesita una legislación más robusta y que esté a la vanguardia mundial en materia informática, cabe advertir que en estos momentos nos encontramos ubicados entre los pocos países sino es que somos el único que aún no cuenta con una legislación sobre firmas electrónicas por ejemplo.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras.

El proceso de globalización en el que estamos inmersos ha llevado a las Naciones Unidas a la aprobación de una Ley Modelo y de una guía para su incorporación a los ordenamientos jurídicos internos. Y es que el carácter gremial que inicialmente tuvo el derecho mercantil ha sido sustituido por un comercio electrónico de ámbito mundial.

El incremento de forma ingente de transacciones comerciales internacionales por medio de intercambios electrónicos ha sido uno de los motivos que han llevado a la UNCITRAL a la elaboración de esta espléndida ley. En el camino hacia la unificación comercial la Asamblea de Naciones Unidas ha recomendado a los Estados la adopción de las medidas contempladas en esta Ley con la finalidad no solo de asegurar la seguridad jurídica en el comercio internacional sino también con la intención de unificar sistemas jurídicos con elementos jurídicos, económicos y sociales diferentes.

Esta Ley Modelo y la guía que incorpora para su aplicación al derecho interno de los Estados constituyen la mayor prueba de los cambios producidos en la forma de contratación. En este nuevo ámbito global en el que nos movemos está claro que las normas sobre contrataciones han de ser marcadamente globalistas.

La Unión Europea ha sido otro de los entes supranacionales que ha regulado esta nueva forma de contratación. Así, el 8 de junio del 2000 dictó la Directiva 2000/31 sobre aspectos jurídicos de la Sociedad de la Información, Comercio Electrónico y Mercado Interior. Su objetivo fundamental es crear un marco jurídico que garantice la libre circulación de los servicios de la información entre los Estados Miembros.

Lo cierto es que esta transnacionalización del derecho no puede reducirse a la Unión Europea.

Los mismos sofisticados medios de que disponen los delincuentes para cometer sus delitos sirven también a los técnicos para establecer medidas de seguridad y obtener pruebas que los identifiquen e inculpen. Por ello debemos confiar en que serán cada vez menor el número de sujetos que se atrevan a vulnerar sistemas informáticos.

Las medidas legislativas que tienen por objetivo armonizar las disposiciones nacionales en materia de delincuencia informática deberían ser completadas mediante medidas no legislativas, en particular:

- la creación de unidades nacionales especializadas (autoridades policiales y autoridades judiciales);
- la formación permanente y especializada de policías y personal de la administración de justicia;
- la armonización de las normas de contabilización en materia policial y judicial así como la creación de instrumentos adaptados para el análisis estadístico de la criminalidad informática;

- cooperación entre los distintos actores mediante la creación de un foro mundial;
- fomentar acciones realizadas directamente por las empresas con el fin de luchar contra la delincuencia informática;
- proyectos en el ámbito de la investigación y el desarrollo tecnológico (IDT) financiados por la mayoría de los Estados.

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

Por otra parte, en el ámbito de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal (hasta ese entonces) era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados. Por todo ello, en vista de que, los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras, a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia.

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

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

Teniendo presente esa situación, considero que, es indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema. En consecuencia, es necesario que, para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada.

Durante la elaboración de dicho régimen, se deberán considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

Al respecto se debe considerar lo que dice el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos el cual señala que, cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.

Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable, tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

En definitiva tanto los terroristas como las Organizaciones Delictivas Transnacionales se están aprovechando de los avances tecnológicos, para cometer sus fechorías a través del uso de las redes de telecomunicaciones en donde han encontrado un sitio propicio para expandir sus tentáculos situación que debe ser detenida por parte de los organismos a cargo del control de esta clase de conductas disvaliosas, pero la acción no debe ser aislada debe existir una cooperación interinstitucional e internacional en este campo.

Ahora bien el problema que se advierte por parte de las instituciones llamadas a perseguir las llamadas infracciones informáticas es la falta de preparación en el orden técnico tanto del Ministerio Público como de la Policía Judicial, esto en razón de la falta por un lado de la infraestructura necesaria, como centros de vigilancia computarizada, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de los llamados Delitos Informáticos, de igual manera falta la suficiente formación tanto de los Fiscales que dirigirán la investigación como del cuerpo policial que lo auxiliara en dicha tarea, dado que no existe hasta ahora en nuestra policía una Unidad Especializada, como existe en otros países como en Estados Unidos donde el FBI cuenta con el Computer Crime Unit, o en España la Guardia Civil cuenta con un departamento especializado en esta clase de infracciones. Por otro lado también por parte de la Función Judicial falta la suficiente preparación por parte de Jueces y Magistrados tratándose de estos temas, ya que en algunas ocasiones (por no decirlo en la mayoría de los casos), los llamados a impartir justicia se ven confundidos con la especial particularidad de estos delitos y los confunden con delitos tradicionales que por su estructura típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin.

Por tanto es esencial que se formen unidades Investigativas tanto policiales como del Ministerio Público especializadas en abordar cuestiones de la delincuencia informática trasnacional y también a nivel nacional. Estas unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley.

CONCLUSIONES

La velocidad con que se suceden los avances tecnológicos (sobre todo luego de la aparición de la informática en los años sesenta), ha provocado en el ser humano una avidez por la información. Junto con ese intentar por conocer cada vez más y asociado también a la informática han aparecido una serie de conductas que atentan precisamente contra la intimidad del hombre y por ende a la seguridad y el orden público.

La acelerada dinámica de desarrollo del conocimiento está reconfigurando las estructuras productivas y las formas de relación social, los procesos actuales de cambio a nivel internacional y un evidente crecimiento en la calidad de la información (que supera la mera disposición cuantitativa de la misma), apuntan a la conformación de una sociedad del conocimiento que poco a poco supera la etapa de la sociedad de la información.

Internet está constituido por una comunidad heterogénea e invisible que no está unida bajo los tradicionales cánones de territorio, política, religión, población, lengua, etc. Por ello ha sido extremadamente complejo establecer la forma idónea de regular ciertas conductas que son una realidad dentro de las relaciones comerciales y humanas facilitadas por este medio de comunicación, y que algunas veces podrían hasta constituir una vulneración real a los derechos humanos. Tal es el caso de la pornografía infantil, la violación de la intimidad en el tratamiento de datos personales, el fomento del terrorismo y la violación de las comunicaciones personales, entre otras irregularidades.

La concepción de delitos informáticos abarca en realidad un conjunto de elementos de distintas características, que afectan bienes jurídicos diversos y que solo son agrupadas bajo este concepto por su relación con las computadoras o los sistemas informáticos. Esta amplitud del concepto, determina que a los fines del análisis jurídico científico, sea un concepto vacío, sin contenido propio, que solo puede adquirir fuerza con la descripción concreta de las conductas que abarca.

La falta de información sobre este fenómeno, ha hecho que los intentos por dar al ciberespacio un marco normativo, se vean meramente reflejados en los diversos escenarios nacionales, lo que ha dado lugar a leyes internas en los mejores casos, mientras que por otro lado, los esquemas de seguridad son imperceptibles o prácticamente nulos.

Ahora los incidentes relacionados con la informática están creciendo en número, sofisticación, gravedad y costo. Nos estamos enfocando en las armas de destrucción

masiva, pero tenemos que tener muy en cuenta las armas de interrupción masiva de servicios que existen en el ciberespacio. El problema lo pueden provocar tanto grandes organizaciones, como pequeños adolescentes, los cuales pueden desde crear un virus, hasta formular lo que hoy se conoce como terrorismo informático, el cuál no tiene fronteras.

La realización de tareas de inteligencia, necesarias para llevar a cabo atentados tanto en el mundo físico o en el mundo virtual es mucho más simple debido a la masa de información disponible electrónicamente sobre casi todos los aspectos de la civilización contemporánea. La fabricación de elementos ofensivos para llevar a cabo atentados explosivos o biológicos es facilitada por la aparición de manuales electrónicos sobre tecnología de bombas o armas químicas y bacteriológicas.

Muchos ataques realizados por medios informáticos no pueden producir el terror necesario para que sean considerados terrorismo internacional, no es menos cierto que ello no invalida la teoría de que ciertos delitos puedan crear situaciones de terror a una población local o incluso nacional.

El uso de las armas de la llamada InfoGuerra (proveniente del mal uso de los medios informáticos hacia la sociedad mundial), pueden brindar una capacidad mucho más sutil y efectiva de causar terror y paralizar a una sociedad. El descubrimiento y análisis de los nodos de convergencia entre el mundo real y el mundo virtual es el primer paso para determinar que tipos de actos terroristas pueden ser realizados.

La tarea de prevención necesaria es mucha y las necesidades de legislaciones y equipos de trabajo acordes al reto por venir es inmediatamente necesaria, lo que se requiere es sólo la voluntad política de los encargados de dirigir los destinos de las naciones a fin de evitar que algo que nació con fines científicos como lo fue Internet termine convirtiéndose en una nueva y poderosa arma de terrorismo internacional por la simple inacción o falta de visión de los políticos.

Existe, actualmente, un consenso internacional que condena este tipo de actos, cuya "sintomatología" se tiende a reproducir entre un hecho y otro, lo que puede poner a la comunidad en el camino de lograr realmente una definición y regulación jurídica específicas que estén en el terreno de la prevención.

El contexto actual de los actos de violencia identificados como terroristas, es decir, los actos que han encontrado su génesis en una posición religiosa y/o ideológica, por lo menos para delimitar sus objetivos políticos, lleva a pensar en el riesgo de que cualquier

ocurrencia pueda esgrimirse como idea para intentar demostrar la bondad de los fines. Esto representa un problema fundamental para el derecho por la multiplicidad de razones que pueden darse. En suma, es una actividad ilegal que utiliza o amenaza con el uso premeditado de la violencia para infundir miedo crónico en la víctima y la sociedad, en busca de metas estratégicas determinadas por el autor material. Sin duda, su combate y erradicación efectiva significará un precio a pagar por parte de la sociedad civil, posiblemente en el terreno de la jurisdicción universal versus soberanía, lo que significará la internacionalización del delito, su prevención y castigo.

Mediante el desarrollo de esta investigación se plantearon reflexiones y se trató de conducir a un debate sobre Internet que giró en torno a la dificultad de establecer límites en los contenidos de éste sin vulnerar la libertad de expresión y comprobar si realmente es necesaria o no esta regulación, lo cierto es que, sólo algunos países toman conciencia del peligro que nos acecha y la necesidad de regular estas conductas ilícitas ha llevado especialmente a las grandes potencias, a contemplar en sus legislaciones al respecto. Así, podemos encontrar países como Alemania, donde se enfoca principalmente a la protección de datos personales contemplados en un soporte magnético, o Estados Unidos (siendo el más avanzado en cuanto a la regulación de los delitos Informáticos), el cual menciona el problema real de los virus informáticos así como también y de manera especial le da un enfoque a dichos delitos en su Ley de Privacidad.

Todo lo anterior es de gran ayuda a países como el nuestro que empiezan a legislar al respecto, así pues, los delitos informáticos constituyen una gran laguna en nuestras leyes penales, y el Derecho Comparado nos permite hacer una lista de los delitos que no están contemplados en nuestro Códigos Penales y que requieren análisis urgente por parte de nuestros académicos, penalistas y legisladores, debido a que, en nuestro país no se cuenta con una legislación que hable sobre los delitos Informáticos, por lo cual las conductas ilícitas que se realizan quedan impunes, y nuestro Estado no queda exento de ello.

A pesar de eso, México cuenta con una regulación administrativa, pero que no contempla de forma expresa los delitos informáticos.

La aplicación del derecho a Internet se fundamenta en el debate entre la defensa de la autonomía, privacidad y anonimato del usuario individual y por otra parte la preocupación por el derecho a la libre actuación en Internet y a la defensa de la seguridad colectiva aún si ésta implica un menoscabo de la seguridad individual.

Las reglas de obligación en el ciberespacio no han aún sido definidas, especialmente no los límites de la asamblea de inteligencia aceptable entre naciones amigas. Entonces, distinta de la claridad de intereses e interdependencia mutua en el mundo físico, el cual ha fomentado la cooperación, el conflicto informático ha tenido el efecto opuesto, esto muestra que en el ciberespacio nadie puede ser amigo, todos son potenciales enemigos.

Las autoridades encargadas de hacer cumplir la ley suelen adaptarse con lentitud a las nuevas tendencias, mientras que los grupos delictivos organizados tienden a adaptarse rápidamente y a aprovechar los adelantos tecnológicos debido a los inmensos beneficios que producen sus actividades ilícitas.

La apertura de nuevos mercados y las nuevas tecnologías de las comunicaciones, junto con la diversidad de actividades en las que participan, también han alimentado el crecimiento de la delincuencia organizada en los países en desarrollo. Los países con economías en transición o en situaciones de conflicto son particularmente vulnerables al crecimiento de ese tipo de delincuencia. En tales casos, la delincuencia organizada plantea una amenaza real para el desarrollo de instituciones reformadas, como la policía, los servicios de aduana y el poder judicial, que pueden adoptar prácticas delictivas y corruptas, planteando un grave obstáculo al logro de sociedades estables y más prósperas.

Aún y cuando son innegables todos estos tipos de conductas que se están realizando con mayor frecuencia, también existen partidarios para la no regulación del uso del Internet.

PERSPECTIVAS

Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área, su clasificación es difícil, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las leyes relacionadas con la informática.

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitirán tener un marco de referencia aceptable para el manejo de dichas situaciones.

Nuevas formas de hacer negocios como el comercio electrónico, puede que no encuentren el eco esperado en los individuos y en las empresas hacia los que van dirigidos, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

Al establecer los reglamentos necesarios se facilitará la implantación de esquemas de seguridad informática, considerando su utilidad para la protección de vidas humanas, información privilegiada, recursos financieros y materiales, mediante la definición precisa de los conceptos y terminología propios del tema en cuestión.

De ahí la necesidad de generar la creación de entidades con amplia participación, en un nuevo modelo democrático aplicado al mundo virtual, que permita tanto la presencia de intereses particulares y gremiales como de intereses políticos constantes en la representación de diversas jurisdicciones.

Las estrategias que se empleen para combatir los delitos, la piratería y el terrorismo informáticos deben ser concebidas con la participación de toda la estructura del Estado-Nación y del mismo modo considerar en la maniobra diseñada la participación de los diferentes actores del sistema internacional. El combate contra estos delitos, debe estar sustentado en Inteligencia, una inteligencia que permita proyectar acciones con visión de futuro, y permitir atacar el fenómeno desde sus raíces, produciendo un conocimiento útil y buscando los consensos para conformar sistemas de inteligencia adecuados en su estructura y en sus fines, por lo que debe ser preocupación no sólo de militares sino también de civiles, profesionales de diferentes áreas, gobernantes y políticos, ya que, en los tiempos actuales este tipo de amenazas tiene todo un soporte económico, social e internacional donde la fuerza militar, es incapaz por muy potente que

sean sus medios, vencerla y menos erradicarla desde sus bases, así pues se debe convocar a la conformación de un régimen jurídico flexible, que se ajuste a la dinámica propia del mundo digital y que coadyuve a su desarrollo y no a su estancamiento; en defensa de los derechos individuales y colectivos.

Se debe de legislar de una manera seria y honesta, recurriendo a las diferentes personalidades que tiene el conocimiento, tanto técnico en materia de computación, como en lo legal (el Derecho), 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.

Muchos de estos delitos deben ser contemplados en legislaciones internas e internacionales, lo cual es también un reto importante. Si la intención es asumir reglas de convivencia y determinar responsabilidades que protejan a los usuarios y a la vez a los agentes privados que facilitan la comunicación global, así como indicar las conductas lesivas a los derechos humanos y condenarlas dentro de un marco de derecho internacional público; debemos entonces establecer las reglas a seguir con la anuencia y participación de todos.

Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática. Una vez tipificados, se debe proceder a realizar actividades para fomentar la cooperación internacional en los campos relativos al Internet, y así, se proyectará como es que más allá de regular situaciones específicas que solo aplican a determinadas circunstancias de espacio, tiempo y sujetos concretos, debe valorarse en un debate internacional cuál es la intención social, política y económica de aplicar un régimen jurídico al mundo virtual, teniendo como base la regulación del ciberespacio y sobre todo de la piratería informática y el terrorismo informático.

La ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información; sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

Es necesario legislar en materia del ciberespacio, siempre y cuando, el legislador tenga presente los preceptos, donde exista una libertad de expresión y el derecho a la información; teniendo en cuenta que la libertad de expresión ya no lo es, si ataca la vida privada, a la moral, y a la paz pública.

Si la pretensión es tener Internet como un mecanismo de comunicación global y de integración supranacional, se deben descartar aquellas propuestas que partan de la supremacía de ciertas instancias autónomas de índole público o privado que únicamente han demostrado poner en jaque principios como el de jurisdicción, soberanía o el de *non bis in ídem.*

Al mismo tiempo, la determinación de las teorías referentes a la regulación del ciberespacio en los niveles administrativos, arbitrales, de mediación o conciliatorios, es una necesidad básica que asegurará además la resolución de conflictos en una alternativa supranacional que también debe estar orientada a definir la jurisdicción competente en caso de infracciones de las normas de convivencia, ya que, el establecimiento de entidades de gobierno a nivel mundial, en donde se obvie la participación de Estados particulares, debe tener en consideración los intereses de todas las partes involucradas, incluyendo los de los países en vías de desarrollo que aún deben superar la brecha digital.

El desarrollo de un marco normativo y legal que comprenda todo el conjunto de delitos vía Internet, especificando qué se entiende por delito, sus posibles castigos y las diversas estrategias políticas, sociales y económicas que deben ser desarrolladas para aplicar un régimen jurídico al mundo virtual donde se consideren los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional, prevendrá las situaciones tan conflictivas que se han estado originando desde la aparición del espacio virtual, por lo que, las estrategias que se empleen deben ser concebidas con la participación de toda la estructura del Estado-Nación y sustentadas en Inteligencia, lo cual permitirá proyectar la acción contra los delitos informáticos y el terrorismo con visión de futuro, uniendo las acciones intermedias y permitir atacar el fenómeno desde sus raíces.

Al convocar a la conformación de un régimen jurídico flexible para la regulación del ciberespacio y por ende del terrorismo informático, con la participación de los gobiernos, de los representantes de todos los organismos competentes, de las Naciones Unidas, de otras organizaciones internacionales gubernamentales y no gubernamentales, el sector privado, la sociedad civil y los medios de comunicación, se hallarán soluciones y alcanzarán acuerdos en los campos de gobernanza de Internet y en los mecanismos de financiación para llenar la brecha digital existente entre los países desarrollados y subdesarrollados que se ajuste a la dinámica propia del mundo digital y que contribuya al desarrollo y no al estancamiento del Derecho Internacional.

ANEXO

GLOSARIO DE TÉRMINOS

- **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 practica 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 mas 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 tenemos 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.
- **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.
- **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 es 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. Algo que hace especialmente peligrosos a los sniffers es que no se pueden detectar, ya que son aplicaciones pasivas y no generan nada, con lo que no dejan ningún tipo de huella, y son especialmente indetectables en DOS y Windows 95 y trabajo en grupo, aunque en UNIX y Windows NT hayan más posibilidades de detectarlo.

ESTADÍSTICAS SOBRE DELITOS INFORMÁTICOS.

Desde hace cinco años, en los Estados Unidos existe una institución que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos a través de las computadoras. Esta entidad es El Instituto de Seguridad de Computadoras (CSI), quien anunció recientemente los resultados de su quinto estudio anual denominado "Estudio de Seguridad y Delitos Informáticos" realizado a un total de 273 Instituciones principalmente grandes Corporaciones y Agencias del Gobierno. Este Estudio de Seguridad y Delitos Informáticos es dirigido por CSI con la participación Agencia Federal de Investigación (FBI) de San Francisco, División de delitos informáticos. El objetivo de este esfuerzo es levantar el nivel de conocimiento de seguridad, así como ayudar a determinar el alcance de los Delitos Informáticos en los Estados Unidos de Norteamérica. Entre lo más destacable del Estudio de Seguridad y Delitos Informáticos 2000 se puede incluir lo siguiente:

Violaciones a la seguridad informática.

Respuestas	PORCENTAJE (%)
No reportaron Violaciones de Seguridad	10%
Reportaron Violaciones de Seguridad	90%

De los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.

- 70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados -- por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

Pérdidas Financieras.

74% reconocieron pérdidas financieras debido a las violaciones de las computadoras.

- Las pérdidas financieras ascendieron a $265, 589,940 (el promedio total anual durante los últimos tres años era $120, 240,180).

61 encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27, 148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10, 848,850.

Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66, 708,000) y el fraude financiero (53 encuestados informaron $55, 996,000).

Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

71% de los encuestados descubrieron acceso desautorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuestados (59%) mencionó su conexión de Internet como un punto frecuente de ataque, los que citaron sus sistemas interiores como un punto frecuente de ataque fue un 38%. Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, los hallazgos del "Estudio de Seguridad y Delitos Informáticos 2000" confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo.

Los encuestados detectaron una amplia gama a de ataques y abusos. Aquí están algunos otros ejemplos:

- 25% de encuestados descubrieron penetración al sistema del exterior.
- 79% descubrieron el abuso del empleado por acceso de Internet (por ejemplo, transmitiendo pornografía o pirateó de software, o uso inapropiado de sistemas de correo electrónico).
- 85% descubrieron virus de computadoras.
- Comercio electrónico.

Por segundo año, se realizaron una serie de preguntas acerca del comercio electrónico por Internet. Aquí están algunos de los resultados:

- 93% de encuestados tienen sitios de WWW.
- 43% maneja el comercio electrónico en sus sitios (en 1999, sólo era un 30%).
- 19% experimentaron accesos no autorizados o inapropiados en los últimos doce meses.
- 32% dijeron que ellos no sabían si hubo o no, acceso no autorizado o inapropiado.
- 35% reconocieron haber tenido ataques, reportando de dos a cinco incidentes.
- 19% reportaron diez o más incidentes.
- 64% reconocieron ataques reportados por vandalismo de la Web.
- 8% reportaron robo de información a través de transacciones.
- 3% reportaron fraude financiero.

Conclusión sobre el estudio csi:

Las tendencias que el estudio de CSI/FBI ha resaltado por años son alarmantes. Los "Cyber crímenes" y otros delitos de seguridad de información se han extendido y diversificado. El 90% de los encuestados reportaron ataques. Además, tales incidentes pueden producir serios daños. Las 273 organizaciones que pudieron cuantificar sus pérdidas, informaron un total de $265, 589,940. Claramente, la mayoría fueron en condiciones que se apegan a prácticas legítimas, con un despliegue de tecnologías sofisticadas, y lo más importante, por personal adecuado y entrenando, practicantes de seguridad de información en el sector privado y en el gobierno.

Otras estadísticas:

- La "línea caliente" de la Internet Watch Foundation (IWF), abierta en diciembre de 1996, ha recibido, principalmente a través del correo electrónico, 781 informes sobre unos 4.300 materiales de Internet considerados ilegales por usuarios de la Red. La mayor parte de los informes enviados a la "línea caliente" (un 85%) se refirieron a pornografía infantil. Otros aludían a fraudes financieros, racismo, mensajes maliciosos y pornografía de adultos.
- Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.
- Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbara Jenson "Acecho cibernético: delito, represión y responsabilidad personal en el mundo online", publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año.
- En Singapur El número de delitos cibernéticos detectados en el primer semestre del 2000, en el que se han recibido 127 denuncias, alcanza ya un 68 por ciento del total del año pasado, la policía de Singapur prevé un aumento este año en los delitos por Internet de un 38% con respecto a 1999.
- En relación con Internet y la informática, la policía de Singapur estableció en diciembre de 1999 una oficina para investigar las violaciones de los derechos de propiedad y ya ha confiscado copias piratas por valor de 9,4 millones de dólares.
- En El Salvador, existe más de un 75% de computadoras que no cuentan con licencias que amparen los programas (software) que utilizan. Esta proporción tan alta ha ocasionado que organismos Internacionales reacciones ante este tipo de delitos tal es el caso de BSA (Bussiness Software Alliance).

TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR NACIONES UNIDAS	
DELITO	**CARACTERÍSTICAS**
La manipulación de programas de entrada	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma

	encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
Manipulación de los datos de salida	Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
Fraude efectuado por manipulación informática	Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.
Falsificaciones informáticas.	
Como objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada.
Como instrumentos	Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.
Daños o modificaciones de programas o datos computarizados.	
Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
Virus	Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
Gusanos	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.
Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde ésta se encuentra.
Acceso no autorizado a servicios y sistemas informáticos	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
Piratas informáticos o hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
Reproducción no autorizada de programas informáticos de protección legal	Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la

	reproducción no autorizada de programas informáticos no es un *delito informático* debido a que el bien jurídico a tutelar es la propiedad intelectual.

En http://www.un.org

Ley Especial contra Delitos Informáticos de la República Bolivariana de Venezuela

Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2001 LA ASAMBLEA NACIONAL DE LA REPUBLICA BOLIVARIANA DE VENEZUELA DECRETA la siguiente, LEY ESPECIAL CONTRA DELITOS INFORMATICOS Título I Disposiciones Generales Artículo 1. Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley. Artículo 2. Definiciones. A los efectos de la presente ley y cumpliendo con lo previsto en el artículo 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por: a. Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data. b. Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas. c. Data: hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado. d. Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas. e. Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos. f. Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas. g. Hardware: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes. h. Firmware: programa o segmento de programa incorporado de manera permanente en algún componente de hardware. i. Software: información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas. j. Programa: plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador. k. Procesamiento de data o de información: realización sistemática de operaciones sobre data sobre información, tales como manejo, fusión, organización o cómputo. l. Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación. m. Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema. n. Tarjeta inteligente: rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla. o. Contraseña (password): secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema. p. Mensaje de datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones. Artículo 3. Extraterritorialidad. Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros. Artículo 4. Sanciones. Las sanciones por los delitos previstos en esta ley serán principales y accesorias. Las sanciones principales concurrirán con las accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley Artículo 5. Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable. La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente **Título II De los delitos** Capítulo I De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información Artículo 6. Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidadestributarias Artículo 7. Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo. Artículo 8. Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios. Artículo 9. Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas. Artículo 10. Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Artículo 11. Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en

un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado. Artículo 12. Falsificación de documentos. El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad. El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro. Capítulo II De los Delitos Contra la Propiedad Artículo 13. Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Artículo 14. Fraude. El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias. Artículo 15. Obtención indebida de bienes o servicios. El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Artículo 16. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. El que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penado con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias. En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema. Artículo 17. Apropiación de tarjetas inteligentes o instrumentos análogos. El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias. La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo. Artículo 18. Provisión indebida de bienes o servicios. El que a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado, se haya indebidamente obtenido, retenido, falsificado, alterado, provea a quien los presente de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Artículo 19. Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Capítulo III De los delitos contra la privacidad de las personas y de las comunicaciones. Artículo 20. Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero. Artículo 21. Violación de la privacidad de las comunicaciones. El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Artículo 22. Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad. Capítulo IV De los delitos contra niños, niñas o adolescentes Artículo 23. Difusión o exhibición de material pornográfico. El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Artículo 24. Exhibición pornográfica de niños o adolescentes. El que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. Capítulo V De los delitos contra el orden económico Artículo 25. Apropiación de propiedad intelectual. El que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias. Artículo 26. Oferta engañosa. El que ofrezca, comercialice o provea de bienes o servicios mediante el uso de tecnologías de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave. **Título III Disposiciones comunes** Artículo 27. Agravantes. La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad: 1º Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido. 2º Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada o al conocimiento

privilegiado de contraseñas en razón del ejercicio de un cargo o función. Artículo 28. Agravante especial. La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito. Artículo 29. Penas accesorias. Además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente sin perjuicio de las establecidas en el Código Penal, las accesorias siguientes: 1º El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos previstos en los artículos 10 y 19 de la presente ley. 2º El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley. 3º La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión, arte o industria, o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función públicos, del ejercicio privado de una profesión u oficio o del desempeño en una institución o empresa privadas, respectivamente. 4º La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica. Artículo 30. Divulgación de la sentencia condenatoria. El Tribunal podrá disponer, además, la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo. Artículo 31. Indemnización Civil. En los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta Ley, el Juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado. Para la determinación del monto de la indemnización acordada, el Juez requerirá del auxilio de expertos. Título IV. **Disposiciones Finales** Artículo 32.Vigencia. La presente Ley entrará en vigencia, treinta días después de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela. Artículo 33. Derogatoria. Se deroga cualquier disposición que colida con la presente Ley. Dada, firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas a los seis días del mes de septiembre de dos mil uno. Año 191° de la Independencia y 142° de la Federación. Willian lara Presidente Leopoldo Puchi Primer Vicepresidente Gerardo Saer Pérez Segundo Vicepresidente Eustoquio Contreras Vladimir Villegas Secretario Subsecretario

En www.delitosinformaticos.com/delitos/

Legislación referente a Seguridad de la Información por País

ARGENTINA

Ley / Decreto	Publicación
11723 - Propiedad Intelectual	30-sep-1933
25036 - Propiedad Intelectual (Modifica 11723)	14-oct-1998
25326 - Habeas Data	02-nov-2000
Decreto 165/1994 - Propiedad Intelectual - Proteccion de Software	03-feb-1994
Ley 24624 - Presupuesto General de la Administración Nacional 1996	29-dic-1995
Decisión Administrativa 43/1996 - Uso de Tecnología. Valor Juridico - Reglamentación	07-may-1996
Ley 24766 - Ley de Confidencialidad	30-dic-1996
Ley 25506 - Firma Digital	14-dic-2001
Decreto 2628/2002 - Reglamentación Firma Digital	20-dic-2002
Disposición 5/2002 - Documentación Técnica de la Autoridad Certificante de la ONTI	06-may-2002
Artículo 5 - Constitución Nacional	24-jul-2006
Proyecto 5864 Delitos Informáticos	10-oct-2006
Otras Disposiciones 1 y 2	

BOLIVIA

Ley / Decreto	Publicación
27329 - Decreto Transparencia y Acceso a la Información Gubernamental	31-ene-2004

BRASIL

Ley / Decreto	Publicación
Artículo 5 - Constitución de la República Federativa de Brasil	27-abr-2006
Lei Federal 9472 - Segredo de Comunicações	16-jul-1997
Lei Federal 9507 - Habeas Data	12-nov-1997

CHILE

Ley / Decreto	Publicación
19223 - Ley Delitos Informáticos	07-jun-1993
19628 - Ley Protección de Datos de Carácter Personal	28-ago-1999
19799 - Ley Firma Electrónica	12-Abr-2002
19812 - Modificación Ley Protección de Datos de Carácter Personal	13-Jun-2002
19927 - Ley contra Pornografíticos Infantil	14-Ene-2004

COLOMBIA

Ley / Decreto	Publicación
Ley 57 - Transparencia y Acceso a la Información Gubernamental	05-Jul-1985
Artículo 15 - Constitución Política de Colombia (Datos Personales)	01-Ene-1991
Ley 527 - Información en forma de mensaje de datos	18-Ago-1999
Decreto 2170 - Certificación y Firma Digital	01-Ene-2003
Proyecto 154 - Proyecto de Ley 154 de 2004 Senado	03-Nov-2004
Acuerdo No. PSAA06-3334 - Reglamentación de medios electrónicos e informáticos en la justicia	02-Mar-2006

ECUADOR

Ley / Decreto	Publicación
Decreto Ejecutivo 3496 R.O. 735 - Reglamento a la Ley de Comercio Electrónico	31-Dic-2002
Ley 24 - R.O. 337 - Ley Orgánica de Transparencia y Acceso a la Información Pública	18-May-2004
Decreto Ejecutivo 163 - Libre acceso a fuentes de Información	07-Junio-2005

ESPAÑA

Ley / Decreto	Publicación
Decreto 994 - Reglamento de Medidas de Seguridad	11-jun-1999
23750 - 15/1999 - Ley Orgánica de Protección de Datos Personales	13-dic-1999
34/2002 - Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico	11-jul-2002

MEXICO

Ley / Decreto	Publicación

Ley para regular las Sociedades de Información Crediticia	15-ene-2002
Ley Federal de Transparencia y acceso a la Información Pública Gubernamental	11-jun-2002
Ley de Transparencia e Información Pública del Estado de Aguascalientes	30-jul-2002
Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	11-jun-2003
Ley del Instituto de Acceso a la Información Pública del Estado de Coahuila de México	04-nov-2003
Ley Federal de Protección de Datos Personales	14-feb-2004
Dictámen 105 de acceso a la información	25-ene-2006
Policy Objectives - A general description of the government's policy objectives	31-mar-2006
Artículo 16 de la Constitución Federal de los Estados Unidos Mexicanos	24-oct-2006

PARAGUAY

Ley / Decreto	Publicación
Ley 1682 de Información de caracter privado	12-dic-2000

PERU

Ley / Decreto	Publicación
27329 - Ley de Transparencia y Acceso a la Información Pública	31-ene-2004
28493 - Uso del correo electrónico comercial no solicitado (SPAM)	13-abr-2005

URUGUAY

Ley / Decreto	Publicación
17.838 - Habeas Data	01-oct-2004
Artículos de la Constitución referentes a la Privacidad y Seguridad	31-oct-2004
Proyecto de Ley AntiSpam	15-dic-2005

VENEZUELA

Ley / Decreto	Publicación
37313 - Ley Especial contra Delitos Informáticos	30-oct-2001

En http://www.segu-info.com.ar/legislacion

FUENTES CONSULTADAS

Bibliografía

- 🕮 Alcaide Fernández, Joaquín, *Las actividades terroristas ante el derecho internacional contemporáneo*, Madrid, Tecnos, 2000, 112 pp.
- 🕮 Alfaro, Reyna, *Los Delitos Informáticos: Aspectos Criminológicos, Dogmáticos y de Política Criminal*, Santiago de Chile, Ed. Jurista Editores, 2002, 269 pp.
- 🕮 Barragán, Julia, *Informática y Decisión Jurídica*, México, Distribuciones Fontamara, Primera Edición 1994, 184 pp.
- 🕮 Barrios Garrido Gabriela, *et al*., *Internet y Derecho en México*, México, Ed. Mc Graw Hill, 1998, 180 pp.
- 🕮 Bassiouni, M., Cherif, *International Criminal Law*, Nueva York, Ed. Transnational Publishers, Inc., vol. I: Crimes, 2a. ed., 1999, 165 pp.
- 🕮 Beccaria, César, *Tratado de los Delitos y de las Penas*, México, Editorial Porrúa, 1995, 168 pp.
- 🕮 Betancourt López, Eduardo, *Teoría del Delito*, México, Editorial Porrúa, 1994, 304 pp.
- 🕮 Bramont-Aria Torres, Luis Alberto, *Delitos Informáticos*, Caracas, Venezuela, Ed. Asesorandina S.R.L. Editores, 2000, 357 pp.
- 🕮 Claudio, Paul, *Análisis de la normativa sobre delincuencia informática en Chile*, Chile, Ed. Fundación Fernando Fueyo Laneri, 2002, 126 pp.
- 🕮 Clutterbuck, Richard, *Terrorism and Guerrilla Warfare, Forecasts and Remedies*, Londres, Ed. Routledge, 1990, 212 pp.
- 🕮 De la Maza, Gazmuri, Derecho y Tecnologías de la información, Chile, Ed. Fundación Fernando Fueyo Laneri, Escuela de Derecho, Universidad Diego Portales, 2002, 216 pp.
- 🕮 De Miguel Asensio, Pedro Alberto, *Derecho privado de Internet*, Madrid, Editorial Civitas, 2ª Edición, 2001, 415 pp.
- 🕮 De Pina y Vara Rafael, *Derecho Civil Mexicano, (Bienes-Sucesiones)*, México, FCE, 6ª edición, Volumen II, 1975, 411 pp.
- 🕮 *Diccionario de la Real Academia Española*, Madrid, España, Espasa Calpe S.A., Vigésima Primera Edición, 1992, 1856 pp.
- 🕮 Domínguez, Carlos Horacio, *La nueva guerra y el nuevo derecho*, Buenos Aires, Argentina, Ed. Militar, 1980, 126 pp.
- 🕮 *Enciclopedia RIALP*, Madrid, 1991, Vol. I, 365 pp.

📖 Fernández Esteban, María Luisa, *Nuevas tecnologías, Internet y derechos fundamentales*, Madrid, Editorial Mc Graw Hill, 1998, 165 pp.

📖 Flores Olea, Víctor, *Internet y la Revolución Cibernética*, México, Ed. Océano de México, 1997, 146 pp.

📖 Flory, Maurice, *Terrorism and International Law*, Nueva York, Ed. Routledge, 1997, 163 pp.

📖 Garfinkel, Simson, *et al*., *Delitos en Internet: seguridad y comercio en el web*, Madrid, Ed. Rústica, 1999, 282 pp.

📖 Garrote Fernández-Díez, Ignacio, *El Derecho de Autor en Internet. La directiva sobre derechos de autor y derechos afines en la sociedad de la información*, Granada, Editorial Comares, 2001, 123 pp.

📖 Gómez Tomillo, Manuel, *Responsabilidad penal y civil por delitos cometidos a través de Internet: especial consideración del caso de los proveedores de contenidos, servicios, acceso y enlaces*, Buenos Aires, Ed. Editorial Aranzadi, 2004, 269 pp.

📖 González de la Vega, Francisco, *Derecho Penal Mexicano*, México, Editorial Porrúa, 1996, 473 pp.

📖 González Quintanilla, José Arturo, *Derecho Penal Mexicano. (Parte General)*, México, Editorial Porrúa, 1993. 504 pp.

📖 Grün, Ernesto, *Una visión sistémica y cibernética del Derecho*, Buenos Aires, Editorial Abeledo-Perrot, 1995, 122 pp.

📖 Habermas, Jürgen, *La inclusión del otro, estudios sobre teoría política*, Barcelona, Editorial Paidós, 1999, 146 pp.

📖 Hance, Olivier, *Leyes y negocios en Internet* (Trad. de Yazmín Juárez Parra), México, McGraw Hill, 1996, 371 pp.

📖 Heinz, Federico, *Software Libre en el Estado*, Córdoba, España, Ed. Vía Libre, 2000, 165 pp.

📖 Hernando Collazos, Isabel, *Contratos informáticos: derecho informático: legislación y práctica*, Madrid, Ed. Librería Carmelo, 1995, 113 pp.

📖 Higgins, Rosalyn, *Problems & Process*, Clarendon press, Oxford, 1996, 103 pp.

📖 Jan Edward Schreibeer, *La última arma terrorismo y orden mundial*, Barcelona, España, 1980, 128 pp.

📖 Kissinger, Henry, *Does America need a Foreign Policy?*, Estados Unidos de América, Ed. Simon & Schuster, 2001, 318 pp.

📖 Laqueur, Walter, *Una historia del terrorismo*, (trad. Tomás Fernández A), Buenos Aires, Ed. Paidos, 2003, 352 pp.

📖 Leyton Zárate, Oscar, *Derecho penal: delitos informáticos*, Caracas, Venezuela, Caracas, Venezuela, Ed. Asesorandina S.R.L. Editores, 1989, 156 pp.

📖 Lima De La Luz, María, *Delitos Electrónicos*, en Criminalia, México, Academia Mexicana de Ciencias Penales, Porrúa, No. 1-6. Año L. Enero-Junio 1984. 100 pp.

📖 Lopezcano, George, *Diccionario De La Microcomputación*, Tomo II, Bogotá, Lexus, 1998, 632 pp.

📖 Malo Camacho, Gustavo, *Derecho Penal Mexicano*, México, Editorial Porrúa, 1998, 315 pp.

📖 Mansell R., *La revolución de la comunicación. Modelos de interacción social y técnica*, Madrid, Alianza editorial, 2003, 268 pp.

📖 Marigela, Carlos, *Mini manual terrorismo y guerrilla urbana, el nuevo frente de liberación mundial de los Estados Unidos*, 1967, 105 pp.

📖 Mc Quail, Denis, *Introducción a la Teoría de Comunicación de Masas*, Barcelona, Paidos Comunicación, 1983, 168 pp.

📖 Mccarty, Mary Pat, *et al*., *Seguridad Digital, Estrategias de Defensa Digital*, Madrid, McGraw Hill, 2002, 165 pp.

📖 Mejan, Luis Manuel, *El Derecho a la intimidad y la informática*, México,2º ed., Porrúa, 1996, 146 pp.

📖 Mkhondo, Rich, *Terrorism*, en Gutman, Roy et al., Crimes of War, Nueva York, Norton & Co. Ltd., 1999, 568 pp.

📖 Molina Salgado, Jesús Antonio, *Delitos y otros ilícitos informáticos en el Derecho de la Propiedad Industrial*, México, Porrúa, 2003, 107 pp. (Breviarios Jurídicos, número 7).

📖 Mora José Luis, Molina Enzo, *Introducción a La Informática*, 1974, 239 pp.

📖 Morón Lerma, E., *Internet y derecho penal: hacking y otras conductas ilícitas en la red*, Madrid, Ed. Rústica, 1999, 143 pp.

📖 O'Donnell, James, *Avatares de la palabra. Del papiro al ciberespacio*, edición española, 2002, 63 pp.

📖 Osorio, Manuel, *Diccionario de las Ciencias Jurídicas, Políticas y Sociales,* Argentina,Ed. Heliasta, 1990, 797 pp.

📖 Pacheco Escobedo, Alberto, *La contratación por medios electrónicos,* en Homenaje a Manuel Borja Martínez. México, Porrúa, Colegio de Notarios del Distrito Federal, 1992, Pág. 207 a 231.

📖 Palomar de Miguel Juan, *Diccionario para Juristas*, México, Mayo Ediciones, 1981, 739 pp.

📖 Pérez Luño, Antonio, *Ensayos de Informática Jurídica*, México, Fontamara, 1996, 151 pp.

📖 Pérez Luño, Antonio, *Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las N.T. de la información*, Madrid, Colección editorial Los libros de FUNDESCO, 1987, 296 pp.

📖 Reinares Nestares, Fernando, *Terrorismo y Sociedad Democrática*, Madrid, España, Akal editor, 1982, 163 pp.

📖 Rivera Llano, Abelardo, *Dimensiones de la informática en el Derecho (perspectivas y problemas),* Santa fe de Bogotá, Jurídica Radar, 1995, 285 pp.

📖 Roszak, Theodore, *El culto a la información. El folclore de los ordenadores y el verdadero arte de pensar* (Trad. de Jordi Beltrán), México, Consejo Nacional para la Cultura y las Artes, Grijalbo, 1990, 277 pp.

📖 Serrano Figueroa, Rafael, *El derecho humanitario frente a la realidad bélica de la globalización*, México, UNAM, Facultad de Derecho, 2002 (tesis doctoral), 130 pp.

📖 Soto, Alberto, *Derecho penal y delitos informáticos: Seguridad de la información, seguridad legal y seguridad jurídica. Una visión en Argentina*, Buenos Aires, Ed. Centro de Investigaciones en Nuevas Tecnologías Universidad Católica de Táchira, 2003, 76 pp.

📖 Tapia Valdés, Jorge A., *El terrorismo de Estado, la doctrina de la seguridad nacional en el cono sur*, México, Editorial nueva imagen, 1980, 106 pp.

📖 Téllez Valdez, Julio, *Derecho Informático*, México, 2º ed., McGraw Hill, 1995, 283 pp. (Serie Jurídica).

📖 Villalobos, Ignacio, *Derecho Penal Mexicano*, México, Editorial Porrúa, 1975, 650 pp.

📖 Williams P., *Redes transnacionales de delincuencia* en Arquilla, J. y Ronfeldt, D., *Redes y guerras en red. El futuro del terrorismo, el crimen organizado y el activismo político*, Madrid, Alianza editorial. 2003, 256 pp.

📖 Zanders, Jean Pascal *et al*., *Risk Assessment of Terrorism with Chemical and Biological Weapons*, en Stockholm International Peace Research Institute, SIPRI Yearbook 2000, Gran Bretaña, Oxford University Press, 2000, 538 pp.

Hemerografía

📄 Cable Associated Press, Washington, D.C., Septiembre, 1995.

📄 Callegari, Lidia, *Delitos Informáticos y Legislación* en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana, Medellín, Colombia, No. 70 Julio-Agosto-Septiembre, 1985, 115 pp.

📄 Castilleja J., et al., *El Quehacer De Los Crackers: ¿Terrorismo Informático?, Indispensable Legislar En Materia De Internet*, en Revista Mexicana de Comunicaciones, Núm. 10, febrero 2000, págs. 23-45.

📄 Fernández Calvo, Rafael, *El tratamiento de llamado "delito informático" en el proyecto de lo Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática),* en Informática y Derecho. 150 pp.

📄 Hertleng, Mark P., *Narcoterrorismo*, en Military Review, Edición hispanoamericana, Mayo/Junio, 1991, págs. 11-38.

📄 Isern, M., *Ciberespacio y Propiedad Intelectual*, mensaje nº 10, Infonomía, 17 de enero del 2001, 43 pp.

📄 Mila, Rodríguez, Ernesto, *Como será el terrorismo del siglo XXI*, Revista de publicaciones navales, Julio/Agosto, 1995, págs. 12- 33.

💾 "Decide Reuters no usar la palabra terrorista para describir a individuos, organizaciones o actos", La Jornada, México, 29 de septiembre de 2001, p. 7.

💾 "El libro de un billón de páginas. La ecología lingüística de la Web" en http://www.jamillan.com/ecoling.htm.

💾 "La OEA busca erradicar santuarios terroristas en América" El Nacional de Venezuela. 24 Noviembre, 1998.

💾 "La OEA creó organismo antiterrorista de las Américas" El Nacional de Venezuela. 25 Noviembre, 1998.

💾 Bryan Pfaffenberger, Linux in Higher Education.

💾 Castañeda, J. "La fiebre de los dominios". Baquía Internacional. 12 de marzo. 2001.

- Castro Bonilla, Alejandra. “La regulación de Internet un reto jurídico” en http://www.uned.ac.cr/redti/documentos/regulacion.pdf
- Crimen y Justicia Internacional, El mundo en breve, C & J: Sección 1, Volumen 14, Número 12, Enero, 1998.
- ECUP. “Por una Sociedad de la Información equilibrada”. Diciembre. 1997.
- El Mundo. “España, el tercer país que más sufre la ciberokupación”. 21 de marzo. 2000.
- Frente al terrorismo, La prensa de Honduras, C.A., 24 de Abril, 1997.
- Giobergia Cecilia, La revolución del Software Libre.
- Guerra, Terrorismo y Energía Nuclear, Greenpeace.
- Isern, M. “Ciberespacio y Propiedad Intelectual”, mensaje nº 10, Infonomía, 17 de enero del 2001.
- Laqueur, Walter. “Cuestiones mundiales, publicación electrónica del servicio informático y cultura de Estados Unidos” (U.S.I.S.), Vol. 2, N 1, Febrero, 1997.
- Laqueur, Walter. “Cuestiones mundiales, publicación electrónica del servicio informático y cultura de Estados Unidos” (U.S.I.S.), Vol. 3, N 3, Julio, 1998.
- Nuestro Mundo, Señala EE.UU. a siete países como auspiciadores de terrorismo en el mundo, 30 de Abril, 1998.
- Palast, Greg, “The Best Democracy Money Can Buy”.
- Rolando Rodrich, “Terrorismo y medios de comunicación”, 11 de Julio, 1998.
- Sáez Vacas, Fernando, Problema del año 2000: El mejor caso de estudio sobre socioinformática.
- Stallman, Richard Articulo ¿Puede confiar en su computadora?
- Todavía en condición de rehenes en el Perú, traducción libre del editorial del “Washington Post” en su edición de Diciembre, 1996.
- U. S. Department of State, Patterns of Global Terrorism 2001, 21 de mayo de 2005, en http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10235.htm
- Vallejo, Ana Luisa,” El terrorismo realidad de nuestro siglo”, Proa 28.

Leyes y documentos

- Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal. 2005.

- Decisión nº 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999 por la que se aprueba el plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. p.1-11.
- Informe del Comité Especial sobre el establecimiento de una Corte Penal Internacional, Asamblea General, quincuagésimo periodo de sesiones, suplemento núm. 22 (A/50/22).
- Legislación sobre propiedad industrial e inversiones extranjeras. Colección Porrúa. Editorial Porrúa. 19ª edición. México 2004.
- Ley de Vías Generales de Comunicación. Colección Porrúa. Editorial Porrúa. 23a edición. México 2003.
- Ley Federal del Derecho de Autor.
- Ley para la Promoción de la Competencia y Defensa Efectiva del Consumidor, Ley Nº 7472, de 20 de diciembre de 1994.
- Organización de las Naciones Unidas, Estatuto de Roma de la Corte Penal Internacional, aprobado en Roma el 17 de julio de 1998 y con las correcciones distribuidas por el depositario el 25 de septiembre de 1998 y el 18 de mayo de 1999 (PCNICC/1999/INF/3).
- Proyecto de Ley Nº 14700, Ley para el acceso y universalización de Internet
- Recomendación del Consejo de 25 de junio de 2001 sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología (2001/C 187/02).
- Resolución del Consejo de 19 de enero de 1999 sobre la dimensión relativa a los consumidores en la sociedad de la información. p. 1-3.
- Resolución del Consejo de 21 de noviembre de 1996 relativa a las nuevas prioridades políticas en materia de sociedad de la información. p. 1-5.
- Resolución del Consejo del 20 de junio de 1994 relativa a la difusión electrónica del derecho comunitario y de los Derechos nacionales de ejecución y a la mejora de las condiciones de acceso. p.3-5.
- Resolución del Consejo del 27 de abril de 1989 relativa a la normalización en el ámbito de las tecnologías de la información y de las telecomunicaciones.
- Resolución del Consejo del 3 de octubre de 2000 sobre la organización y gestión de Internet (2000/C 293/02).

- Resolución del Consejo y de los representantes de los Gobiernos de los Estados Miembros reunidos en el seno del Consejo de 17 de febrero de 1997 sobre contenidos ilícitos y nocivos en Internet, p.1-2.
- Resolución del Consejo, de 7 de febrero de 1994 relativa a los principios del servicio universal en el sector de las telecomunicaciones.
- The Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, (conocido como Anti-terrorism Act). En http://216.110.42.179/docs/usa.act.final.102401.html
- Tratado de Libre Comercio (TLC) entre Canadá, Estados Unidos de América y México

Ciberografía

- http: //www. infoservi.com.privado
- http://colossus.rhon.itam.mxl/spiosmalindex.html
- http://es.gnu.org/Licencias/gples.html
- http://info.lib.uh.edu/sepb/toc.htm
- http://www.aaba.org.ar
- http://www.apbnews.com
- http://www.archivovirtual.org/seminario/libroelectronico.htm
- http://www.bsa.org
- http://www.caast.org
- http://www.cafelug.org.ar/eventos/agosto/charlas.shtml,
- http://www.cita.es
- http://www.ciudadfutura.com
- http://www.clarin.com
- http://www.cnnenespanol.com
- http://www.cofe.edu
- http://www.comunidad.derecho.org
- http://www.cybercrimes.net
- http://www.derechoinformatico.com
- http://www.distrowatch.com
- http://www.dmoz.org

- http://www.faqs.es
- http://www.fast.org.uk
- http://www.fbi.gov/
- http://www.federacioneditores.org/
- http://www.freebsd.org/es/copyright/freebsd-license.html
- http://www.hackCanada.com
- http://www.iebaf.org/winners2001.asp
- http://www.infolibro.org
- http://www.infopanama.com
- http://www.interpol.com/Public/Terrorism/default.asp
- http://www.ips.edu.ar
- http://www.isu.edu
- http://www.itu.int/wsis/documents/listing-all-es-s|1.asp
- http://www.jjf.org
- http://www.libreros.org
- http://www.linux.org, Linux, Sistema Operativo, Página Web
- http://www.margay.fder.uba.ar
- http://www.mcu.es/Propiedad_Intelectual/indice.htm
- http://www.members.es
- http://www.members.xoon.com
- http://www.microsoft.com, Microsoft Corporation, Página Web
- http://www.microsoft.com/office/, Microsoft Office, Herramienta de Oficina
- http://www.microsoft.com/win/, Microsoft Windows, Sistema Operativo
- http://www.multired.com
- http://www.openebook.org
- http://www.openoffice.org, Open Office, Herramienta de Oficina, Página Web
- http://www.potosinstitute.org
- http://www.publishersweekly.com/
- http://www.redcyt.secyt.gov.ar
- http://www.sarenet.es
- http://www.securityfocus.com/
- http://www.siia.net

- http://www.softwarelegal.org.ar
- http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10235.htm
- http://www.stj-sin.gob.mx
- http://www.tiny.uasnet.mx
- http://www.turing.iimas.unam.mx
- http://www.un.org/Pubs
- http://www.un.org/spanish/docs/sc98/scrl98.htm
- http://www.undcp.org
- http://www.usia.gov/journals/itgic/0297/ijgs/spgj-8.htm
- http://www.websitemaker.com