UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

PATRULLAJE CIBERNÉTICO EN EL MÉXICO FOXISTA. REPORTAJE

T E S I N A

QUE PARA OBTENER EL TÍTULO DE LICENCIADA EN CIENCIAS DE LA COMUNICACIÓN PRESENTA:

NORMA ANA SPÍNOLA FERNÁNDEZ

DIRECTORA: MTRA. MA. GUADALUPE AÍDA LUNA LÓPEZ

CIUDAD UNIVERSITARIA, FEBRERO, 2008

DEDICATORIA

A mis padres Ignacio, por su amor y Olga por su ejemplo y guía. A ambos, por enseñarme el camino.

A mi esposo Alejandro, por su amor incondicional, su apoyo y paciencia, por ser mi cómplice en este reto que decidí emprender a destiempo.

A Bernardo y Diego Carlo, mis hijos, porque son mi estímulo para seguir adelante, mi tesoro invaluable.

A mis hermanos: Enrique, Lourdes, Graciela y Daniel, por su cariño y aliento, por la maravillosa aventura de crecer juntos.

A toda mi familia, y amigos más cercanos, por sus palabras.

"El tiempo de espera fue largo,
pero logramos el sueño"

AGRADECIMIENTOS

A mi asesora Maestra María Guadalupe Aída Luna, por su entusiasmo y sus consejos para poder concluir este trabajo. Por su calidad humana.

A mis sinodales, por sus comentarios y apreciaciones que me ayudaron a complementar este trabajo.

A Rosa de Guadalupe Guillén y Riebeling, por su apoyo y comprensión.

A María de Lourdes Quirós Pacheco, porque sin su ayuda no habría podido llegar a esta meta.

A todas mis compañeras y compañeros de trabajo, a mis amigos, quienes siempre estuvieron al pendiente de mis avances.

A mi querida Facultad de Ciencias Políticas y Sociales de los años setenta.

A la Universidad Nacional Autónoma de México, por el orgullo de poder llegar a sus aulas.

“POR MI RAZA HABLARÁ EL ESPÍRITU”

LA INTELIGENCIA CONSISTE NO SÓLO EN EL CONOCIMIENTO, SINO TAMBIÉN EN LA DESTREZA DE APLICAR LOS CONOCIMIENTOS EN LA PRÁCTICA

ARISTÓTELES

ÍNDICE

INTRODUCCIÓN

El uso de la tecnología informática es un instrumento que facilita a la sociedad su crecimiento económico y cultural, mediante su empleo en todas las áreas del desarrollo nacional.

El avance logrado en los últimos años en este sector, ha permitido que un creciente número de personas tengan acceso a esta tecnología y la utilicen cotidianamente para realizar actividades de muy diversa índole, como las educativas, culturales, comerciales, industriales, financieras o de comunicación, entre muchas otras. Hoy en día tiene tal importancia, que muchas de esas actividades no podrían realizarse sin el uso de equipos y sistemas informáticos.

Un ejemplo evidente de ello es la Internet que probablemente, en mayor medida que otros medios convencionales de comunicación, ha cambiado la concepción del trabajo, entretenimiento, educación, política y comercio que manifiesta una forma particular de operación.

Paralelamente al avance tecnológico, los comportamientos antisociales se han introducido en los equipos y sistemas informáticos convirtiéndolos en instrumentos para delinquir. Adicionalmente, se presentan conductas en las que dichos equipos o sistemas constituyen el objeto o fin en si mismo de la infracción.

El manejo y el uso de la información en la red de redes, tiene muchas líneas por explorar. Existen vacíos en los sistemas de seguridad informática, que garantizan que los recursos informáticos estén protegidos de factores externos, y que además no puedan ser dañados o alterados; así como en la aplicación y formulación de leyes; dicha situación convierte a la *internet* en un espacio propicio para la ejecución de los llamados “delitos cibernéticos.”

Por ello, es necesario contar con informaciones confiables, pertinentes y seguras frente a la diversidad y cantidad de mensajes propagados, así como de ilícitos concretados en la red, ya que se producen delitos como: la

comercialización de datos personales, delitos de fraudes financieros, abuso de menores, actos de ciberterrorismo, entre otros, en los que la información electrónica es la puerta de acceso.

Ante esta situación, es necesario conocer mejor las nuevas tecnologías, para poder entender, asociar, comparar, descifrar más claramente los hechos aparentemente inofensivos, de los que nos provee la *internet* como un medio de comunicación con ventajas y desventajas, como cualquier otro.

Se deben identificar las fuentes confiables de la información, en un universo que parece infinito y dicha tarea es un verdadero desafío. Determinar los delitos cibernéticos, también llamados “ciberdelitos”, entre otras acciones, supone y exige un análisis y una forma de lectura e interpretación para poder realizar una discriminación de la información.

Hay que resaltar que la *Internet*, como cualquier medio de comunicación, no es un vehículo que desarrolle o propicie por sí mismo la ejecución de actividades delictivas. Sin embargo, y porque existen las policías cibernéticas en el ámbito internacional y en nuestro país, éstas son una instrumento innovador de las corporaciones de procuración de justicia para la seguridad de todos los usuarios que navegan en la red, sea cual fuere su región geográfica en el mundo.

En este trabajo abordo la labor de la Policía Cibernética mexicana en cuanto al tipo de ilícitos que persigue, los problemas a los que se enfrenta ante la legislación añeja que no contempla delitos vía *internet,* y las historias de éxito de los últimos años.

Desde el inicio de la administración del Presidente Vicente Fox, México se colocó entre los principales países del mundo que cuentan con una Policía Cibernética dedicada a la prevención de delitos que se cometen a través de la *internet.*

Conformada por expertos en el manejo de sistemas informáticos, Psicología, Criminalística, Sociología, Ciencias de la Comunicación y otras disciplinas, la Unidad Especial de Policía Cibernética y Delitos Contra Menores, realiza “patrullajes” en la red a fin de detectar y prevenir delitos, en particular, aquellos que atenten contra las instituciones y/o contra la población más vulnerable.

La misión de esta Policía se basa en cuatro objetivos básicos:

- **Identificación y desarticulación** de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración y distribución y promoción de pornografía infantil.
- **Localización y puestas a disposición** ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos.
- **Realización de operaciones de patrullaje** antihacker, utilizando *internet* como instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red
- **Análisis y desarrollo de investigaciones** en el campo sobre las actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

Desgraciadamente, la *internet* se ha convertido en una especie de paraíso, lejos, muy lejos de las autoridades, lo que ha permitido que sea un sitio sumamente peligroso. En México, no tenemos el nivel de seguridad deseado, pero la Policía Cibernética está logrando progresos.

Realizo este trabajo como reportaje, porque refleja mi experiencia profesional. El reportaje es uno de los géneros del periodismo más versátiles, ya que permite relatar, describir y exponer los aspectos desconocidos, de algún tema. En el reportaje se pueden desarrollar casi todos los géneros periodísticos.

De acuerdo con Carlos Marín, en su Manual de Periodismo, el reportaje es el "(…) género mayor del periodismo, el más completo de todos. El periodista, en el reportaje, satisface el qué, quién, cuándo, cómo, dónde, por y para qué del acontecimiento del que se ocupa (…)"[1].

Los pasos para la realización del reportaje según este autor son:

a) la preparación, que incluye la motivación y la planeación con base en objetivos y enfoque de la indagación

b) la realización, que considera el acercamiento de todas las fuentes de información

c) el examen de datos, que posibilita la valoración de la información que derivará en la selección y jerarquización de los datos

d) la redacción, que realiza la estructura y escritura del reportaje

e) la publicación.

En este caso, realizo un reportaje narrativo que, según la clasificación de Marín, relata un suceso, hace la historia de un acontecimiento. En este trabajo investigo los antecedentes, historia, creación y operación de la Policía Cibernética mexicana.

Para la elaboración de este trabajo escogí la metodología estructuralista de Abraham Moles. El punto del cual parte Moles para sentar la base de su teoría de la comunicación es la consideración del hombre como individuo profundamente relacionado con su medio ambiente, del cual ha recibido siempre los primeros mensajes comunicativos y con el cual mantiene estrecha relación. Como consecuencia directa, modifica su comportamiento en función de los mensajes recibidos.

[1] Marín, Carlos, *Manual de Periodismo,* Ed. Debolsillo, 2006, pp 351

Moles señala que “(…)la comunicación es la acción que permite a un individuo o a un organismo, situado en una época y en un punto dado, participar de la experiencias-estímulos del medio ambiente de otro individuo o de otro sistema, situados en otra época o en otro lugar, utilizando los elementos o conocimientos que tiene en común con ellos (..)”*. Para Moles los elementos del acto de comunicación son: un emisor, un receptor, un canal y un mensaje[2]. En este caso la *internet* es el canal.

El individuo transforma su conducta de acuerdo con los mensajes que recibe, es decir, el medio (la Internet) puede ser usado como instrumento para delinquir o para enviar mensajes que pueden transformar la vida de las personas (la actividad de los pedófilos).

En el primer capítulo me refiero a la evolución de la *internet*, de cómo se ha popularizado su uso y la necesidad de contar con este medio de comunicación para realizar muchas actividades cotidianas y sobre todo abordo puntualmente el tema de los ciberdelitos. Asimismo, cito a diversos especialistas quienes se refieren al concepto de estos delitos.

También hago una breve cronología de las instituciones que antecedieron a la Policía Federal Preventiva, su creación y el nacimiento de la Policía Cibernética; además de cómo se llegó a la necesidad de crear una Policía Cibernética pues ante el acelerado crecimiento de la *internet*, ésta se convirtió en una puerta abierta para los malhechores.

Esta expansión de la delincuencia ha llegado a convertirse en un asunto que preocupa a todas las naciones del mundo. Es en el segundo capítulo en el que se muestran los esfuerzos de tres naciones para combatir la delincuencia on line. Seleccioné tres países con diferente desarrollo en esta actividad.

[2] Toussaint, Florence, *Crítica de la información de Masas,* Ed. Trillas, México, 1975, p43

En el tercer capítulo hablo de la actividad de la Policía Cibernética, la clasificación de los diferentes delitos informáticos y el patrullaje que llevan a cabo los vigías de la red en nuestro país.

El capítulo cuarto hace referencia a las historias de éxito que ha tenido esta corporación, explicando un caso concreto que muestra la forma en que actúa en el ciberespacio, como es el “Caso Decuir”.

“El Patrullaje Cibernético en el México Foxista”, pretende dar a conocer la forma en que una institución relativamente nueva, se abre paso en el espacio cibernético para mantener la seguridad de sus usuarios. La Policía Cibernética ya tiene cierto reconocimiento a nivel internacional; sin embargo, los intereses políticos y la inestabilidad de mandos dentro de la institución han provocado que no pueda mantener un desarrollo sostenido.

Capítulo I

EL ORIGEN DE UN NUEVO MODELO

1.1 Patrullando el ciberespacio

A lo largo de la historia el hombre ha necesitado transmitir y tratar la información de forma continua. Recordamos las señales de humo y los destellos con espejos, y más recientemente los mensajes transmitidos a través de cables utilizando el código Morse, o la propia voz por medio del teléfono. La humanidad no ha cesado en la creación de métodos para procesar información. Con ése fin nace la informática[3], como ciencia encargada del estudio y desarrollo de máquinas y métodos, y además con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo.

Luego nace *internet*[4] como una tecnología que pondría la cultura, la ciencia y la información al alcance de millones de personas de todo el mundo

El avance y la popularización de la *internt* durante la década del noventa en nuestro país, ofreció a los usuarios diversas formas de comunicación aparte de las ya existentes en los medios de comunicación tradicionales. Dos fenómenos favorecieron este proceso: la digitalización y la interactividad que brinda la posibilidad a usuarios conectados en red de comunicarse, navegar, conversar (chat), enviar mensajes por correo electrónico, etc.

Entre las principales razones del éxito de *internet* está el hecho de ser una red abierta. Como el protocolo o comunicación utilizado por las computadoras que se conectan a *internet* es gratuito, cualquier red y cualquier equipo pueden conectarse sin más costos que los de la conexión. No hay ningún propietario de

[3] Conjunto de conocimientos y herramientas científicas, técnicas y tecnológicas que se encarga del tratamiento racional y estructurado de la información por medios automáticos electrónicos digitales.
[4] INTERNET**.** Red mundial que conecta entre sí a computadoras del mundo y proporciona diversos servicios de intercambio de información. En su primera etapa la conexión de las computadoras fue a través de la red telefónica existente. Actualmente se desarrollan conexiones por medio de fibra óptica y vía inalámbrica.

internet, no hay ninguna autoridad central que pueda imponer un precio o unas condiciones diferentes de las estrictamente técnicas.

Hay cientos de millones de usuarios de *Internet* en todo el mundo. El cálculo estadístico de cuántos individuos tienen acceso a Internet ha perdido ya sentido. Hay clubes, cafés-*internet* y sitios públicos en ciudades de todo el mundo, incluyendo los países menos desarrollados, por lo que son miles de millones los individuos que pueden en cualquier momento, por un precio mínimo, conectarse a *internet*. Esta extraordinaria facilidad de acceso y popularidad es el principal atractivo desde el punto de vista comercial, pero también es la causa de que esté abierto a todo tipo de situaciones y sujetos.

En realidad, cualquier calle comercial de alguna ciudad del mundo es también accesible a los malhechores. Transacciones económicas realizadas por medios tradicionales son susceptibles de ser aprovechada por los amantes de lo ajeno. Las comunicaciones comerciales realizadas por medios tradicionales, cartas o teléfono, son mucho más fáciles de interceptar que las comunicaciones a través de *internet*. Realizar actividades delictivas a través de la red requiere de conocimientos técnicos que no están al alcance de cualquiera. Sin embargo, los delincuentes han logrado introducirse en el *ciberespacio*.

El término "*ciberespacio*" fue utilizado por primera vez por William Gibson[5] popularizado por el escritor estadounidense, John Perry Barlow[6], (autor de la Declaración de Independencia del Ciberespacio), para designar el "lugar" que se crea entre computadoras, redes y la información en ellos contenida.

El concepto de “delitos informáticos” o términos similares como “delitos cibernéticos” o “ciberdelitos”, se acuñó a finales de los años noventa, a medida que *internet* se expandió por toda Norteamérica. Después de una reunión en Lyón, Francia, en 1996, se fundó un subgrupo del grupo de naciones que conforman el

[5] William Gibson escritor americano de ciencia ficción que vive en Vancouver. Ha escrito relatos cortos desde finales de los 70. Su revolucionaria primera novela "Neuromancer" apareció en 1984. En este libro apareció el concepto de "ciberespacio".
[6] John Perry Barlow granjero retirado, cantante del grupo Grateful Dead y co-fundador y presidente ejecutivo del Electronic Frontier Foundation. Fue la primera persona en referirse al internet por la palabra de William Gibson "ciberespacio".

denominado G8 con el objetivo de estudiar los problemas de criminalidad que eran propiciados en la red. El “Grupo de Lyon” utilizó el término para describir, todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones.

Al mismo tiempo, y guiado por los participantes en el grupo de Lyón, el Consejo de Europa[7] comenzó a diseñar el *Tratado sobre Delito Informático.* Este tratado, fue presentado a la opinión pública por primera vez en el año 2000.

Fraudes, pornografía infantil, tráfico de personas, venta de drogas y armas, piratería, extorsión, amenazas, agresión, robos de señales satelitales, prostitución, clonación de tarjetas de crédito y terrorismo son algunos de los delitos que diariamente se comenten a través de la *internet*, muy comunes en países de primer mundo y que desde hace tiempo existen en México.

Miles de niños y jóvenes están expuestos en la red, los delincuentes y depredadores utilizan este medio para introducir material inapropiado como la pornografía infantil y solicitudes sexuales que pueden derivar en robos, abusos e, incluso, homicidios. Es por esa razón que en México surge un grupo de expertos en delitos Cibernéticos, cuya principal misión es velar por los derechos de las personas que usan computadoras para satisfacer sus necesidades de información y comunicación.

[7] [7] El Consejo de Europa, creado en 1949, es una organización política intergubernamental con sede permanente en Estrasburgo, Francia. Representa a 46 democracias pluralistas europeas, con cinco observadores: Canadá, Estados Unidos, Japón, México y El Vaticano. Entre sus objetivos tiene proteger los derechos humanos y hallar soluciones a problemas sociales como la discriminación hacia las minorías, xenofobia, intolerancia, terrorismo, tráfico de seres humanos, crimen organizado, **cibercriminalidad** y violencia contra la infancia.

1.2 Delincuencia *On Line*: los Ciberdelitos

El Tratado sobre Delito Informático elaborado por el Consejo de Europa, clasifica los ciberdelitos de la siguiente manera:

- Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
- Delitos relacionados con las computadoras (falsificación y fraude).
- Delitos relacionados con el contenido (pornografía).
- Delitos relacionados con la violación del derecho de autor y los derechos asociados (piratería, plagio).

Este tratado es el primer gran intento por tipificar lo que es un delito informático, lo cual nos lleva a plantearnos la primera interrogante que surge, es saber de qué hablamos cuando nos referimos a delitos informáticos. Si bien, no es unánime la definición es conveniente citar algunas de ellas:

Rafael Fernández Calvo, periodista, profesor y consultor español, autor del *Glosario Básico Inglés-Español para Usuarios de internet,* entre otras obras, define el 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 derechos y libertades de los ciudadanos (…)"[8].

Carlos Sarzara, tratadista penal italiano dice que el ciberdelito es "(…) cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena" (…)[9]. A su vez, la mexicana Nidia Callegari, especialista en derecho informático lo define

[8] Fernández Calvo Rafael, *Glosario Básico Inglés-Español para Usuarios de* internet www.ati.es/novatica/glosario/glosario
[9] Observatorio Bibliográfico del Derecho de la Economía. http:// www.iusimpresa.com (consulta 17/07/06)

como “(…) aquel que se da con la ayuda de la informática o de técnicas anexas"(…)[10].

Al respecto, la abogada mexicana María de la Luz Lima Malvido, ex Subprocuradora de Coordinación General y Desarrollo de la Procuraduría General de la República y presidenta de la Sociedad Mexicana de Victimología, entre otros cargos, apunta: "(…) delito electrónico en un sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel principal, ya sea como método, medio o fin.(…)" [11],

Como actividad delictiva en el ciberespacio, considera la Doctora en Derecho por la Universidad de Alcalá, Yolanda Fernández, "(…)todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen un uso indebido de cualquier medio informático (…)"[12] Algunos autores van más allá de una definición y los clasifican como es el caso del escritor mexicano Julio Téllez Valdés[13], maestro cofundador de la asignatura Metodología Sistemática e Informática del Derecho del Instituto Internacional del Derecho y del Estado, quien, utiliza dos criterios:

1. Como instrumento o medio, se tienen a las conductas criminógenas que se valen de las computadoras como método, medio en la comisión del ilícito.
2. Como fin u objeto, conductas criminógenas que van dirigidas en contra de las computadoras, accesorias o programas como entidad física.

De acuerdo con los autores Téllez Valdez y Lima Malvido, es imposible conocer la verdadera magnitud de los "delitos informáticos" ya que la mayor parte de éstos no

[10] http://www.portaldeabogados.com.ar (consulta 18/02/08)

[11] http://www.portaldeabogados.com.ar/noticias/derin03.htm (consulta 12/08/06)
[12] http:// www.portaldeabogados.com.ar/noticias/derin03.htm (consulta 18/02/08)
[13] Téllez Valdez, Julio. *Derecho Informático*. Editorial McGraw Hill, 282 p

son descubiertos o no son denunciados a las autoridades responsables; sumado al temor de las empresas de evidenciarlos por el desprestigio y la consecuente pérdida económica que esto pudiera ocasionar, hace que éste tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Según una iniciativa de ley propuesta el 22 de marzo de 2000, ante el pleno de la Cámara de Senadores de la Quincuagésima Legislatura, 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.”

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, que día con día muestran un incremento en México, expandiéndose de forma sumamente rápida.

1.3 Antecedentes

La Secretaría de Seguridad Pública a través de la Policía Federal Preventiva creó la Unidad Especial de Policía Cibernética y Delitos contra Menores, para conocer su nacimiento, comenzaré por hablar de sus antecedentes.

La Policía Federal Preventiva (PFP) nació el 13 de diciembre de 1998 como brazo operativo federal, con el fin de abatir los índices delictivos con una policía bien entrenada, equipada y mejor organizada. Uno de los argumentos para su constitución fue que se buscaba "(…) un cambio de fondo en lo relativo a seguridad pública, con el propósito de que la Federación cumpliera debidamente con su responsabilidad constitucional, en lo referente a la prevención del delito y mejorar orgánica y funcionalmente los servicios de seguridad pública a su cargo (…)".[14]

Cabe señalar que la aprobación de la iniciativa de ley para la creación de la Policía Federal Preventiva no fue fácil, ya que hubo opiniones encontradas. Algunos legisladores la calificaban de "represiva y autoritaria", mientras que otros la consideraron como "un peligro para la sociedad" y cuestionaron que no se llevara a cabo una consulta pública para medir sus consecuencias. Sin embargo, luego de largas discusiones la iniciativa fue aprobada con 89 votos a favor y siete en contra, el 11 de diciembre de 1998[15].

En este apartado es importante hacer referencia a los cuerpos de seguridad en nuestro país antes de la creación de la PFP.

En la época de la posguerra, se hizo el primer esfuerzo para crear una policía científica cuando por un acuerdo con los Estados Unidos se inició la lucha contra

[14] Secretaría de Seguridad Pública (SSP) federal.

[15] Senado de la República (Boletín de Prensa 98/259 11 de diciembre de 1998)

el narcotráfico, apareció el contrabando a gran escala y organizaciones criminales comenzaron a diversificar sus acciones.

Durante la administración del Presidente Miguel Alemán (1946-1952) se instituyó la Dirección Federal de Seguridad (DFS), el objetivo era tener una organización eficiente y moderna que protegiera al Presidente y que controlara la acción de la disidencia política, es decir, era una especie de policía política al servicio de los presidentes en turno.

Con el presidente Adolfo Ruiz Cortines (1952-1958) la DFS dejó de estar ligada a la Presidencia de la República y pasó a depender de la Secretaría de Gobernación, más que una transformación institucional se trató de un asunto personal, pues el nuevo mandatario no estaba de acuerdo con el perfil de la Federal de Seguridad.

Al asumir la presidencia, Adolfo López Mateos (1958-1964) designó a Gustavo Díaz Ordaz como secretario de Gobernación, quien a su vez nombró a Luis Echeverría Álvarez como subsecretario de Gobernación y fue éste el que eligió a Fernando Gutiérrez Barrios como subdirector de la Federal de Seguridad. Este pequeño grupo operó la línea dura contra la disidencia en todo el gobierno de López Mateos.

El presidente Gustavo Díaz Ordaz (1964-1970) ascendió como director de la DFS a Fernando Gutiérrez Barrios, con ello sólo se acentuaron las deficiencias estructurales. Entre 1947 y 1973 la DFS era una ínsula de poder. Era como un Estado dentro del propio Estado. Por tal motivo, Luis Echeverría ordenó regularla, pues durante su desempeño como secretario de Gobernación en el sexenio de Díaz Ordaz, comprobó que era un "monstruo incontrolable". La Federal de Seguridad, se transformó en símbolo de delincuencia. En la lista de quienes la recibían se incluyeron los capos de la droga y sus guardaespaldas[16].

[16] Aguayo Quezada Sergio, *"La Charola: Una historia de los servicios de inteligencia en México",* 2001 (Ed. Grijalbo, 2001)

Con Luis Echeverría Álvarez (1970-1976) la DFS siguió bajo el control de Fernando Gutiérrez Barrios. Durante su sexenio, LEA emitió un decreto en el Diario Oficial de la Federación el 16 de agosto de 1973 para reglamentar sus operaciones y atribuciones. No obstante, de esa aparente regulación, la DFS fue el instrumento más activo durante la llamada "guerra sucia".

El gobierno de José López Portillo (1976-1982) mantuvo los servicios de la DFS y le aumentó el presupuesto. El control de la información pasó de Fernando Gutiérrez Barrios a Javier García Paniagua y a partir de 1979 el cargo fue ocupado por Miguel Nazar Haro. En 1985 llegó José Antonio Zorrilla Pérez.

Dedicadas a actividades ajenas a sus funciones legales, el secretario de Gobernación en el sexenio de Miguel de la Madrid, (1982-1988), Manuel Bartlett Díaz, disolvió la DFS en 1985.

El presidente Carlos Salinas de Gortari (1988-1994) creó el Centro de Investigación y Seguridad Nacional (CISEN) que, según decreto presidencial, sería el organismo federal encargado de esclarecer y operar un sistema de investigación e información para la seguridad del país. Aún cuando Salinas de Gortari nombró a Fernando Gutiérrez Barrios secretario de Gobernación, no le permitió asumir el control del CISEN; nombró a Jorge Carrillo Olea como primer director, pero sólo lo mantuvo en el cargo un par de años. De hecho, durante su sexenio Carlos Salinas controló directamente al CISEN a través de José María Córdoba Montoya[17].

El Centro de Investigación y Seguridad Nacional (CISEN) fue instituido como un centro de inteligencia para la seguridad nacional, integrado por profesionistas especializados; era un organismo de inteligencia que no contaba con una parte operativa, no existía en México una corporación que instrumentara la información real generada por el CISEN para garantizar, mantener y restablecer el orden y la paz pública a nivel federal.

[17] Columna Indicador Político, Carlos Ramírez, El Financiero on Line, 20 julio 2007

Ante la necesidad de contar con un órgano que articulara a nivel federal los esfuerzos de prevención y combate al delito fue diseñada y puesta en marcha la Policía Federal Preventiva (PFP).

1.4 *Torre Pedregal*

La Policía Federal Preventiva (PFP), es el primer cuerpo de seguridad establecido por mandato del Congreso de la Unión en la historia del país, fue aprobada por el Congreso a finales de 1998, a propuesta del presidente Ernesto Zedillo Ponce de León (1994-2000) y formada por la Policía Federal de Caminos (PFC), una brigada del Ejército Mexicano y los cuadros establecidos en el CISEN, que se unieron a la Coordinación de Inteligencia para la Prevención. Como comisionado de la PFP fue nombrado Omar Fayad.

Al mismo tiempo, en Lima, Perú, en marzo de 1999 se llevaba a cabo la reunión de Ministros de Justicia o Procuradores Generales de las Américas (REMJA), constituida por los Estados miembros de la OEA y creada con la finalidad de impulsar la cooperación y apoyar los procesos de reforma y modernización de los sistemas de justicia en la región[18]. La REMJA recomendó establecer un grupo de expertos intergubernamentales sobre delito cibernético con el mandato de hacer un diagnóstico de la actividad delictiva vinculada a las computadoras y la información en la región.

También, exhortaron a realizar un diagnóstico de la legislación, las políticas y las prácticas nacionales con respecto a esa actividad, además de identificar las entidades nacionales e internacionales que tienen experiencia en la materia, y buscar mecanismos de cooperación dentro del sistema interamericano para combatir el delito cibernético.

Este diagnóstico concluyó que la delincuencia internacional ha convertido la *internet* en el medio más eficaz para superar las barreras geográficas y estar fuera del alcance de la policía, por lo que es necesario establecer, entre los Estados

[18] Países miembros: Argentina, Bahamas, Barbados, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Estados Unidos De América, Guatemala, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Saint Kitts Y Nevis, Suriname, Trinidad Y Tobago, Uruguay, Venezuela. Observadores permanentes ante la OEA: Egipto, España, Francia, Italia y La Santa Sede.

miembros de la OEA, una entidad o entidades públicas con la autoridad y función específica para llevar adelante la persecución del delito cibernético.

Asimismo, se hizo un exhorto a emprender acciones necesarias para implementar legislación sobre dicho delito, si aún no cuentan con ella. Se recomendó además, realizar todos los esfuerzos necesarios para armonizar sus legislaciones en materia de delito cibernético a fin de facilitar la cooperación internacional para la prevención y combate de estas actividades ilícitas.

En México, la Reunión de Ministros (REMJA), así como una situación especial aceleró la creación de una institución encargada de perseguir los delitos cibernéticos, la Policía Cibernética, dependiente de la recién creada Policía Federal Preventiva. Esta, es la historia:

En el año 2000, el Servicio de Aduanas de los Estados Unidos, que ya contaba con una policía cibernética llamada, News Customs Cibersmoglen Center, mejor conocida como C-3, por las tres C que tiene, informó a la Dirección de Tráficos y Contrabando de México, que se detectó la llegada de correos electrónicos de gente de Estados Unidos que invitaba a hacer turismo sexual infantil en Acapulco, Guerrero.

Un “benefactor” se dedicaba a tomar fotografías y grabar a niños. Este material era “cargado” en la *internet* y mediante correos electrónicos comenzaba a hacer contactos con gente que pertenecía a lo que en su momento se llamó la “Asociación Nacional de Amantes de Niños en Estados Unidos” (actualmente, existen innumerables páginas de este tipo con el título de “boy lovers”).

Es así como surge la necesidad de crear un área que tratara el aspecto técnico en la comisión de los delitos. Bajo este esquema, se empezó a trabajar coordinadamente con el C-3, a principios del gobierno del Presidente Vicente Fox, ya como La Unidad Especial de Policía Cibernética y Delitos contra Menores, (UEPCDM) dependiente de la Coordinación de Inteligencia para la Prevención de

la Policía Federal Preventiva (PFP), y primera en su tipo en México para responder al fenómeno de la red y las nuevas formas de convivencia social surgidas en el ciberespacio, así como a los delitos novedosos originados en ese ámbito o propagados a través de él.

La UEPCDM está integrada por setenta elementos de diversos perfiles: licenciados en Sistemas de Computación Administrativa, Ingenieros en Computación, en Electrónica, psicólogos, comunicólogos, sociólogos, y especialistas en Informática, ya que esta unidad tiene que ser multidisciplinaria porque no todos los temas son dominados por una sola persona; es un trabajo en equipo.

No necesariamente se requiere ser 100% informático, pero sí, ser de nivel superior terminado; además de aprobar diferentes exámenes como psicológico, polígrafo, toxicológico, físico, de conocimientos generales, médico y tomar un curso en la academia de la PFP.

Estos profesionales trabajan en un moderno edificio inteligente, conocido como Torre Pedregal, al sur de la ciudad de México, cubierto completamente por enormes cristales azules. Cada rincón de este lugar es vigilado por innumerables cámaras que observan el trabajo de los policías federales. Doce pisos albergan varias oficinas de la Policía Federal Preventiva; en un ala del octavo piso, los investigadores cibernéticos patrullan la supercarretera de la información, "a bordo" de un sofisticado equipo de cómputo, los "vigías" de la red están allí día y noche.

Durante su patrullaje cibernético, visitan lugares que son frecuentados por personas que distribuyen pornografía infantil o la fomentan con mensajes en sitios, comunidades o portales. Se hacen pasar por menores de edad, o por adultos que buscan pornografía, de esta forma tienen contacto con los pederastas. Es decir, realizan operaciones encubiertas, todo esto a través del "patrullaje" en *internet* mediante el cual es posible detectar estas personas ya que toda actividad en las

computadoras queda registrada en las mismas, ya sea en las del usuario final, en los nodos o en servidores que hospedan sitios web o de correo electrónico.

La Policía Cibernética trabaja en conjunto con instituciones educativas en el país; tal es el caso de la UNAM, que ayuda a ver la seguridad en sistemas de cómputo a través del UNAM-CERT[19] (Equipo de Respuesta a Incidentes de Seguridad en Cómputo). Con el ITAM en cuestiones jurídicas; con el ITESM en asuntos relacionadas a El Network Information Center (NIC México), que es la organización encargada de la administración del nombre de dominio territorial MX, el código de dos letras asignado a cada país. Con todas ellas, se tienen convenios para cursos y capacitación.

La Policía Cibernética tiene una base de datos en la que se tienen registrados tanto pedófilos como traficantes de menores. Con relación a los pederastas se ha propuesto que se legisle para que estas personas estén obligadas a informar a la policía cuando se cambian de domicilio, como se hace en los Estados Unidos. Esto es porque, de acuerdo con fuentes de la PFP, un pedófilo tiende a repetir su conducta[20]; es una persona que no se rehabilitará aunque haya pasado 20 años en la cárcel o haya tenido terapias psicológicas, por lo que, si se comete un abuso sexual o desaparece un menor de un lugar, éstos serán los principales sospechosos y rápidamente se podrán verificar los domicilios cercanos al lugar del crimen.

Además de los delitos contra menores, también se ve el fraude, *hackeo*, intrusiones a sistemas de cómputo y piratería por *internet*, localización de actividades ilícitas como la venta de drogas, armas, amenazas vía correo electrónico, anarquismo, terrorismo y todos aquellos delitos que utilicen una computadora en su proceso.

---

[19] UNAM-CERT se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún "ataque", así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios.

[20] "Ningún tratamiento consigue la curación de la pedofilia. La encarcelación, incluso a largo plazo, no cambia los deseos ni las fantasías de los pedófilos". Manual Merck de información médica, 2005, MSD. http://www.msd.es/publicaciones/mmerck_hogar/seccion_07/seccion_07_087.html (consulta 17/01/2007)

En este sentido, la Policía Cibernética es una instrumento innovador de las corporaciones de procuración de justicia para la seguridad de todos los usuarios que navegan en la web, sea cual sea su región geográfica en el mundo.

Hay que resaltar que la *internet* no es un medio que desarrolle o propicie la ejecución de actividades delictivas, sino que representa una fuente de recursos ya que el avance logrado en los últimos años en este sector, ha permitido que un creciente número de personas tengan acceso a esta tecnología y la utilice cotidianamente para realizar actividades de muy diversa índole, como las educativas, culturales, comerciales, industriales, financieras o de comunicación, entre muchas otras. Hoy en día tiene tal importancia, que muchas de esas actividades no podrían realizarse sin el uso de equipos y sistemas informáticos.

Además, el acelerado desarrollo de esta tecnología ha contribuido a la demanda de aplicaciones por parte de los usuarios, ya que su empleo hace más rápida y cómoda la comunicación y el proceso de la información.

1.5 *Un Asunto de Seguridad Nacional*

Paralelamente al avance tecnológico, han surgido nuevas formas de conducta antisocial y otras ya conocidas se han adecuado a los sistemas informáticos usándolos como instrumentos para delinquir. Adicionalmente, se presentan comportamientos en los que dichos equipos o sistemas constituyen el objeto o fin en si mismo de la infracción.

El crimen cibernético es un importante desafío global que, junto con otros tantos, requiere de una respuesta internacional coordinada.

La magnitud de los daños ocasionados por estas conductas depende de la información que se vulnere, al grado que pueden tener un fuerte impacto en el desarrollo de la economía, en las relaciones comerciales o en la seguridad nacional, o bien otro tipo de delito, como la pornografía infantil, por ejemplo.

Los delincuentes han descubierto que la *internet* puede ofrecer nuevas oportunidades y multiplicar los beneficios de los negocios ilícitos. El lado oscuro de la web, no solamente incluye el fraude y el robo, la pornografía y las redes de pedofilia, sino también el narcotráfico y las organizaciones criminales dedicadas al terrorismo, venta de armas, etc.

La creciente coincidencia entre el crimen organizado y el crimen cibernético demanda una estrategia integral ya que se ha convertido en una seria amenaza para la seguridad mundial. Sin embargo, sigue habiendo resistencia por parte de la comunidad internacional que aún no acepta la forma en que se equilibran los intereses de seguridad nacional en lo que se refiere a la confidencialidad, respeto a la libertad de expresión y manifestación de las ideas.

Un ejemplo de que muchas de las decisiones y acciones contra los delitos en el ciberespacio debe ser de manera coordinada es el Grupo de Trabajo de

Acción Financiera (GTAF)[21], organismo establecido en 1989 durante la reunión del Grupo de los Siete (G-7) realizada en París, Francia.

Este grupo ha intentado establecer normas y pautas que los gobiernos e instituciones financieras puedan utilizar en la creación de leyes, reglamentos y mecanismos de aplicación en cada país, además de investigar el flujo internacional de dinero obtenido a través de actividades ilícitas, como el narcotráfico y el terrorismo.

Luego de diez años de trabajo, el GTAF ofrece un plan de acción para que la comunidad internacional pueda combatir el crimen organizado. Por ejemplo, la Convención sobre el Crimen Cibernético adoptada por el Consejo de Europa[22], es el primer paso importante en esta dirección y se le puede considerar el inicio del proceso de fijar normas, con lo que finalmente se esperaría que los gobiernos de cada nación tomen en cuenta en sus gestiones legislativas, regulatorias y policiales.

En este esfuerzo es clave la cooperación regional que países como México tiene con la Organización de Estados Americanos mediante algunos instrumentos como el Grupo de Especialistas en Seguridad Cibernética, así como la creación de una red con equipos de respuesta a incidentes de seguridad para computadora, como parte de una amplia estrategia de seguridad cibernética que ha sido desarrollada por el Comité Interamericano Contra el Terrorismo de la OEA, establecido en 1998 por los ministros de justicia y fiscales del hemisferio y que su misión es buscar mecanismos para hacer frente al terrorismo, principalmente.

---

21 El GTAF es un cuerpo internacional independiente cuyo secretariado se encuentra en la OCDE [Organización para la Cooperación y el Desarrollo Económicos]. Los 29 países y gobiernos miembros de el GTAF son Alemania, Argentina, Australia, Austria, Bélgica, Brasil; Canadá, Dinamarca, España, Estados Unidos, Finlandia, Francia, Grecia, Hong Kong, China, Irlanda, Islandia, Italia, Japón, Luxemburgo, México, Nueva Zelandia, Noruega, Portugal, el Reino de los Países Bajos (Holanda), el Reino Unido (Gran Bretaña), Singapur, Suecia, Suiza y Turquía. Dos organizaciones internacionales son también miembros del GTAF: La Comisión Europea y el Consejo de Cooperación del Golfo.

22 Ibid., p.9

México trabaja para tener un marco jurídico nacional compatible y armónico con lo que sostiene la Convención Sobre el Crimen Cibernético. Los antecedentes de lo que está haciendo México en lo que se refiere a delitos cibernéticos se remontan a la suscripción, en 1996, de la Declaración de Estocolmo contra la explotación sexual infantil con fines comerciales, con la que nuestro país se comprometió a establecer medidas legislativas para evitar la pornografía y la prostitución infantiles.

Cabe destacar que la Convención sobre el Crimen Cibernético es el primer tratado internacional sobre crímenes cometidos por medio de la *red* y otras redes computarizadas; para lograr su plena vigencia, se han involucrado expertos de 45 países del Consejo de Europa y otros de Estados Unidos, Canadá y Japón.

Este tratado, sin duda, es uno de los más completos en su género pues abarca tanto los temas de pornografía infantil, fraude en la computación y violación de la seguridad de las redes, como el establecimiento de una política criminal común sobre el delito cibernético. Proporciona herramientas para combatir el terrorismo, los ataques contra las redes de computadoras y la explotación sexual de niños en la Internet.

En este convenio se clasifican los delitos informáticos en cuatro grupos y se definen los tipos penales que han de considerarse como delito informático.

1. **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.**

➠ Acceso ilícito a sistemas informáticos.

➠ Interceptación ilícita de datos informáticos.

➠ Interferencia en el funcionamiento de un sistema informático.

➠ Abuso de dispositivos que faciliten la comisión de los anteriores delitos.

2. Delitos informáticos.

➠ Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.

➠ Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

3. Delitos relacionados con el contenido.

➠ Producción, oferta, transmisión, adquisición o tenencia en sistemas o soportes informáticos, de contenidos de pornografía infantil.

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

En este sentido, el 17 de mayo de 1999 se publicó la modificación al título noveno del Código Penal Federal, con el nombre de "Revelación de Secretos y Acceso Ilícito al Sistema y Equipos de Informática" y se creó un Capítulo II con siete nuevos tipos penales.

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

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

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

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

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

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

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

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

ARTICULO 211 BIS 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

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

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

Un año después, el 29 de mayo de 2000, se publicaron diversas reformas y adiciones en materia de comercio electrónico al Código Civil para el Distrito Federal en materia común y para toda la República en materia federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor. A partir de la creación de la Unidad Especial de Policía Cibernética y Delitos Contra Menores, en 2002, se multiplicaron las reformas y modificaciones legales.

En junio de 2002, se publicaron las reformas y adiciones a diversas disposiciones del Código de Comercio, en materia de firma electrónica, para su regulación y efectos jurídicos en las transacciones y certificaciones electrónicas. En ese mismo año, inició funciones el Grupo de Coordinación Interinstitucional para Combatir los Delitos Cibernéticos, integrado por el gobierno federal y los gobiernos estatales, instituciones académicas, proveedores de servicio de *internet* y organizaciones civiles y privadas.

Casi un año y medio más tarde, comenzaron a notarse los cambios. En enero de 2004, se llevó a cabo en la Cámara de Diputados el Foro Legislativo en Materia de Delitos Cibernéticos, organizado conjuntamente con la OEA y el Departamento de Justicia de los Estados Unidos. Como resultado de estas reuniones, la Comisión Permanente del Congreso de la Unión exhortó a la

Secretaría de Relaciones Exteriores, a comenzar las gestiones para la adhesión de México al Convenio del Consejo de Europa sobre *cibercrimen*.

Varias semanas después, el subgrupo jurídico y de consultoría legislativa de Grupo DC México[23] entregó a la Comisión de Comunicaciones de la Cámara de Diputados, una propuesta de modificaciones a diversos ordenamientos legales para ser estudiada con el fin de elaborar una iniciativa al respecto. Esta es la iniciativa con proyecto de decreto que adiciona, reforma y deroga diversas disposiciones del Código Penal Federal, Código Federal de Procedimientos Penales, Ley federal Contra la Delincuencia Organizada y la Ley de la Policía Federal Preventiva.

La iniciativa plantea reformar el Código Federal de Procedimientos Penales para hacer más viable la conformación del cuerpo del delito y la probable responsabilidad, sobre la información contenida y transmitida a través de equipos y sistemas informáticos. También para incluir en este código y clasificar como graves los delitos de corrupción de menores, pornografía y lenocinio infantil.

Se contempla además la reforma a la Ley de la Delincuencia Organizada para el Tráfico de Menores considerando, dentro de este contexto, agregar los mismos delitos, ya que para su ejecución o para que se realice el delito descrito en la norma, en muchas ocasiones, participan tres o más individuos. Asimismo, se propone, y esto es muy importante, reformar la Ley de la Policía Federal

---

23 Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos en México (DC MÉXICO), se crea el 9 de Diciembre de 2002; tiene como sede las instalaciones de la Policía Federal Preventiva de la Secretaría de Seguridad Pública, en la Ciudad de México. El Secretario Técnico del Grupo DC, es el Coordinador General de Inteligencia para la Prevención de la PFP. DC MEXICO es un cuerpo colegiado interinstitucional que concentra la información necesaria para la identificación, monitoreo, rastreo y localización de todas aquellas manifestaciones delictivas en nuestro territorio como fuera de él, con efectos internos que implican fraudes, falsificaciones, intrusión en sistemas de cómputo, explotación sexual comercial y pornografía infantil, amenazas vía correo electrónico, operaciones de compra-venta de drogas y armas, apropiación y uso ilícito de propiedad intelectual, la sofisticación de fraudes electrónicos y, en general toda acción que ocurra en Internet y/o se apoye en el uso de un sistema computacional. Lo integran todas las corporaciones policiacas estatales y federales, así como los proveedores de servicio de Internet y todas las compañías privadas o públicas que ofrecen seguridad informática en el país. 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.

Preventiva, con el fin de que en el capítulo donde se señalan sus atribuciones, se incluya la verificación del tráfico de información a través de la *web.*

Con esta ley, además, se pretende formalizar la Unidad de la Policía Cibernética dentro de la estructura orgánica de la PFP, pues si bien, ya existe como Departamento de Análisis de Delitos Cibernéticos, resulta necesario que sea concebida como un cuerpo especializado, contemplado orgánicamente para dotarle de mayor eficacia, además de organización en sus recursos financieros, humanos y materiales. Sin la aprobación de esta iniciativa, la legislación mexicana seguirá sin observar muchas disposiciones especializadas para combatir el delito cibernético que dispone la Convención del Consejo de Europa.

La delincuencia organizada cuenta con avanzadas tecnologías y definitivamente, es capaz de desafiar a los gobiernos que no han reparado en la necesidad de actualizar su marco jurídico adecuándolo a las transformaciones que ha impuesto. Nuestro rezago jurídico, en esta materia, nos ubica en una situación de extrema vulnerabilidad frente a la ciberdelincuencia organizada.

Algunos proyectos financiados por la UE -como el *Cyber Tools On-line Search for Evidence* (CTOSE), (búsqueda de pruebas en línea con herramientas cibernéticas)- proporcionan espacios de referencia de las mejores prácticas para recopilar, analizar, almacenar y presentar las pruebas electrónicas a fin de reducir la delincuencia cibernética. Su objetivo consiste en establecer con absoluta precisión y sin lugar a dudas, lo que pasa cuando son cometidos los delitos informáticos e incluso durante una simple operación en la web.

Gracias a este desarrollo, los investigadores pueden utilizar “instrumentos de identificación criminal informática” para recoger y almacenar pruebas que puedan ser presentadas a lo largo de procedimientos judiciales.

Así, desde los administradores del sistema, el personal responsable de la seguridad de los sistemas de información y los investigadores encargados de incidentes informáticos hasta autoridades de policía y representantes de la ley, seguirán procedimientos coherentes y normalizados en las investigaciones sobre incidentes informáticos con la ayuda de "instrumentos de identificación criminal".

Para lograr esa política, es necesaria la cooperación internacional y la adopción de una legislación apropiada para cada país, ya que para que la ayuda jurídica mutua entre en vigor, es necesario un requerimiento de criminalidad doble es decir, el acto delictivo debe ser calificado como tal en ambas jurisdicciones. En otras palabras, la cooperación internacional se facilita enormemente con la concordancia de lo que es penalizado en las jurisdicciones nacionales.

Por ejemplo, Alemania ha sido el primer país de la Unión Europea en elaborar un proyecto de ley que regule expresamente el tema de los contenidos en *internet.* El proyecto de ley que ahora se debate en las cámaras legislativas alemanas va dirigido a perseguir la pornografía infantil y la propaganda neonazi, que en Alemania está prohibida.

No obstante, respecto a la responsabilidad por dichos contenidos se refiere exclusivamente a los autores de introducirlos en la red. De esta manera, los proveedores de acceso a *internet* no serán responsables por los contenidos albergados en su servidor o en otros servidores de la red, excepto en el caso de que se demuestre su conocimiento o su participación en la actividad infractora.

De acuerdo con informes de la Policía Federal Preventiva, en México, la Policía Cibernética tiene que enfrentarse a muchos obstáculos para realizar su labor, la delincuencia siempre le lleva la delantera a las autoridades policiales de las distintas corporaciones, pues la tecnología cambia cada año, mientras que la legislación está rezagada. Por ejemplo, en las leyes de nuestro país todavía no hay una tipificación de delitos como la pornografía infantil en *internet*.

Durante su gestión, el secretario de Seguridad Pública Federal, Alejandro Gertz Manero (2000-2004) envió una serie de iniciativas al Congreso para ampliar el margen de maniobra de la Policía Federal en todo el país. Dentro de esas iniciativas, la policía cibernética se vería beneficiada ya que podría contar con mejores herramientas para realizar su trabajo.

De acuerdo con "Roberto"[24], suboficial de la Policía Cibernética, aunque no se tiene una legislación que especifique los delitos que se cometen a través de una computadora, sí cuenta con los elementos jurídicos necesarios para que por medio del Ministerio Público los delincuentes cibernéticos puedan ser encerrados. Explica que el Ministerio Público "encuadra" el ilícito en un cierto patrón y lo equipara con uno tipificado. "Por ejemplo, no existía el delito de clonación de teléfonos celulares. ¿Cómo puede decir la legislación que se "roban" la señal de un celular cuando el Código Penal viene de 1929?, ¿Qué se hace en este caso? Hacer el equiparable:

"Una onda de teléfono celular viaja por una frecuencia, podría ser equiparable a un ducto por donde pasa el agua, la electricidad o la señal de cable. Se tuvo que hacer un peritaje para que se estableciera que una señal de teléfono celular viaja por un conducto. Así se estableció que la clonación de celular es equiparable al robo de fluido", señala "Roberto".

Las leyes en México deben incluir anexos en materia de Telemática, Informática y protección de la información, ya que esta tiene un valor muy importante para las empresas y si se encuentra o no vulnerable a la presencia de *hackers, crackers* o gente dentro de la empresa que no sea ética.

Se necesitan varios elementos, como asegurar que los delitos estén definidos en la ley; establecer poderes de investigación legales para combatir los

[24] "Roberto" es un elemento de la Policía Cibernética quien realiza patrullajes en la red, por razones de seguridad se omite su nombre real.

delitos cibernéticos y realizar estas actividades de manera que ofrezcan garantías que protejan los derechos humanos y las libertades fundamentales.

Uno de los primeros retos jurídicos que se plantean es establecer una definición de "datos sobre el tráfico" e "información sobre el suscriptor". La Convención sobre los Delitos Cibernéticos del Consejo de Europa, por ejemplo, define los datos sobre el tráfico como*: "(…) todo dato de computadora relativo a una comunicación por medio de un sistema de computadoras, generado por un sistema de computadoras que forma parte de una cadena de comunicación, y que indica el origen de la comunicación, el destino, la ruta, la hora, la fecha, el tamaño, la duración o el tipo de servicio (…)"*[25]*.*

La Convención define la información sobre el suscriptor como *"toda información, contenida en forma de datos de computadora o en cualquier otra forma, en posesión de un proveedor de servicios, relativa a los suscriptores de sus servicios, distinta de los datos sobre el tráfico o sobre el contenido, mediante la cual se puede determinar:*

a. El tipo del servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas y el período del servicio;

b. La identidad del suscriptor, su dirección postal o geográfica, el número de teléfono y otros números de acceso, información sobre facturas y pagos, disponible sobre la base del acuerdo o arreglo de servicios;

c. Toda otra información sobre el sitio en que está instalado el equipo de comunicaciones, disponible sobre la base del acuerdo o arreglo de servicios

A fin de respetar los derechos soberanos de los Estados y facilitar la cooperación internacional, es necesario estudiar la posibilidad de ofrecer

[25] http://www.coe.int

mecanismos internacionales formales, como las convenciones, ya que con ellas se han logrado consensos internacionales para combatir los delitos cibernéticos. Para que la asistencia judicial recíproca funcione efectivamente, los delitos sustantivos y los poderes procesales de una jurisdicción deben ser compatibles con los de la otra.

La comunidad internacional apenas está comenzando a enfrentar los múltiples desafíos que siguen apareciendo en este campo. Un ataque masivo de denegación de servicio que utilice cientos de computadoras de varios países para atacar sitios *web* comerciales en otro país, o el daño considerable causado por un virus o parásito que abarca a dos tercios del mundo plantean problemas fundamentales, por ejemplo, ¿dónde se ha cometido el delito y a quién hay que enjuiciar?.

Otra cuestión fundamental es cuál Estado podría tener la capacidad y la voluntad de comprometerse a realizar la investigación y comenzar actuaciones penales. Es evidente que los delincuentes cibernéticos transnacionales están preparados para explotar las lagunas creadas por las diferencias de los marcos jurídicos y de la capacidad de los sistemas de justicia penal. Por ejemplo, a falta de una compatibilidad funcional de los delitos sustantivos, lo que en un país puede ser un delito grave, en otro puede hasta pasar desapercibido.

Al mismo tiempo, se acepta cada vez más que cuando se requiere la doble incriminación, es decir, las conductas o los elementos básicos del delito los que deben corresponder, y no solamente la forma en que se tipificó el delito en los países de que se trate.

A diferencia de unos años atrás, ahora es posible hablar de un consenso internacional para combatir los delitos cibernéticos, especialmente, las formas trasnacionales que se dan con frecuencia. Por consiguiente, hay al final de cuentas, un “clima moral” para una acción concertada, ya sean medidas civiles,

penales o administrativas, y esta cooperación reconoce lo que los sociólogos denominan “comunidades de destinos compartidos”, las comunidades que comparten los mismos intereses.

La Convención sobre el Delito Cibernético se firmó el 23 de noviembre de 2001 y ha sido suscrita por 30 Estados y ratificada por 8 Estados. (La Convención puede ser refrendada por Estados no europeos y ya la han rubricado cuatro Estados no europeos (Canadá, los Estados Unidos, Japón y Sudáfrica). La convención entró en vigor el 1 de julio del 2004 y demanda que los Estados que la integran armonicen las leyes de su respectiva nación y que definen los delitos sustantivos. Éstos incluyen los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de computadoras, así como los delitos relacionados con las computadoras como la falsificación y el fraude cibernético, los delitos relacionados con la infracción de los derechos de autor, y los de pornografía infantil cometidos por medio un sistema de computadoras.

Además, la cuestión de los “delitos motivados por prejuicios” en la *internet* dio lugar a un protocolo adicional de la Convención sobre el Delito Cibernético para penalizar actos de naturaleza racista o xenofóbica cometidos mediante sistemas de computadoras.

Puede decirse que la ausencia de regulación jurídica, de límites y de control sobre los flujos de información son algunas de las notas características básicas de la autopista de la información. Como señala la abogada chilena Esther Morón Lerma: "(…) *Internet* no tiene presidente, director ejecutivo o mandatario. No existe la figura de una autoridad máxima como un todo. En realidad, nadie gobierna la red, no existe una entidad que diga la última palabra. No está bajo el control de ninguna empresa y, de hecho, son los propios usuarios quienes asumen la responsabilidad de su funcionamiento. Cada red integrante de *internet* tiene sus propias reglas (…) "[26].

[26] http://www.alfa-redi.org/area_tematica.shtml?x=173

Capítulo II

ALGUNAS EXPERIENCIAS INTERNACIONALES ANÁLOGAS

2.1 El desafío, tres naciones

La *internet* nació como una tecnología que puso la cultura, la ciencia y la información al alcance de millones de personas de todo el mundo, y que además permite que los usuarios actúen más allá de las fronteras del Estado en el que están situadas. Sin embargo, delincuentes diversos encontraron el modo de utilizarla para delinquir y, lo que es peor, hacerlo impunemente.

La red ya traspasa las fronteras territoriales, y une a la denominada aldea global[27], transportándonos a un mundo virtual. Estas nuevas tecnologías aportan beneficios, pero también han abierto la puerta a conductas antisociales y delictivas; este es el aspecto negativo que nos presenta la informática. Dentro de las conductas ilícitas más comunes que constituyen los llamados "delitos informáticos"[28], se encuentran: el acceso no autorizado a computadoras o sistemas electrónicos, la destrucción o alteración de información, el sabotaje por computadora, venta de drogas, armas, pornografía infantil la intercepción de correo electrónico, robo de identidad, el fraude electrónico y la transferencia ilícita de fondos.

Nuestro país, así como otras naciones del mundo, enfrentan el desafío del control y la vigilancia en el *ciberespacio*, sin poder evitar la transgresión a la territorialidad, la privacidad de los ciudadanos, la seguridad nacional, el derecho a la información, la libertad de expresión, el desarrollo de nuevos mecanismos de

---

[27] Marshall McLuhan, Bruce R. Powers, *La aldea global: Transformaciones en la vida y los medios de comunicación mundiales en el siglo XXI.* Colección El Mamífero Parlante. Barcelona: , Gedisa, 1996.

El escritor canadiense Marshali McLuhan, llamó "aldea global", al fenómeno de interrelación de los habitantes del planeta, por la cual, la población mundial forma una sola comunidad. Todas las novedades, incluidos los valores, las ideas y los adelantos científicos y culturales, trascienden las fronteras a través de los medios de comunicación, los libros, la música y el cine. El turismo intercontinental está en auge y el inglés se convirtió en un idioma casi universal.

[28] Según una iniciativa de ley propuesta el 22 de marzo de 2000 ante el pleno de la Cámara de Senadores de la Quincuagésima Legislatura, 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.”

seguridad, el adiestramiento constante de los órganos de vigilancia, la legislación vigente, y la colaboración de la iniciativa privada y la sociedad.

De acuerdo con la empresa Internet Systems Consortium, Inc.[29], hasta enero de 2007, existen en el mundo 600 millones de usuarios de *Internet.*

Sólo en el 2006 se reportaron, a nivel mundial un total de 41 mil 536 nuevas amenazas informáticas; durante noviembre y diciembre del 2005 se generaron siete mil nuevas formas de ataques en la red.

Por su parte, la empresa Symantec[30] identificó los países con mayor actividad maliciosa originada desde sus redes. Estados Unidos obtuvo el porcentaje más alto de actividad maliciosa total con 31%; China ocupó el segundo lugar con 10%; y Alemania fue tercero con 7%.

Cada día, aumenta la preocupación por el crecimiento desenfrenado de los delitos cibernéticos. Ante esta situación, muchos países del mundo han comenzado a tomar medidas, aquí se muestra los esfuerzos realizados por tres países que se toman como referente de cómo trabajan y organizan otras policías cibernéticas en algunos países donde existen estos organismos, ya que aún no todas las naciones cuentan con policías de este tipo.

[29] Empresa que ofrece servicios de software.

[30] Fundada en abril de 1982, Symantec es una empresa dedicada a ofrecer soluciones de seguridad informática. Tiene presencia en todo el mundo.

2.2 El Ciber Gendarme

En España, existe un organismo denominado Grupo de Delitos Telemáticos que fue creado para atender, dentro de la Unidad Central Operativa de Policía Judicial de la Guardia Civil, todas aquellas investigaciones que requirieran conocimientos técnicos para la persecución de los delitos que se sirven de la *internet* o de las nuevas tecnologías para su comisión.

Su origen se remonta a 1996, cuando en el seno de la Unidad Central Operativa de Policía Judicial, se desarrolló la primera investigación directamente relacionada con los medios informáticos. Ahí se puso en evidencia la necesidad de crear un grupo específicamente destinado a perseguir esta clase de delitos y que estuviera compuesto por agentes que combinaran su formación en investigación, con conocimientos de informática.

Compuesto por cuatro personas, en 1997, se creó el Grupo de Delitos Informáticos (GDI), que se encargó desde ese momento, de la investigación de las denuncias relacionadas con delitos informáticos que se presentaban a la Guardia Civil. Aquel Grupo participó en los casos de mayor relevancia, por su novedad y sofisticación técnica, ocurridos en España, como fueron la Operación **Toco**, en la que se detuvo en Tarragona a dos intrusos informáticos relacionados con el acceso ilegal a las computadoras de la Universidad de Tarragona, Universidad de Valencia, Centro de Supercomputación de Cataluña y Registro Mercantil de Tarragona.

También realizó la operación **Hispahack**, en la que se logró la detención de cuatro intrusos informáticos relacionados directa o indirectamente con el robo de dos mil quinientos datos de carácter reservado de un proveedor de *internet* de Girona, acceso ilegal a 16 computadoras de la Universidad Politécnica de Cataluña, modificación de la página *Web* del Congreso de los Diputados, e intentos de accesos no autorizados a equipos de la Universidad de Oxford y de la NASA.

En la Operación Diablo y Basura se detuvo a dos individuos en Palma de Mallorca y Madrid, por corrupción de menores y pornografía infantil a través de la *net*. A mediados de 1999, debido a que el campo de actuación del GDI se había ampliado no sólo a investigaciones que tenían que ver con redes de computadoras, sino a las relacionadas con el sector de las telecomunicaciones, se cambia su denominación adoptando la terminología empleada por otras unidades similares del mundo anglosajón (Hight Technology), para llamarse Departamento de Delitos de Alta Tecnología (DDAT).

En agosto de 2000, fruto de continuo crecimiento, este órgano adecua su estructura hacia una mayor especialización de sus miembros en cuatro áreas de trabajo, coincidentes con las presentadas en los debates del Convenio de Ciberdelincuencia del Consejo de Europa[31] en las que participaba personal del Grupo como expertos policiales.

Esta nueva estructura vino acompañada de cambio de nombre del Grupo, para llamarse Departamento de Delitos Telemáticos (DDT), con cuatro equipos de investigación centrados en las áreas de pornografía infantil, fraudes y estafas, propiedad intelectual y delitos de *hacking*. En febrero de 2003, la Unidad Central Operativa en la que se encuentra encuadrado el Departamento, sufre una reestructuración. El Departamento, sin modificar estructura, plantilla ni misiones, adquiere su actual nombre, Grupo de Delitos Telemáticos (GDT).

El incesante incremento de los ya conocidos como delitos informáticos y los innumerables apoyos que se le solicitan desde todas las unidades de la Guardia Civil, restó eficacia al GDT, por lo que se inició una política de descentralización de las investigaciones consistente en formar y crear Equipos de Investigación Tecnológica (EDIT) en cada una de las provincias de España. Este proceso de formación es asumido por el GDT, lo que le proporciona un *plus* en el terreno de la

[31] El 23 de noviembre de 2001 se firmó en Budapest el "Convenio de Ciberdelincuencia del Consejo de Europa", cuyo fin es definir el marco de referencia de la Unión Europea (UE) sobre los delitos cometidos a través de la red.

formación para investigación informática, que posteriormente, exportará a otros países de latinoamérica.

Muy importante en la historia del Grupo, ha sido su presencia cada vez mayor, en seminarios y conferencias internacionales, lo que ha permitido contar con una red de contactos policiales a nivel internacional, esenciales en la resolución de determinados casos. Cabe destacar, que desde octubre de 1997, el GDI es miembro de los Grupos de trabajo europeos de INTERPOL[32] en delitos relacionados con la Tecnología de la Información (EWPITC), y participa en sus reuniones como miembro de pleno derecho. Asimismo, desde que EUROPOL[33] asumió el mandato sobre cibercrimen, este grupo participa en cuantas reuniones se desarrollan en ese ámbito.

Desde 2002, el GDT organiza anualmente un Foro Iberoamericano de Encuentro de Ciberpolicías (FIEC), que se ha constituido en un referente de la colaboración internacional entre las unidades de lucha contra la delincuencia informática a nivel americano y nexo de unión con otros foros a nivel europeo.

Cabe destacar que una de las acciones más importantes realizadas por el GDT es la "Operación Azhar", que se llevó a cabo el 24 de febrero de 2006. La Guardia Civil creó el programa informático Híspalis, dedicado al rastreo e identificación en la red que permitió desarrollar con éxito una operación policial en 19 países de Europa, Sudamérica y México, operación que sigue abierta. Este

[32] INTERPOL es la mayor organización de policía internacional, con 186 países miembros, por lo que es la tercera organización internacional más grande del mundo. Creada en 1923, apoya y ayuda a todas las organizaciones, autoridades y servicios, cuya misión es prevenir o combatir la delincuencia internaciona. La sede de la organización está en Lyon, Francia. www.interpol.int/

[33] EUROPOL La Oficina Europea de Policía fue creada en 1992 para explotar a nivel europeo la información sobre actividades delictivas. Su sede está en La Haya, en los Países Bajos, y su personal incluye a representantes de organismos nacionales relacionados con la Justicia: policía, aduanas, servicios de inmigración, etc. El Consejo de administración de Europol consta de un representante de cada país de la UE. Su objetivo es ayudar a los Estados miembros a cooperar estrecha y eficazmente a fin de prevenir y combatir la delincuencia internacional organizada, en particular: el tráfico de drogas, las redes de inmigración, el tráfico de vehículos, la trata de seres humanos, así como la pornografía infantil, la falsificación de dinero y otros medios de pago, el tráfico de sustancias radiactivas y nucleares y el terrorismo. http://europa.eu/agencies/pol_agencies/europol/index_es.htm

'software' está diseñado específicamente para detectar el rastro de determinadas imágenes de carácter pedófilo en la *internet*.

La operación consistió en el registro de docenas de “domicilios"**,** en los que se detuvo a casi cien personas, veinte de ellas en España, y se incautaron equipos de cómputo para obtener las pruebas necesarias.

En este caso, por primera vez la Guardia Civil identificó y detuvo a una mujer distribuidora de pornografía infantil, a la que se le intervinieron numerosas imágenes y videos.

La acción fue coordinada por Eurojust e IberRed[34], y se desarrolló de forma simultánea en 19 países: España, Portugal, Francia, Polonia, Bélgica, Dinamarca, Estonia, Finlandia, Lituania, Reino Unido, Estados Unidos, México, Argentina, Chile, Brasil, Venezuela, República Dominicana, Panamá e Israel.

El programa Híspalis permite obtener las direcciones IP de las computadoras emisoras de ciertas imágenes de carácter pedófilo que han sido previamente identificadas, de forma que pueden localizar tanto a los usuarios como los domicilios en los que se encuentran en cualquier país del mundo**.**

Una vez localizados los equipos, Eurojust organizó una reunión de coordinación para preparar las acciones de forma simultánea. Tras la labor de investigación de las policías de los 19 países, se logró la identificación de 131 personas y el registro de 485 domicilios.

Esta herramienta, puesta a disposición de todas las policías del mundo, supone un antes y un después en la investigación en *internet*. Hasta la fecha, las actuaciones policiales se iniciaban a raíz de denuncias, tanto oficiales como anónimas. Ahora, se puede detectar a los pedófilos a través de miles de fotografías y vídeos que la Guardia Civil ha "marcado" para seguir su rastro cuando las intercambian en la red.

[34] Red de cooperación judicial de Iberoamérica

De esta manera, la Guardia Civil, así como el resto de policías del mundo que lo deseen, podrán "patrullar la *red*" en busca de consumidores de pornografía infantil. Esta iniciativa, pionera a nivel mundial, supone acabar con el anonimato de las personas que distribuyen pornografía infantil apoyándose en identificadores de imágenes y archivos, llamados *hash* (una especie de "huellas digitales" de cada archivo y que son colocados en una lista que se incluye en el programa) que pueden ser rastreados por la policía en los servidores conocidos como “Peer to Peer” (P2P)[35].

[35] Redes de intercambio de archivos

2.3 La Ciber Brigada en La Patagonia

La Policía de investigaciones de Chile, consciente de los avances tecnológicos en el ámbito delincuencial, crea el 16 de Octubre del año 2000, la "Brigada Investigadora del Ciber Crimen", unidad especializada en los delitos cometidos vía *internet*, tales como, amenazas, estafas, falsificación y pornografía infantil, entre otros.

Esta unidad, es pionera en la investigación de los delitos de carácter informático. Ya en 1995, se descubrió que estaba intervenido el sitio *web* de la Cumbre de Presidentes. En 1996, puso al descubierto el sabotaje del sistema computacional del SII, en este caso el autor fue detenido. En 1997, se llevó a cabo una importante misión llamada "Operación Catedral", sobre pornografía Infantil.

Fue en septiembre de 1998 cuando más de un centenar de sospechosos de veinte países son detenidos en la "Operación Catedral". Esta acción fue coordinada por la Policía británica para investigar la red de "Wonderland". Se hallaron bases de datos con más de cien mil fotografías pornográficas de niños, algunos menores de dos años.

En coordinación con países de varios continentes, en 2003 participó en la "Operación Global"[36], con el objeto de atacar los sitios de pornografía infantil. Durante esta operación que inició en mayo de 2004, se detuvo a tres sujetos de nacionalidad chilena, a quienes se les encontraron más de 10 mil imágenes de pornografía infantil.

La "Operación "Global", que comenzó en España en 2003 y luego se extendió a Argentina, Brasil, Colombia, México y Chile, ha logrado la detención de más de veinte personas. La investigación internacional estableció que los implicados operaban en *internet* como una comunidad cerrada, intercambiando imágenes y videos de pornografía infantil y textos con relatos pedófilos, mediante

[36] La operación Global encabezada por Chile, detectó una red pederasta en 77 países y se estima que la integran mas de dos mil personas.

páginas web, correos electrónicos y foros dirigidos a menores de edad, en los que se hace apología del abuso sexual.

La Brigada chilena se encuentra en permanente capacitación a sus policías, manteniéndolos al día en las nuevas tecnologías, además de asistir a diversos foros internacionales relacionados con los delitos cibernéticos. Tiene entre sus filas a policías con estudios universitarios, en materias relacionadas con la Informática, Derecho y Psicología, lo que hace que sea una unidad profesional y científica.

También se mantiene en contacto con la comunidad, mediante constantes charlas y presentaciones en escuelas, centros comunitarios, universidades, programas de televisión de radio y empresas, donde informa sobre delitos informáticos, pornografía infantil o el debido uso de la *internet*.

2.4 Ciber Incas

La División de Investigación de Delitos de Alta Tecnología DIVINDAT es el cuerpo especializado dedicado a investigar y combatir los delitos realizados a través de *internet* en Perú.

La DIVITAD nació en agosto del 2005. Esta División fue creada por disposiciones de la Alta Dirección de la Policía Nacional peruana (PNP) y no se trata de cualquier trabajo policial, sino de un patrullaje virtual en el *ciberespacio* que demanda estar en las mismas o en mejores condiciones tecnológicas que los delincuentes informáticos. Sin embargo, este grupo no cuenta con recursos para operar y sólo recibe un presupuesto muy bajo. A pesar de llevar en su nombre las palabras “alta tecnología”, no tiene el equipo necesario para llevar a cabo su “patrullaje” y las computadoras que utiliza son donaciones de la iniciativa privada.

En 2005, se registraron 456 denuncias; de ellas, 243 casos se resolvieron, y quedaron pendientes 213. Según menciona en su página electrónica, actualmente está en un proceso de equipamiento de tecnología de última generación, tanto de *hardware* como de *software* y la capacitación de su personal, para combatir los delitos informáticos.

Uno de los logros más importantes de esta modesta policía es el “Caso Dragoneti”, Un falso productor de cine de películas "triple x" con el seudónimo de Dragoneti**,** contactaba a menores de edad a través de *internet* a quienes convencía para posar desnudas ante cámaras fotográficas y de video. Luego de varios meses de investigación, el pedófilo fue detenido cuando esperaba a una menor de edad, le fueron encontrados varios diskettes que contenían fotografías de niñas con poses sugerentes y sexo explícito.

De acuerdo con el Director de Investigaciones Criminales de la PNP, General Eduardo Montero Romero, dentro de poco tiempo, la DIVITAD interactuará con otros cuerpos policiales de Estados Unidos y naciones de Europa para realizar operaciones conjuntas en el ciberespacio.

Aún hay mucho que hacer a nivel mundial en materia de combate a los delitos cibernéticos. Países como Estados Unidos, Rusia, Inglaterra, España, Holanda, Alemania y Australia, junto con México, se encuentran a la vanguardia en el combate de este tipo de delitos e intercambian experiencias y datos.

Sin embargo, es preciso avanzar hacia normas comunes de armonización internacional, por medio de tratados internacionales que deberán quedar complementados con medidas de cooperación internacional de tipo judicial y policial. Asimismo, es necesario prestar atención a los avances técnicos para poder perfilar, en el futuro, un mayor control sobre la información ilícita que circula en la red a nivel mundial.

Capítulo III
MEXICO BAJO LA LUPA

3.1 Unidad Especial de Policía Cibernética y Delito contra Menores

Como ya lo mencionamos en el primer capítulo, en México, La Unidad Especial de Policía Cibernética y Delito contra Menores, es una unidad dependiente de la Policía Federal Preventiva (PFP), primera en su tipo en México. Se encarga de llevar a cabo las estrategias preventivas de delitos que se cometan en el *ciberespacio* y a través del uso de medios informáticos; tienen un área exclusiva para la prevención y atención de denuncias de delitos contra menores.

La misión de esta Policía se basa en cuatro objetivos básicos:

- **Identificación y desarticulación** de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración y distribución y promoción de pornografía infantil.

- **Localización y puestas a disposición** ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos.

- **Realización de operaciones de patrullaje** antihacker, utilizando *internet* como instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.

- **Análisis y desarrollo de investigaciones** en el campo sobre las actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

La UEPCDM opera de la siguiente manera: vigila la red mediante sistemas convencionales para rastreo. Su patrullaje se centra sobre *hackers*, sitios de *internet*, comunidades y *chat rooms* en los que promueven la pornografía y el

turismo sexual infantil. Utiliza la misma *internet* como un instrumento para detectar a delincuentes que organizan sus actividades en algún lugar del ciberespacio. Además, lleva a cabo análisis sobre actividades de organizaciones locales e internacionales de pedofilia así como de redes de prostitución infantil y de tráfico de menores que son explotados en otros países.

3.1.1 La Ciberpolicia se Organiza

Dentro de la Unidad de la Policía Cibernética existen dos grandes divisiones, la división de delitos cibernéticos propiamente, es decir los que se cometen usando computadoras y por otro lado los ataques contra menores.

Esta Unidad comprende las siguientes áreas:

DELITOS CIBERNÉTICOS

- Atención a Delitos Cibernéticos
- Atención a Delitos Usando Computadoras
- Análisis de Cómputo Forense (instalación de trampas para atrapar intrusos)

DELITOS CONTRA MENORES

- Análisis de Explotación de Menores
- Atención a Menores Desaparecidos

COORDINACIÓN INTERINSTITUCIONAL

- DC México
- Centro de Análisis e Intercambio de Información para la Identificación de Alerta Temprana y Riesgos
- Mecanismos de Coordinación Interinstitucional
- Información y Prevención

3.2 Una Amenaza sin Pasaporte

La Policía Cibernética mexicana está incorporada al Grupo de los Ocho[37], a través del High Tech Force, una corporación internacional que reúne a las fuerzas públicas de los distintos países, para hacer las persecuciones en *internet* y poder asegurar que los delincuentes sean castigados; sobre todo, cuando se ha magnificado el uso de la tecnología para cometer actividades ilícitas.

Esta Policía Cibernética trabaja codo a codo con distintas corporaciones, se desempeña en un esquema de coordinación interinstitucional que incluye no solamente a dependencias del gobierno, sino también académicos, organizaciones de la sociedad civil, incluso, proveedores de servicio de la *red*, como la estadounidense Microsoft[38] la cual ha decidido apoyar decididamente a este grupo para darle un portal en *internet* y para asegurar que en todos los portales horizontales[39] aparezca ya un *banner* o anuncio de la policía cibernética para que la gente tenga oportunidad de hacer denuncias.

Los trabajos de inteligencia que desarrolla la Policía Cibernética se han concentrado, primero, en identificar plenamente quiénes son los traficantes que están operando en México, y segundo en elevar a grado de certeza la información que da la ciudadanía a través de las denuncias.

Una de las tareas es justamente, el trabajo coordinado con otras dependencias para combatir el tráfico ilícito de personas. En México, la cercanía con los Estados Unidos, nos hace un país de tránsito constante de muchos

---

[37] El G-8 esta integrado por Alemania, Canadá, Estados Unidos, Francia, Italia, Japón, Reino Unido y Rusia. Los gobernantes de estos ocho estados se reúnen una vez al año en lo que se conoce como la "Cumbre del G8", para hablar sobre la evolución de la economía, la política y la sociedad mundial, y para acordar líneas comunes de actuación en dichos campos.

[38] Microsoft es una empresa multinacional estadounidense fundada en 1975 por Bill Gates y Paul Allen dedicada al sector de las tecnologías de la información con sede en Redmond, Washington, Estados Unidos. Microsoft creó y ofreció gratuitamente Internet Explorer.

[39] Portales horizontales, también llamados portales masivos o de propósito general, se dirigen a una audiencia amplia, tratando de llegar a toda la gente con muchos temas. Como ejemplo de portales de esta categoría están AOL, AltaVista,UOL, Lycos, Yahoo, MSN.

migrantes que desean tener en los Estados Unidos un futuro alentador para sus familias; sin embargo, son presa de gente sin escrúpulos que los explota y abusa de ellos para lucrar con sus necesidades.

¿Cuándo nos íbamos a imaginar que nuestras computadoras se convertirían en una amenaza para nuestra seguridad, la de nuestros hijos y para nuestra economía?, ¿cuándo íbamos a pensar que navegar en la red, en pleno auge de la cibernética, sería un peligro?

A medida que se va ampliando la *internet*, aumenta el uso indebido de la misma. Los denominados delincuentes cibernéticos se pasean por el mundo virtual y estos son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables "enlaces" o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden dañar las comunicaciones o esconder pruebas delictivas en "paraísos informáticos", es decir, en países que carecen de leyes o experiencia para seguirles la pista.

Se habla constantemente de los beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual; sin embargo, este avance también nos muestra otra cara de la moneda: las conductas delictivas. Esto ha provocado que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información. Este hecho puede obstaculizar el desarrollo de nuevas formas de comunicación, de hacer negocios, del intercambio de productos y servicios, etc.

Ante esta situación, se han implementado nuevas formas de seguridad. Actualmente, en los años dos mil en México, la red está vigilada las 24 horas, la Policía Cibernética lucha contra la pornografía infantil y protege a los usuarios contra acosadores pedófilos, estafadores y otros delincuentes de la web.

La Policía Federal Preventiva, lleva a cabo un despliegue de operaciones encubiertas en la red. Para los oficiales de la Unidad el día laboral comienza a las 8:45 de la mañana, hora en que empiezan a atender y dar seguimiento a las denuncias que realiza la población. El patrullaje consiste en navegar bajo ciertos patrones de búsqueda para localizar sitios con contenido ilícito: venta de drogas, armas, pornografía infantil, activismo de hackers, crackers, páginas falsas para engañar al usuario y que pierda dinero, etcétera.

¿Cómo lo realiza?, los policías cibernéticos cuentan con ciertas claves y métodos para poder ingresar a las páginas de *internet*. Lógicamente estas "claves" no se pueden dar a conocer, porque son la herramienta con la que trabajan para poder detectar esos sitios.

Una vez que ubican el problema y al responsable, se apoyan en el Ministerio Público (MP) para actuar. La Policía Cibernética no hace directamente las detenciones, a menos que se los requiera el MP o al sorprender en flagrancia al presunto infractor.

La labor de la Policía Cibernética ha permitido ir conociendo una serie de patrones que son resultado de sus extensos patrullajes en la red. De acuerdo con "Roberto", los delincuentes actúan entre las 12 del día y las tres de la tarde para subir las "ofertas"; utilizan cuentas bancarias donde las víctimas realizan sus depósitos. 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 localiza en los estados de Jalisco, Estado de México, Morelos, Yucatán, Sonora y Sinaloa".

Otra de las actividades de la Policía Cibernética es el rastreo de programas malignos (virus), en promedio, se crean y diseminan alrededor del mundo más de 100 virus cada semana, y éstos mutan, por lo que la multiplicación y réplica de los virus informáticos es alarmante.

A nivel mundial, México ocupa el tercer lugar en la comisión de delitos cibernéticos. Aquí, de acuerdo a informes publicados por la Policía Cibernética de la Secretaría de Seguridad Pública Federal, el 50% de los delitos cibernéticos tiene que ver con pornografía infantil. El otro 50% está relacionado con fraudes, introducción de virus, usurpación de identidad, robo y alteración de información, pedofilia, pirateo de páginas oficiales, tráfico de menores, terrorismo, sabotaje, así como clonación de señales satelitales y de tarjetas de crédito.

Con respecto a esta incidencia delictiva, la Policía Cibernética en México y según la misma dependencia desarrolla actividades de colaboración e intercambio de información con policías similares en el mundo con actividades como:

- ubicación en el ambiente informático y/o en el uso de computadoras personales,
- comisión de posibles ilícitos,
- rastreo e identificación de redes criminales de sujetos vinculados a la pornografía infantil por *internet*,
- amenazas y hostigamiento vía *e-mails*,
- fraudes asociados al comercio electrónico,
- la piratería informática,
- el robo de señal de compañías televisivas y concesionarios de satélite
- la clonación de señales celulares y de tarjetas de crédito,
- la identificación de posibles ilícitos en la red, que asocien vínculos con crimen organizado
- la identificación de posibles delitos contra la salud, entre otros.

También, la Ciberpolicía mexicana realiza la detección temprana de vulnerabilidades en sistemas, con el objeto de sentar las bases legales de acción en contra de transgresores informáticos y de personas que recurren a la

"ingeniería social"[40] como una actividad de engaño para apropiarse de información confidencial para fines delictivos, así como en la identificación de personalidades expertas en el uso de programas y sistemas que luego de penetrar en sitios privados, perjudican las redes informáticas, particularmente, lo que se refiere a la seguridad nacional y de las Instituciones.

La PFP como Secretaría técnica del Grupo DC México, es la representante nacional ante el Grupo de Coordinación Internacional 24x7 que vigila mundialmente las operaciones en la red y está alerta a incidentes graves dentro de ésta.

El Grupo de Coordinación Internacional 24x7 es un organismo creado en 1998 al interior del G-8 por el subgrupo de Alta Tecnología y de expertos en Crimen Transnacional Organizado. Está conformado por una red de expertos en la investigación de crímenes vinculados con el abuso de las nuevas tecnologías. Dicha red funciona las 24 horas del día, los siete días de la semana con el fin de asegurar que no haya paraísos de impunidad en algún lugar del mundo, para quienes cometen delitos en el ciberespacio**.**

Además, la red permite que las autoridades en distintos países, tengan las capacidades técnicas y legales para encontrar y llevar ante los tribunales, a los delincuentes que abusan de los medios tecnológicos. Opera también con base en una serie de principios que son traducidos en políticas nacionales y reformas legales en cada país.

El Grupo 24X7 permite, que en un máximo de 15 minutos ya se tenga la información preservada, sobre los delincuentes, mientras que se realizan todas las gestiones que las reglas diplomáticas establecen y que pudieran llevar hasta días para actuar.

[40] Ingeniería Social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usa comúnmente el teléfono o internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas.

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. La representación mexicana de este organismo internacional es un grupo conformado por los poderes Legislativo y Ejecutivo Federal; Gobiernos de los estados y del Distrito Federal, organizaciones académicas y proveedores de servicio de la *Internet.*

DC México es un cuerpo colegiado que concentra la información necesaria, que permita la identificación, monitoreo, rastreo y localización de todas aquellas manifestaciones delictivas en *internet,* dentro y fuera de nuestro territorio.

Como instancia de control y apoyado en la participación de las autoridades persecutoras de delitos, DC México se convierte en un canal confiable de enfrentamiento inmediato y con seguimiento de toda denuncia de ilícitos informáticos en México y en el extranjero. También, es el único punto de contacto oficial con sus contrapartes en los Estados Unidos, en términos de los acuerdos bilaterales con esa nación y los que se propicien con otras entidades internacionales. Así, DC México se inscribe en el modelo de seguridad del Sistema Nacional e-México, para constituirse como un observatorio de control y seguimiento de incidencias delictivas.

Sin embargo, DC México tuvo un tropiezo. En 2004 permaneció inactivo durante nueve meses, debido a cambios en su estructura y a la salida de la Policía Federal Preventiva de su creador, Hervé Hurtado, quien fue separado del cargo en marzo de este año, sin que la administración de Alejandro Gertz Manero explicara los motivos.

En noviembre de 2004, la Secretaría de Seguridad Pública federal (SSPF) informó la reactivación de los trabajos del Grupo Interinstitucional de Combate a los Delitos Cibernéticos, "DC México". Ante este anuncio, la embajada de Estados Unidos hizo un reconocimiento a la labor desarrollada por dicha unidad.

En ese entonces, la SSPF señaló que reactivar a DC México demostraba el compromiso de la sociedad por abatir los ataques informáticos ante el creciente surgimiento de cibercriminales.

Representantes de diversas secretarías de Estado, organismos de Procuración de Justicia, empresas prestadoras de servicios, instituciones de Educación Superior, las cámaras de Diputados y Senadores así como de la Suprema Corte de Justicia de la Nación celebraron la primera reunión de esta nueva etapa del DC México.

Otro organismo con el que la Policía Cibernética tiene relación es el Servicio Mundial de Comunicación Policial Protegida de INTERPOL, el I-24/7, que conecta entre sí la Secretaría General, las Oficinas Regionales y las Oficinas Centrales Nacionales de los países miembros, creando una red mundial que permite el intercambio de información y facilita a los organismos encargados de la aplicación de la ley, un acceso instantáneo a las bases de datos y a los servicios de INTERPOL.

Desde 2003, fecha en que INTERPOL puso en marcha su sistema I-24/7, con el propósito de revolucionar el modo en que la policía de todo el mundo intercambia información y lleva a cabo investigaciones internacionales, este sistema ha superado todas las expectativas en términos de utilización y eficacia.

Por su parte, la Universidad Nacional Autónoma de México participa en este grupo con UNAM-CERT, (Equipo de Respuesta a Incidentes de Seguridad en Cómputo) que es una unidad de profesionales en seguridad en cómputo, que se encarga de proveer el servicio de respuesta a incidentes a sitios que han sido víctimas de algún "ataque"[41].

[41] Ataque dirigido a la computadora en el cual el intruso ha iniciado una sesión interactiva, es decir, desde el teclado. También puede tener como objetivo una computadora diferente. Diccionario Casero UNAM-CERT http://www.seguridad.unam.mx/usuario-casero

El UNAM-CERT también publica información sobre vulnerabilidades y alertas de seguridad y realiza investigaciones de la amplia área del cómputo para mejorar la seguridad de los sitios. UNAM- CERT, está localizado en el Departamento de Seguridad en Cómputo (DSC) de la Dirección General de Servicios de Cómputo Académico (DGSCA)[42], de la UNAM.

[42] La Dirección General de Servicios de Cómputo Académico de la UNAM (DGSCA) es la entidad universitaria encargada de la operación de los sistemas centrales de cómputo académico y de las telecomunicaciones de la institución; su esfuerzo más amplio es la capacitación en tecnología de la información, de prospección e innovación y de asimilación de estas tecnologías en beneficio de la Universidad y de la sociedad en general.

3.3 Delitos informáticos

Hay algunas formas de delitos informáticos que atacan a las propias tecnologías de la información y las comunicaciones, éstos incluyen daños a los servicios de telecomunicación y de servicios computacionales, como el robo económico, los ataques de piratería contra bancos o sistemas financieros, o el fraude.

De acuerdo con la información presentada en el 1er Congreso Navega Protegido realizado el 4 y 5 de Octubre de 2006 por el Jefe del Departamento de Delitos Cibernéticos de la Policía Cibernética, en nuestro país los principales delitos cometidos en Internet son:

Principales delitos cometidos en Internet	
Tipo I	Robo de identidad
	Phreaking (mecanismos que vulneran la seguridad de los sistemas telefónicos)
	Amenazas
	Fraudes en e-commerce (portales de subasta)
	Fraudes online (compras en tiendas virtuales)
	Clonación de tarjetas de crédito
	Robo de información
	Carding (utilización ilegal de tarjetas de crédito)
	Traspasos ilegítimos
	Phishing (correos falsos para robar datos del usuario)
Tipo II	Extorsiones, secuestros o localización de objetivos
	Pornografía infantil
	Explotación sexual comercial infantil
	Lenocinio infantil en Internet
	Abuso de menores
	Turismo sexual en Internet
	Robo y substracción de menores
Fuente: Congreso Navega protegido. Policía Cibernética.	

La Policía Cibernética y empresas dedicadas a la seguridad informática como Symantec coinciden en clasificar los delitos cibernéticos, por sus características, en dos tipos:

Delitos cibernéticos Tipo I	
Delito	**Descripción**
Phishing:	Sin duda este es el fraude más común en la actualidad y consiste en obtener información sensible (números de cuenta, contraseñas, etc.) de un usuario bancario mediante el envío de correos falsos, en los que un delincuente se hace pasar por tu banco para engañarte. De acuerdo con la Policía Cibernética en lo que va del año hasta el mes de octubre se han atendido 669 casos de desactivación de sitios phishing.
Pharming	Es un tipo de fraude que cumple el mismo objetivo que el phishing: robo de la información financiera del usuario. Este tipo de delito se realiza cuando una aplicación o programa se instala en tu computadora, una vez instalado cuando deseas entrar a tu banco, a través de un navegador, se reedirecciona a otra predeterminada por el atacante con el mismo diseño y apariencia que el original con el fin de obtener claves, contraseñas y números de cuenta.
Fraude en e-commerce:	Es comercio electrónico que se realiza entre particulares a través de portales de subasta. El riesgo de este tipo de sitios es que la responsabilidad de compra-venta depende de quienes participan en la transacción no del sitio de Internet.
Spyware:	Son programas que pueden ser instalados en la computadora sin tu conocimiento o autorización con la finalidad de registrar información de tus actividades, como por ejemplo: los programas, archivos e información que utilizas
Fuente: Banamex, Symantec y Profeco.	

Delitos cibernéticos Tipo II	
Delito	**Descripción**
Pornografía infantil	Es el material distribuido en Internet con carácter explícitamente sexual en donde cualquier usuario puede erigirse como productor, difusor y receptor del material pornográfico infantil. De acuerdo con la Policía cibernética este tipo de ilícitos ya ha involucrado no sólo niños y niñas de un año en adelante sino que actualmente se manejan bebés de dos o tres meses de edad.
Pedófilia	Son personas que muestran cierta preferencia y/o atracción sexual por personas que son menores de edad. El atacante puede ponerse en contacto con la víctima en una sala de discusión (chat) con la intención de llegar a establecer una relación al cabo de cierto tiempo.
Acoso sexual	El acoso sexual puede ocurrir entre personas del mismo sexo o del opuesto y presenta conductas como: pedir favores sexuales, lenguaje de naturaleza sexual, propuestas o insinuaciones sexuales. Esto puede presentarse de manera frecuente en los chats o en mensajes de correo electrónico.
Turismo sexual infantil	Son grupos u organizaciones que utilizan anuncios a través de Internet con información oculta mediante la cual se promueve "niños de catálogo", es decir niños que son utilizados para brindar servicios sexuales.
Espionaje	Es el acceso no autorizado a sistemas informáticos o la intercepción de correos electrónicos a través de diferentes mecanismos como por ejemplo las

	cookies (archivos que se almacenan en el equipo del usuario) mediante las cuales se puede conocer todo lo que se hace el usuario desde un ordenador y copiar todos los archivos almacenados.
Narcotráfico	Algunos grupos delictivos han utilizado Internet como un medio de comunicación e inclusive de comercialización de diferentes productos y sustancias ilícitas.
Fuente: Policía Cibernética, Profeco, Symantec y www.onnet.es	

En el contexto internacional, la Organización de las Naciones Unidas (ONU) ha reconocido que los delitos por computadora constituyen un grave problema, ya que las leyes, los sistemas de impartición de justicia y la cooperación internacional no se han adecuado a los cambios tecnológicos. La propia Organización instó a los Estados miembros a intensificar sus esfuerzos para combatir este tipo de conductas, entre otras medidas, mediante la creación de procedimientos de investigación para hacer frente a estas nuevas y sofisticadas formas de actividad criminal.

La ONU clasifica los delitos cibernéticos de la siguiente forma:

Tipos de Delitos Informáticos Conocidos por Naciones Unidas	
Delitos	***Características***
Fraudes cometidos mediante manipulación de computadoras	
Manipulación de los datos de entrada	Este tipo de fraude informático conocido también como sustracción de datos, representa el delito Informático mas comun ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
La manipulación de programas	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método comun 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 mas comun es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos 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 computo. 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.

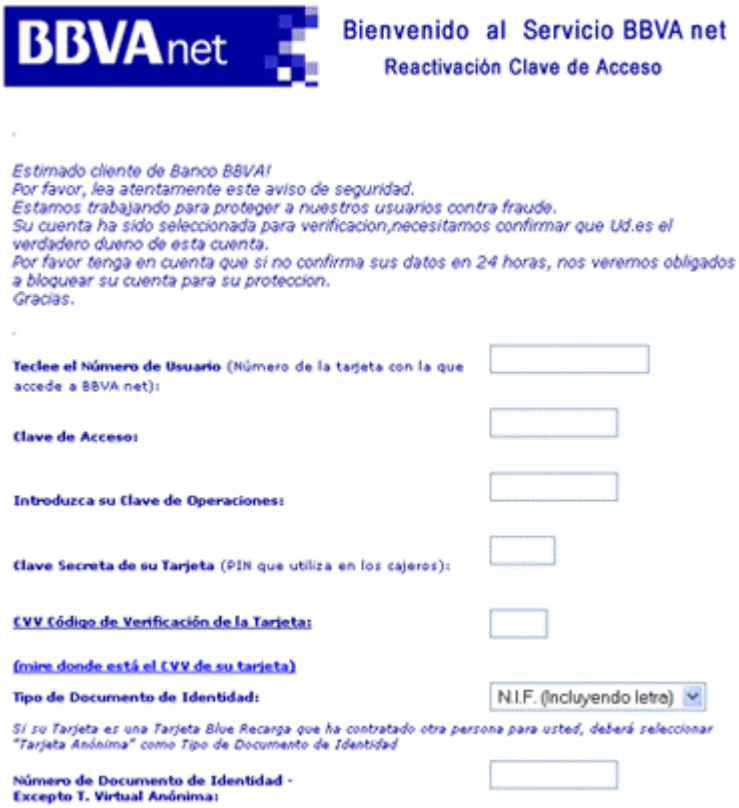
Falsificaciones Informáticas	
Como Objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada
Como instrumentos	Las computadoras pueden utilizarse también pare efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas 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 solo 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 legitima 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 pare 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 se halla la bomba.
Acceso no autorizado a Sistemas o Servicios	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) 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 perdida 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 trafico 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.

Especial atención merece uno de los delitos más comunes en nuestro país y en el mundo, se trata de la “pesca” de información o *phishing*. Son mensajes de correo electrónico que intentan adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, mejor conocido como *phisher* se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, y solicita información personal para cometer fraude. Se ha detectado que los delincuentes logran obtener contraseñas de tarjetas de crédito ofreciendo premios o regalos.

Un claro ejemplo del *phishing* es esta página de un banco, en la que le solicitan al usuario datos confidenciales.



Igual que la basura informática, *Spam,* se distribuyen millones de esos mensajes de correo electrónico fraudulentos; en lugar de solicitar directamente la compra de productos o servicios, los mensajes simulan provenir de bancos, subastas en línea y otros sitios legítimos que pretenden inducir a los usuarios a que respondan proporcionando datos personales o financieros o contraseñas.

Spam son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general, es la basada en el correo electrónico. El *Spam* también puede tener como objetivo, los teléfonos celulares a través de mensajes de texto y los sistemas de mensajería instantánea.

Mensaje de *Spam*

La red se ha utilizado también para otros delitos, como la distribución de propaganda como la xenofobia. En los últimos años, se ha prestado cada vez más atención a la relación entre el terrorismo y la *internet*, aunque también en este caso, hay una gran diversidad de actividades. Se presume que la *net* se utiliza para financiar el terrorismo y como instrumento logístico para planificar y ejecutar actos de ese tipo.

Según el secretario norteamericano de Defensa, Donald Rumsfeld[43], un manual de entrenamiento de Al Qaeda hallado en Afganistán, explica que "es posible reunir al menos el ochenta por ciento de toda la información necesaria sobre el enemigo, mediante el uso de fuentes públicas y sin recurrir a medios ilegales".

Una computadora de Al Qaeda contenía los detalles de la estructura arquitectónica y de ingeniería de una presa, detalles que se habían descargado de *internet* y habrían permitido a los ingenieros y planificadores de Al Qaeda simular

[43] Secretario estadounidense de Defensa del gobierno de Gerald Ford de 1975 a 1977, y de George W. Bush entre 2001 y 2006.

fallas catastróficas. En otra terminal capturada, los investigadores estadounidenses hallaron pruebas de que los técnicos de Al Qaeda al parecer, navegaron por sedes que ofrecían programas e instrucciones de programación de los interruptores digitales que hacen funcionar las redes de energía, agua, transporte y comunicaciones[44].

Los terroristas utilizan la *net* no sólo para aprender a fabricar bombas, sino también para planear y coordinar ataques específicos. Los miembros de Al Qaeda dependían en gran parte de la red para planear y coordinar los ataques a las Torres Gemelas del 11 de septiembre. En la computadora de Abu Zubayda, terrorista de Al Qaeda detenido y del que se dice que habría sido el cerebro de los atentados, los agentes federales encontraron miles de mensajes codificados sacados de una parte de un sede web protegida con una contraseña.

Página de Al Qaeda

También se presta más atención a la función de la *internet* en la difusión de propaganda terrorista y en el uso para el reclutamiento. Esas actividades son distintas del terrorismo *cibernético*, que ha sido definido por el Centro Nacional de

[44] Agencia de noticias AFP 12 mayo 2006.

Protección de la Infraestructura de los Estados Unidos (NIPC)[45] como: "(…)Un acto delictivo perpetrado con el uso de computadoras que resulta en violencia, muerte y/o destrucción, y que crea terror con el propósito de ejercer presión sobre un gobierno para que cambie sus políticas(…)".

A través de su página web, la secta japonesa de la Verdad Suprema (Aum-Shinrikyo) muestra su propaganda terrorista. En 1995, algunos integrantes de la secta realizaron un atentado mortal con gas sarín en el metro de Tokio que costó la vida de 12 personas e intoxicó a otras cinco mil.

Las transferencias bancarias, las operaciones de bolsa y otras transacciones comerciales, son canales importantes que puede ser objeto de ataques por parte de "terroristas tecnológicos" con el fin de causar daños económicos a sectores determinados.

Los grupos extremistas requieren de fondos para mantenerse. Al Qaeda, por ejemplo, siempre ha dependido en gran medida de los donativos y su red global de recaudación se apoya en sociedades benéficas, organizaciones no gubernamentales y otras instituciones financieras que disponen de sedes, salas de charla y foros en *internet.* Los combatientes chechenos también han utilizado *internet* para divulgar las cuentas bancarias en las que sus simpatizantes pueden hacer aportaciones. El Gobierno estadounidense confiscó en diciembre del 2001 los fondos y bienes de una sociedad benéfica con sede en Texas a causa de sus vínculos con Hamas.

La planificación de ataques, y la comunicación entre miembros de células terroristas se ha vuelto tan sencilla que puede establecerse desde cualquier *cibercafé* vía correo electrónico o en vivo vía *chat.* Las organizaciones terroristas reúnen información sobre los usuarios que navegan por sus sedes, luego

[45] (NIPC) Creada en 1998 con el fin de detectar, dar la alarma, responder e investigar intrusiones en computadoras. http://usinfo.state.gov/journals/itps/1101/ijps/pj63fbi.htm (consulta 6/09/2006)

contactan a aquellos visitantes que parecen más interesados en la organización o más apropiados para trabajar en ella.

La propaganda de los grupos catalogados como terroristas se ha hecho común en *internet* como Sendero Luminoso, ETA y Hezbollah. Los grupos armados como El Ejército de Liberación Nacional colombiano (ELN), las Fuerzas Armadas Revolucionarias de Colombia (FARC) y el Ejército Zapatista de Liberación Nacional (EZLN) también tienen presencia en la *web* lo que hace evidente la utilización de tecnología por parte de estos grupos. Hay otras organizaciones que hacen propaganda a través de Internet; este es el caso del Ku Klux Klan.

3.4 Informática Forense vs. *Ciberterrorismo*

El valor de la información en nuestra sociedad, es cada vez más importante. Así como los delincuentes utilizan la red para cometer ilícitos, los métodos para encontrar a los culpables también han cambiado y ya se cuenta con modernos sistemas de cómputo que analizan y detectan las pistas para encontrar a los delincuentes. Derivado de este aspecto, adquiere cada vez mayor trascendencia la Informática Forense, sus usos y objetivos. ¿En qué consiste esta ciencia relativamente reciente?

La informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en una computadora. Incluye la recolección segura de datos de diferentes medios digitales y evidencias digitales, sin alterar los datos de origen. Cada fuente de información se cataloga, preparándola para su posterior análisis y se documenta cada prueba aportada. Las evidencias digitales recabadas permiten elaborar un dictamen claro, conciso, fundamentado y con justificación.

El jefe del Departamento de Seguridad en Cómputo de la Dirección General de Servicios de Cómputo Académico y Coordinador del Equipo de Respuesta a Incidentes en Seguridad en Cómputo UNAM-CERT, Juan Carlos Guel, señala que "(…) informática o cómputo forense es un conjunto de técnicas especializadas que tiene como finalidad la reconstrucción de hechos pasados basados en los datos recolectados, para lo cual se procesa la información que pueda ser usada como evidencia en un equipo de cómputo (…)".

"(…) A través de diferentes aplicaciones en cómputo, explica, podemos determinar cómo fue violentado un sistema, la manera en que fue traspasada su seguridad, y una vez que los intrusos estuvieron dentro, determinar con técnicas sumamente sofisticadas, qué fue lo que hicieron y cuáles fueron los archivos que borraron, así como las modificaciones que realizaron, mientras se precisa la duración del ataque, desde la entrada hasta la salida (…)".

Los intrusos se valen de trucos para evitar ser descubiertos cuando se aplican las técnicas forenses por eso, explica el especialista de la UNAM, en el momento en que se detecta una intromisión, se debe actuar con sumo cuidado, pues existe el peligro de que al momento de analizar el sistema se active una "bomba de tiempo" que detone el sistema y ponga al descubierto al informático forense ante el infractor[46].

Quienes van a requerir de esta disciplina van a ser las fuerzas policíacas y los abogados para poder realizar los peritajes de sus clientes, así como las agencias federales. Pero no nada mas el cómputo forense se realiza de manera judicial o pericial para presentarlo ante la ley. El cómputo forense también puede ser utilizado como instrumento dentro de las empresas para determinar si alguien está realizando un fraude, ha robado información o secretos industriales, es decir, para demostrar qué pasó en la computadora o infraestructura de cómputo.

De acuerdo con estadísticas de la Policía Federal Preventiva, en México se han realizado fraudes por cerca de mil 380 millones de pesos en un año por medio de la *internet*,

Pero el cómputo forense no sólo se realiza a computadoras; en los últimos años en nuestro país, se ha incrementado la difamación a través de correo electrónico, el cual es rastreable por medio de esta disciplina.

Algo que ha empezado a cambiar dentro del mundo de la tecnología son las empresas aseguradoras, que ya cuentan con seguros para la protección de información o los famosos Seguros Contra Hackers.

Pero, si en un proceso legal, el cómputo forense puede ser utilizado como peritaje para brindar evidencia acerca de acciones que se encontraron dentro de una computadora, entonces, ¿por qué hay tan poca información acerca de esta

[46] http://www.enterate.unam.mx/Articulos/2004/octubre/forense.htm (consulta 29/11/2006)

disciplina? La respuesta es sencilla, para que esto se lleve a cabo, es necesario tener un marco legal que lo soporte de una mejor manera. En este momento, México cuenta con muy poca legislación al respecto y se puede identificar y aceptar medios electrónicos como pruebas dentro de una denuncia, pero muchas veces la tipificación directa de un delito informático no se encuentra.

Otro delito que crece cada día más es el narcotráfico vía *internet*, se trata de la transmisión de fórmulas para la fabricación de estupefacientes, el blanqueo de dinero y para la coordinación de entregas y recogidas de la droga. En este caso, la luz de alerta está encendida y surge la necesidad de implementar medidas que permitan interceptar y descifrar los mensajes encriptados[47] que utilizan los narcotraficantes para ponerse en contacto con los cárteles. Las mismas ventajas que encuentran en la *internet* los narcotraficantes, pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas.

Según un informe publicado el 10 de mayo de 2006 por Amnistía Internacional y TransArms[48], es urgente reforzar las medidas, totalmente ineficaces y anticuadas de control de las armas, para impedir que la creciente red de intermediarios, empresas logísticas y transportistas que intervienen en el comercio de armas agrave los abusos masivos contra los derechos humanos en el mundo.

El informe muestra que por medio de operaciones cada vez más complejas de corretaje y transporte, se expiden ya centenares de miles de toneladas de armas en el mundo, un porcentaje creciente de las cuales van a parar a países en desarrollo, donde fomentan algunos de los conflictos más brutales que existen.

---

[47] La criptografía (del griego *kryptos*, «ocultar», y *graphos*, «escribir», literalmente «escritura oculta») es la ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos. Los mensajes encriptados son mensajes que se envían codificados, es decir, con claves secretas que sólo el receptor puede descifrar.

[48] Amnistía Internacional es la organización defensora de derechos humanos más grande del mundo. Tiene más de 2.2 millones de integrantes en alrededor de 150 países y territorios que forman un frente común para luchar por el respeto a los derechos humanos. TransArms es un pequeño grupo independiente de investigación, centrado en la logística del comercio internacional de armas.

El documento señala que en México, los márgenes de ganancias netas de las organizaciones criminales llegan a 550 % y destaca también diversos casos en los que se han concertado los servicios de contratistas privados implicados en envíos ilegales de armas para apoyar misiones de mantenimiento de paz de la ONU y envíos de ayuda humanitaria a costa de los contribuyentes.

Por otra parte, preocupa a toda la comunidad internacional el problema de la pornografía infantil. Aunque este tipo de pornografía ha existido durante muchos años (en forma de fotografías, revistas, películas y vídeos), desde finales de la década de los ochenta, ha habido una tendencia creciente a distribuir pornografía infantil mediante una diversidad de redes de computadoras, usando variados servicios de *internet*.

Estas redes se han utilizado para facilitar intercambios de información, comerciar con imágenes o videos de pornografía con niños, realizar transacciones monetarias y trasmitir información con respecto al turismo sexual de este sector poblacional. Sólo una parte de la distribución de este tipo de pornografía, tiene fines comerciales, más que de intercambio no monetario entre pedófilos, y está vinculada a la delincuencia organizada transnacional.

Lamentablemente, el problema se agrava con la aparición de nuevas tecnologías, como la criptografía, que sirve para ocultar pornografía y otros materiales ofensivos. Se estima que mediante este medio en todo el mundo la explotación sexual infantil permite que más de dos millones de niños y niñas sean tratados como mercancías.

Según datos de la Policía Cibernética, en cinco años se detectaron más de cuatro mil páginas de pornografía infantil en *internet* en nuestro país. Desde España, se ha dejado al descubierto que las redes de pederastia que operan allí, tienen conexión con países latinoamericanos como México, Argentina, Chile, Costa Rica, Panamá, República Dominicana y Uruguay, realizando un operativo policial que reflejó 900 conexiones de las cuales 200 son de México.

En marzo de 2007, la organización Ecpat Internacional[49], presentó el "Informe Global de Monitoreo de las Acciones en Contra de la Explotación Sexual Comercial de Niños, Niñas y Adolescentes" en el que señala que México es considerado el segundo país en el mundo con mayor producción de pornografía infantil, pero la tenencia o posesión de material pornográfico infantil no esta sancionada por las leyes.

Pese a las evidencias que proporcionan las denuncias, los reportes periodísticos, los informes y estudios, "no se puede actuar con contundencia jurídica", asegura el informe, ya que aún existen grandes vacíos legales para identificar y sancionar delitos cibernéticos y delitos asociados, como la distribución de material pornográfico.

La impunidad "contribuye al incremento de la oferta de material pornográfico infantil, y a que su venta se vuelva abierta y pública, como ocurre en Tepito y La Merced, en la Ciudad de México", considera Ecpat Internacional.

Según las estadísticas de la Policía Federal Preventiva (PFP), cita el organismo, la explotación sexual de menores de edad a través de internet se incrementa aceleradamente por lo que ya ocupa el tercer lugar en la lista de delitos cibernéticos, después de los fraudes y las amenazas.

Tan sólo en enero de 2004, se registraron 72 mil 100 sitios de pornografía sexual de menores de edad, mientras que a inicios del 2006 ya había más de 100 mil sitios. De acuerdo con el texto, hasta el año 2003 la Policía Cibernética de México tenía la clasificación de imágenes de pornografía infantil en *internet* en cuatro rangos: de cero a cuatro años, de cuatro a ocho, de ocho a doce y de doce a diecisiete, grupo en el que predominaban las imágenes pornográficas.

[49] ECPAT es una red de organizaciones y individuales que trabajan en conjunto para la eliminación de la prostitución infantil, la pornografía infantil y el tráfico de niños (as) con propósitos sexuales. Se dedica ha motivar a la comunidad mundial a asegurar que la niñez en todas partes disfrute de sus derechos fundamentales libres y seguros de todas las formas de explotación sexual comercial. Posee Estatus Consultivo ante el Consejo Económico y Social de las Naciones Unidas (ECOSOC).

Sin embargo, en el primer cuatrimestre del 2004 se creó un nuevo rango como consecuencia del visible aumento en la detección de imágenes de pornografía con bebés, por lo que la nueva categoría comprende a niñas y niños de cero a un año de edad, ya que se registró un incremento del 5 por ciento en fotografías e imágenes de abuso de recién nacidos, subraya el informe.

Hace diez años, en 1996 México participó en el Primer Congreso sobre Explotación Sexual Comercial de Niñas, Niños y Adolescentes (ESCNNA) realizado en Estocolmo, Suecia y suscribió la Declaración y Agenda para la Acción, compromiso que ratificó durante el Segundo Congreso Mundial contra la ESCNNA, realizado en Yokohama, Japón en el 2001, subraya el Informe Ecpat Internacional.

Como consecuencia, surgió el Plan Nacional de Acción para Prevenir, Atender y Erradicar la Explotación Sexual Comercial Infantil. No obstante, dicho instrumento no está sustentado jurídicamente por lo que depende de la voluntad del gobierno en turno dar continuidad a su realización, señala el monitoreo.

Desgraciadamente, destaca el documento, la Coordinación Nacional para Prevenir, atender y Erradicar la Explotación Sexual Comercial Infantil, creada en 2002, no cuenta con los mecanismos y recursos económicos necesarios para permitir la implementación del Plan y mantener la continuidad de sus programas, ni para articular los sectores públicos, social y privado para enfrentar la explotación sexual de manera efectiva.

De acuerdo con el profesor-investigador del Instituto Nacional de Ciencias Penales (INACIPE), Erick Gómez Tagle López, en México hay cerca de 20 mil menores de edad que son víctimas de explotación sexual, de los cuales cinco mil se localizan en el Distrito Federal.

Al intervenir en el Foro sobre trata de personas y explotación sexual infantil organizado por la Facultad de Ciencias Políticas y Sociales de la UNAM, donde participó en la mesa ¿Turismo sexual infantil en México?, el especialista señaló que el país ocupa el lugar 28 en el mundo y el quinto en América Latina con mayor comercio sexual infantil, solamente detrás de Brasil, Colombia, Guatemala y República Dominicana.

Consideró que a pesar de la creación de la Policía Cibernética en México la cual, dijo, ha dado buenos resultados, los delincuentes y las redes de pedófilos y pederastas en el mundo ya no están encubiertos, “lo hacen a todas luces, a través de sitios web, boletines, revistas y estaciones de radio en diferentes partes del mundo”. Incluso, en Holanda, algunas de estas organizaciones pretenden crear un partido político, “que propugne por la legalización de la pederastia, el sexo con animales y las drogas blandas y duras”, entre otros aspectos, precisó.

Durante el evento, que se llevó a cabo en abril de 2007, expuso que según una encuesta realizada por Microsoft a cuatro millones de personas menores de 18 años, el 30 por ciento proporciona sus datos personales a desconocidos, por lo que es necesario hablar abiertamente del tema con los pequeños, para prevenir que se conviertan en víctimas. De acuerdo con esta empresa, “cada minuto hay 50 mil depredadores sexuales en la red”, agregó.

Tan sólo en Estados Unidos, explicó, los casos de menores víctimas de comercio sexual infantil llegan a 250 mil, mientras que en la India son 400 mil. Cabe recordar que Norteamérica es una de las mayores generadoras de turismo sexual en el mundo, y es una de las grandes productoras de pornografía, infantil o adulta.

El profesor Gómez Tagle López denunció que se estima que en todo el mundo entre uno y dos millones de infantes son incorporados anualmente a este mercado.

De acuerdo con datos de CIMAC,[50] el Sistema Nacional para el Desarrollo Integral de la Familia (DIF), señala que hay 17 mil niños y niñas explotados por el comercio sexual infantil, existiendo un tráfico de infantes entre México y Estados Unidos de 260 mil menores utilizados para el sexo servicio. Esta es una de las causas de la desaparición de niños en nuestro país.

El Instituto Nacional de Migración (INM), acepta que en el país operan 100 bandas dedicadas al tráfico de personas y 10 de ellas están especializadas al tráfico y trata de menores.

La Policía Cibernética 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. Se estima que quinientos sitios Web de este tipo son creados diariamente, asegura "Roberto"[51]

Las estimaciones de 7 mil millones de dólares de ganancias por el tráfico y explotación de menores demuestran que se habla de un fenómeno grande y en crecimiento. Si bien, se debe reconocer la tarea inicial de la Policía Cibernética que tiene un área para las investigaciones sobre los delitos contra menores, con una base de datos nacional y con investigaciones sobre patrones, rangos, preferencias y *modus operandi* de los delincuentes en México, este nauseabundo comercio requiere de una mayor voluntad política que permita una efectiva coordinación de recursos.

[50] Comunicación e Información de la Mujer, A.C. (CIMAC) es una institución multimedia que desde 1988 promueve en los medios de comunicación un nuevo punto de vista sobre la condición actual de las mujeres en México y el mundo.
[51] "Roberto" es un elemento de la Policía Cibernética, por razones de seguridad no se da su nombre real.

3.5 Vigías de la Red, el Patrullaje

¿Cómo realiza su patrullaje el investigador?, por ejemplo, al recibir una denuncia anónima o una denuncia formal de un padre de familia, de un vecino, de una ONG, de una autoridad estatal, municipal, federal, el policía cibernético la presenta ante el Ministerio Público (MP). Luego, se recaba toda la información que, con el tiempo debido, se convierte en acciones. Posteriormente, el MP pide por oficio una serie de datos que van a servir para ejercer la acción penal contra los posibles autores del ilícito, (fraude, prostitución u otros) que estén utilizando la red para promover pornografía.

A veces, los delincuentes cibernéticos logran escapar aún cuando existen elementos sólidos para encerrarlos, reconoce “Roberto”, “hemos llegado casi al final de procesos importantes con pederastas y no podemos alcanzar la meta porque el denunciante no coopera, ya no quiere continuar con el proceso”. Si ya no hay víctima, ya no hay quien señale a los delincuentes. “Roberto” explica que sostener la denuncia contra viento y marea es muy importante para castigar a los infractores.

Hay que hacer entender a las víctimas que es necesario que sigan hasta el final y agrega que, para ello, se requiere un proceso de educación que fomente la cultura de la seguridad[52]. Ese, puntualiza, es una de los objetivos de la PFP con su política de prevención del delito, en la que la denuncia anónima es una parte importante. El sitio de la Policía Cibernética cuenta con una sección destinada a recibir las denuncia anónimas. Entre las funciones de la oficina de la Policía Cibernética y Delitos contra Menores, están: promover esa cultura de la seguridad, fomentar la denuncia anónima y realizar campañas de información sobre los delitos cibernéticos.

[52] La cultura de la seguridad en internet consiste en que los usuarios sepan cómo utilizar internet y saber distinguir cuando exista un posible riesgo. Se trata de saber proteger los equipos, su información personal, así como a la familia de contenidos, mensajes y aproximaciones personales que sean considerados como riesgos de integridad física e los usuarios, principalmente en los niños. AMIPCI (Asociación Mexicana de Internet)

A su vez, “Eduardo” señala que, a pesar de las dificultades, su trabajo, “el punto fino de nuestra chamba, es encontrar elementos sólidos para poder encerrar a los delincuentes cibernéticos; y lo logramos, al fin y al cabo, lo hacemos”.

En uno de los casos destacados, en septiembre de 2000, la Policía Cibernética identificó y desarticuló la organización de abuso sexual a niños más extendida de México, que operaba desde Acapulco. Se expulsó del país a Robert Decker, ciudadano estadounidense que, según las evidencias, dirigía dicha organización. En el caso de Decker, la Policía Cibernética colaboró con autoridades policiales de Estados Unidos, lo que revela la importancia de la cooperación internacional para perseguir esta clase de delitos.

Según estimaciones de UNICEF[53], dos millones de niños y niñas son objeto cada año de explotación sexual con fines comerciales y 0,6% de los viajeros emprende su periplo con el fin de mantener relaciones sexuales con menores en países generalmente más pobres. El mismo organismo estima que en México son prostituidos 16,000 niños. Acapulco es considerado uno de los focos más importantes.

A nivel mundial la situación es preocupante. Tan sólo en un operativo se llevaron a cabo más de 1,200 arrestos en todo el mundo en un caso masivo de pornografía infantil: En lo que se cree que es la mayor investigación sobre pornografía infantil por *internet* y la primera vez que el gobierno de Estados Unidos se ha concentrado en el aspecto financiero de la pornografía infantil por la red, agentes del ICE[54] detuvieron a 237 personas en Estados Unidos y han proporcionado información a policías en el extranjero que ha llevado a la detención de más de 1,000 personas. Los arrestos en Australia, Canadá, China, Dinamarca, Finlandia, Japón,

[53] Estudio "Infancia Robada", dado a conocer el 3 de marzo de 2006 por Yoriko Yasukawa, representante de UNICEF en México.

[54] El Servicio de Inmigración y Control de Aduanas de Estados Unidos (U.S. Immigration and Customs Enforcement o ICE), creado en marzo de 2003, es la mayor entidad investigadora del Departamento de Seguridad Nacional (Department of Homeland Security o DHS), el cual fue creado tras el 11 de septiembre de 2001 para combinar las dependencias de la ley del antiguo Servicio de Inmigración y Naturalización (Immigration and Naturalization Service o INS) y el antiguo Servicio de Aduanas de Estados Unidos (U.S. Customs Service)

Liechtenstein, Holanda, Nueva Zelanda, Noruega, Suecia, Suiza y el Reino Unido son parte de una investigación en curso de Regpay, una empresa de cobros por *internet* en Minsk, Belarusia.

Capítulo IV
HISTORIAS DE ÉXITO

4.1 Piltzin (Niño Querido)

2003 fue un año importante en lo que se refiere a aprehensiones de pederastas, lo que dejó una gran satisfacción para las naciones involucradas. El 4 de abril en Acapulco, Guerrero, se llevó a cabo el operativo “Piltzin”, en el que se aseguró a 17 pedófilos, tres canadienses, tres mexicanos y once estadounidenses, uno de ellos detenido en flagrancia cuando abusaba de un menor.

Los detenidos fueron puestos a disposición del Ministerio Público, fincándoles los delitos de pornografía infantil, prostitución y corrupción de menores. Se recuperaron 10 niñas, en igual número de domicilios en los que se encontró material pornográfico infantil, diversos artículos como juguetes para regalar a los pequeños, cuadernos con claves utilizadas por los infantes para comunicarse, además de juguetes utilizados para abusar sexualmente de ellos.

El Operativo Pilztin -niño querido en Náhuatl-, permitió la captura de los estadounidenses Philip Marthen de 62 años; David Rusell Wold de 53; Raymon Allen de 57; Irving Harmontz de 69; Denis Hoffman de 65; Phill Setchfield de 50 años; James Kerr de 58; Douglas E. Walle de 64 y Robert Teerin de 53 años de edad.

De igual manera, fueron detenidos los canadienses Ronald Farell de 72 años; Claude Noel de 59 y Hillary Legere de 67, además de los mexicanos Felipe Marín Ortega de 22; Javier Gardo de 55; Federico de la Aldea González de 48; Frank Biller de 50 y Rafferson Edris de 50 años de edad.

Dos días después, la PFP detuvo al norteamericano Keith Minton de 46 años de edad, quien reside en un suburbio de Meridan, en Washington D. C. y lo

puso a disposición de las autoridades ministeriales al quedar plenamente acreditado que éste, valiéndose de engaños, abusaba sexualmente de niños bajo el ofrecimiento de juguetes y golosinas.

De acuerdo con la información de la Policía Cibernética, el presunto pederasta viajó como turista al puerto de Acapulco, Guerrero, estableciéndose en un edificio de apartamentos de la calle Constitución, en la colonia La Mira. Su detención se produjo después de que éste fue denunciado por un menor de once años de edad, quien incluso tuvo que morderlo para escapar de él y ponerse a salvo.

El norteamericano fue detenido a las afueras del inmueble en compañía de otro menor de 13 años de edad, y al ahondar en las investigaciones, con apoyo de la Procuraduría General de Justicia del estado de Guerrero, pudo establecerse que éste se valía de muñecas, carritos de control remoto y otros juguetes para atraer a sus víctimas. Entre sus pertenencias, a Keith Minton se le encontraron películas en video, revistas pornográficas y otro material que fue analizado por las autoridades.

Por otra parte, el mexicano José Guadalupe Borja Borbón de 55 años, fue asegurado y puesto a disposición de las autoridades de Guerrero. Utilizaba una supuesta casa franciscana de asistencia para niños desamparados y quien enfrenta varias denuncias por abuso sexual en agravio de menores.

Por este operativo, el gobierno de Estados Unidos reconoció el esfuerzo de México en materia de combate cibernético mediante la Policía Cibernética de la Policía Federal Preventiva y entregó un reconocimiento a un ciberpolicía mexicano que contribuyó a la captura de los pedófilos.

Bárbara Singh y Dale Edwars, representantes de los departamentos de Migración y Aduanas de Estados Unidos, reconocieron el trabajo de la Policía

Cibernética e informaron que el suboficial Aarón Pereyra Navarrete recibió de la oficina del procurador norteamericano de Justicia, un premio en la categoría de Contribuciones Excelentes, acto que se llevó a cabo en el anfiteatro del Centro de Comercio Exterior Internacional Ronald Reagan, en Washington, DC.

4.2 Hallazgos

Gracias a la cooperación nacional e internacional, de diversos organismos, se ha podido avanzar en la identificación de *modus operandi*, localización y ubicación física de objetivos tanto nacionales como extranjeros. Asimismo, se han obtenido los datos específicos de personas que cometen delitos por la *internet*, así como la ubicación física del equipo de cómputo desde el cual se delinque.

Aunque algunos delitos no se llevan a cabo vía *internet,* en su patrullaje la Policía Cibernética ha conocido de la desaparición de menores y ha cooperado para su recuperación.

El 7 de julio del 2001, en colaboración con la ONG, Asociación Pro-recuperación de Niños Extraviados AC, (APRENEM), se logró recuperar a tres menores robados, dos de quince años y uno de catorce años de edad en Celaya, Guanajuato, donde fue puesta a disposición del Ministerio Público la presunta tratante de menores quien los prostituía. En la comparecencia, las niñas, acompañadas de sus padres, testificaron que fueron abusadas sexualmente.

Casi dos meses después, el 30 de julio, en San Luis Potosí, fue detenido un sujeto que trasladaba a dos menores de doce y trece años de edad. Las pequeñas manifestaron que sus padres las habían vendido a otro sujeto que se encontraba en Sabinas, Coahuila, lugar donde las llevaron y las obligaron a prostituirse; allí, únicamente les daban un alimento al día y cuando las castigaban, ninguno.

En Valle de Chalco, Estado de México, se recuperó a un menor sustraído en el Distrito Federal el 23 de septiembre del 2001. Unos días después se recibió una petición de ayuda para la localización de un adolescente de 16 años quien había desaparecido. Mediante una búsqueda inmediata y entrevistas con familiares y amistades del primer círculo, se pudo establecer en 24 horas, que el

menor solicitó hospedaje en un convento, cercano a Cuernavaca, Morelos; después de su recuperación fue entregado a sus padres.

En mayo del 2001, en el Distrito Federal, se detuvo a una pareja México-norteamericana que pretendía hacer pasar por suyo un bebé al que le habían comprado un acta de nacimiento falsa.

En el estado de Aguascalientes, se puso a disposición del Instituto Nacional de Migración (INM) a un matrimonio México-norteamericano, que llevaba a un grupo de ocho niños de tres familias diferentes; estas personas afirmaron que los padres de éstos les pidieron llevarlos a los Estados Unidos.

Durante los operativos llevados a cabo en el mes de agosto de 2001 en el Estado de México, se intervinieron cuatro giros negros donde se rescató a once menores que estaban siendo forzados a prostituirse. Al año siguiente, en 2002, continuaron los operativos, esta vez, conjuntamente con autoridades de los Estados Unidos, el Servicio de Inmigración y Naturalización (INS), ahora ICE (Immigration and Customs Enforcement) y el (FBI), en Tijuana, Baja California, y Naucalpan, Estado de México, se llevó a cabo un operativo en el que se logró detener a tres traficantes internacionales de niños. En la acción, se recuperaron cinco menores que pretendían ser llevados a Tijuana, para después entregarlos en San Diego, California, a otra traficante que fue detenida, junto con tres adultos y dos menores indocumentados.

Con información recabada por la Policía Federal Preventiva (PFP), los gobiernos de Guatemala y El Salvador, en colaboración con el INS de Estados Unidos, realizaron operativos contra esta organización de traficantes. En esta acción, que se realizó el 5 de Abril del 2002, se detuvo a seis de sus principales dirigentes, doce operadores y cuatro autobuses con 49 menores de edad, que iban a ser llevados a los Estados Unidos, vía México. Los cabecillas fueron interceptados en la frontera de Guatemala con San Cristóbal, El Salvador.

El 27 de julio del 2002, en el estado de Jalisco, dos estadounidenses y dos mexicanos fueron detenidos acusados de corrupción de menores y pornografía infantil. Les fueron aseguradas más de 21 mil imágenes de pornografía infantil y de adolescentes. Los pedófilos tenían dos páginas de *internet* (chicomex.com y wetbackmanor.com) donde subían las imágenes de los menores.

Acapulco, Guerrero también ha sido un destino atractivo para este tipo de actividades ilícitas; muy conocidos en el puerto son los condominios de pedófilos, o los centros para niños desamparados como “La Esperanza” que se convirtió en la sede de una sórdida empresa ilegal que reclutaba a niños de la calle y que las ONG´s han denunciado.

Un sujeto identificado como “Chilaquil O’Neil”, fue puesto a disposición del Ministerio Publico el 4 de junio, en el Distrito Federal. Chilaquil O’Neil distribuía grandes cantidades de imágenes de pornografía infantil en *cd’s* que promovía en la *internet*.

También en la ciudad de México, se detuvieron dos mujeres, por falsificación de documentos y tráfico de menores. En esta acción, realizada el 27 de junio, fueron recuperados tres infantes.

El año 2004 es considerado como uno de los periodos más fructíferos en la labor de la Policía Cibernética. En enero, con información de la Policía Federal Preventiva, en Estados Unidos, el Departamento de Seguridad Nacional (DHS) logró la detención de cuatro lenones y traficantes de menores. Cinco adolescentes fueron rescatados. Un mes después, en el estado de Tlaxcala, se detuvo a tres miembros de esta misma organización.

Esta acción se llevó a cabo luego de un patrullaje en lugares que son frecuentados por personas que distribuyen pornografía infantil o la fomentan con mensajes en sitios, comunidades o portales. Los policías se hicieron pasar por

menores de edad, o por adultos que buscan pornografía, de esta forma se tuvo contacto con los delincuentes.

Ese mismo año, en la ciudad de México, se recuperaron a dos menores de edad, originarias de San Juan del Río, Querétaro.

A finales de 2004, la Policía Cibernética dio apoyo a un Ministerio Público del estado de Aguascalientes, para realizar el análisis forense de cómputo a un disco duro, propiedad de un acusado de delito sexual contra una menor de edad; se trataba de su propia hija.

En Cancún, Quintana Roo, no sólo la periodista Lydia Cacho ha sido amenazada y demandada por calumnias por haber puesto al descubierto las redes que abusan de niños y niñas, sino también la vida y libertad de las víctimas de los pederastas corren ese riesgo.

De acuerdo con información de CIMAC[55], Edith Escalada[56] denunció el abuso sexual que sufrió por parte de Jean Succar Kuri desde niña, hoy cuenta con 21 años y ha sido presionada por personas cercanas a su agresor, al grado de que se retractó de todas sus acusaciones ante notario en Estados Unidos, fuera del marco jurídico mexicano, incluso, fue internada en un centro siquiátrico en California.

Cabe destacar que la periodista Lydia Cacho causó revuelo luego de publicar su libro “Los Demonios del Edén”. Los resultados de su denuncia revelaron la ilegalidad, el tráfico de influencias y la impunidad que priva en nuestro país.

[55] Comunicación e Información de la Mujer, A.C. (CIMAC)

[56] Joven que a los 17 años decidió denunciar por primera vez al presunto pederasta Jean Succar Kuri, quien abusó sexualmente de ella cuando tenía 13 años de edad

4.3 Caso Decuir

Con la intervención de la Unidad Especial de Policía Cibernética y Delitos Contra Menores de la PFP, se logró la localización, ubicación y aprehensión de José Luis Morales Decuir, por su presunta responsabilidad en el homicidio de Gildardo Herrera Zamora, cometido durante el 2003 en el estado de Veracruz.

José Luis Morales Decuir, acude a la casa de su ex esposa e inicia una discusión con su ex suegro. Morales Decuir saca un arma blanca y agrede a Gildardo Herrera Zamora (padre de su ex esposa) causándole heridas que le provocan la muerte. Se da inicio a la indagatoria 313/2003, por el delito de homicidio calificado.

El 13 de octubre de ese mismo año, se recibe un oficio de colaboración del entonces Procurador de Justicia del estado de Veracruz, quien solicita el apoyo para la ubicación, localización y aprehensión de José Luis Morales Decuir.

Producto de intensas labores de inteligencia, fue posible ubicar 51 correos electrónicos en los que el presunto homicida se comunicaba con su ex esposa. El origen de estos mensajes fue en los Estados Unidos, por lo que se solicitó el apoyo de la División de Policía Cibernética del Servicio de Aduanas, a fin de coadyuvar en la búsqueda y localización de Morales Decuir.

Cronología de hechos

El presunto homicida huye hacia los Estados Unidos; sin embargo, se tiene la certeza de que mantiene comunicación con su ex esposa, mediante correo electrónico y "*messenger*", por lo que personal de la Policía Cibernética establece contacto con el inculpado, a través de un elemento que simulaba ser su ex esposa.

En la tercera conversación, se logró obtener diversas fotografías de Morales Decuir, así como su ubicación y número telefónico donde se encontraba oculto.

La información fue facilitada al contacto en el Departamento de Aduanas de los EUA, con el fin de que lo rastrearan. Dicha instancia ubica y detiene a José Luis Morales en un rancho en las inmediaciones de Chicago, Illinois y el Paso Texas, es deportado a México y puesto a disposición de Interpol.

En diciembre de 2005, José Luis Morales Decuir, es sentenciado a 15 años de prisión, por homicidio calificado.

El Gobierno de los Estados Unidos, envió un documento de felicitación a la Unidad Especial de Policía Cibernética mexicana, por la buena colaboración en este caso, el cual es considerado como el primero, a nivel mundial, en que se logra la detención del inculpado gracias al intercambio de información entre Policías Cibernéticas de distintos países.

Este cuerpo policial ha aprendido a sortear parte de los obstáculos con los que se topa en sus investigaciones. Uno de éstos es la falta de colaboración de proveedores de *internet* como la empresa Uninet (filial de Telmex), que en un caso sostuvo como argumento que la PFP no contaba con facultades legales para obligarla a revelar los datos de sus clientes.

4.4 Resultados significativos

- Se han recuperado 105 menores de edad
- 67 personas se han puesto a disposición de las autoridades correspondientes
- Con la asesoría de la PFP, fueron creadas unidades de Policía Cibernética en los estados de Jalisco, Yucatán, Baja California, Nuevo León, Guerrero y el Distrito Federal.

Diagnóstico de la Explotación Sexual Comercial Infantil situación en México:

- Más de 16 mil niños y niñas han padecido explotación sexual.
- Se estima que en el Distrito Federal, cinco mil menores están involucrados en la prostitución Infantil.
- El 80 por ciento de menores que han padecido este delito son niñas entre 10 y 14 años.
- El 90 por ciento de los niños en situación de calle, son víctimas de abuso sexual.
- En 21 de las 32 entidades de la República Mexicana, se han registrado este tipo de delitos. Destacan las ciudades de México, Tijuana, Ciudad Juárez, Guadalajara, Acapulco, Tapachula y Cancún.

Ante un caso de delito cibernético puede llamar a la policía cibernética al 01800PFPGUIA o al 01 800 440 3690 o bien al correo electrónico denuncia@ssp.gob.mx y en el estado de Jalisco al 01 333 668 7900 ext. 18041 o al correo policiacibernetica@jalisco.gob.mx.

Cuando reciba un correo phishing puede reenviarlo a la Comisión Nacional para la Protección y Defensa de los usuarios de Servicios Financieros Condusef al alertasphishing@condusef.gob.mx para que tenga conocimiento y a su vez notifique al público usuario, a las autoridades, organizaciones e instituciones que tengan que ver en el caso.

Por su parte, la privacidad y la protección de los datos personales en *internet* está regulada por el artículo 76 bis de la Ley Federal de Protección al Consumidor, la cual obliga a los sitios a mantener la confidencialidad de la información y les

prohíbe difundirla o transmitirla a menos que el consumidor lo autorice por escrito. Si algún sitio no respetó su política de privacidad al compartir sus datos con otras empresas, denúncielo al Teléfono del Consumidor al 01 800 468 8722 o en la delegación Profeco más cercana.

CONCLUSIONES

Seguramente, las generaciones que hoy son adultas jamás se imaginaron tener a tan sólo un click, la posibilidad de adquirir algún bien o servicio, conversar con otras personas o acceder a información de una manera tan sencilla, lo cierto es que para este grupo de población y los más jóvenes no es posible imaginar el mundo sin *internet*.

La sociedad en que vivimos nos ha enseñado desde que éramos niños reglas básicas de protección de nuestras propiedades. Cerrar la puerta de casa, los límites que nos imponemos a la cantidad de efectivo que llevamos en el bolsillo, la forma en que reaccionamos cuando nos aborda un extraño por la calle, son comportamientos que hemos aprendido a lo largo de nuestra vida. En cambio, nuestra experiencia con *internet* es muy breve y ni nuestros padres ni nuestros profesores nos dijeron nunca cómo debíamos comportarnos en el ciberespacio.

En una sociedad que, cada día basa más sus dinámicas en sistemas de cómputo, comunicaciones y redes, la seguridad debe pasar de ser una tarea más a una prioridad para los gobiernos, instituciones, compañías e individuos.

¿Qué podemos decir entonces? ¿La *internet* es dañina? De ninguna manera, ya que es, sin duda, una de los más útiles instrumentos que facilita las actividades cotidianas que en otra época hubieran requerido mayor inversión de esfuerzo, dinero y tiempo. Por tanto, lo único que debemos hacer es tomar las precauciones adecuadas para que no se convierta en una verdadera pasadilla.

En sus inicios, la Policía Federal Preventiva se constituyó como una herramienta decisiva en la lucha contra la delincuencia. Sin embargo, con el paso del tiempo se modificó el concepto, debido, en parte, a los constantes cambios en los mandos superiores, pues se perdía la continuidad en sus estrategias.

Hay que reconocer que el ideario de la Policía Cibernética es muy claro, pero no se lleva a la práctica. En sus primeros años se dedicó a realizar un

verdadero patrullaje y al mismo tiempo a crear lazos con otras corporaciones del mundo que tienen el mismo fin: la seguridad en el ciberespacio. Sin embargo, su personal se ha visto disminuido, los intereses de los altos mandos son otros, al parecer, no hay ningún interés en darle los apoyos necesarios para su desarrollo y mejor funcionamiento.

Simplemente, su página de internet *ni siquiera puede consultarse. me parece lamentable que el portal de la Secretaría de Seguridad Pública y en particular el apartado de la Policía Cibernética carezca de vínculo visible para hacer denuncias o formulario de contacto, que el vínculo correspondiente sólo redireccione a la página de inicio, y lo que es peor, que el único enlace a la página de denuncia en línea no esté funcionando. Tampoco existe ya el apartado para denuncias.*

Hoy, tristemente, la Policía Cibernética no está en su mejor momento. A pesar de ello, su maquinaria sigue funcionando, cada elemento realiza su tarea y prueba de ello son los logros alcanzados.

Es necesario que la gente conozca esta labor, y quizá sería importante que el trabajo de la Policía Cibernética tuviera más difusión, aunque surge una interrogante ¿Qué tanto debe saber la población acerca de de su labor, pondría en riesgo la información privilegiada con que cuenta para la persecución de pedófilos y delincuentes?

Si el público conociera mejor el trabajo de la Policía Cibernética, a través de los medios de comunicación y tuviera todas las facilidades para denunciar, facilitaría la labor de esta corporación.

Lo cierto es que luego de tener acceso a las imágenes obtenidas por los ciberpolicías, en las que se muestra el abuso a los niños, queda claro que esto, sólo es la punta del iceberg y que hace falta mucho trabajo, recursos y empeño por parte de las autoridades.

Mientras nuestras autoridades no tomen conciencia del grave problema que significa los delitos cibernéticos, mientras los altos mandos sólo se preocupen por

mantener su imagen ante los medios de comunicación, los delitos en la internet *continuarán en ascenso.*

Queda claro que en estos momentos, la Policía Cibernética es incapaz de cumplir el fin para el cual fue creada y tristemente se suma al resto de los pretenciosos e inútiles "organismos" que son la herencia del sexenio de Vicente Fox.

GLOSARIO

Ciber Viene del griego y significa "máquina". Se utiliza como prefijo para palabras como Ciberespacio.

Cibernética:La cibernética es una ciencia interdisciplinaria que trata de los sistemas de control y de comunicación. La palabra cibernética proviene del griego κυβερνητική y significa "arte de pilotar un navío", aunque Platón la utilizó en La república con el significado de "arte de dirigir a los hombres" o "arte de gobernar". En el siglo XIX, André-Marie Ampère y James Clerk Maxwell retomaron el sentido político de la palabra.

Computadora Máquina compuesta de elementos físicos, en su mayoría electrónicos, capaces de realizar una serie de trabajos a gran velocidad y con gran precisión, siempre que se le den las instrucciones adecuadas.

Programa Conjunto de ordenes que se dan a una computadora para realizar un proceso determinado

Informática Tratamiento automático de la información.

Aplicación informática Conjunto de uno o varios programas más la documentación correspondiente.

Sistema Informático Conjunto de elementos necesarios (Computadoras, terminales, impresores, etc.) para la realización y exploración de aplicaciones informáticas.

Información Es el conocimiento producido como resultado del procesamiento de los datos

Datos Informaciones no elaboradas y que una vez procesados (ordenados, sumados, comparados, etc.) constituyen lo que se denomina información útil.

Hardware Conjunto de elementos materiales que componen un sistema Informático.

CPU (Unidad central de proceso) Unidad, o cerebro, que coordina y realiza todas las operaciones del sistema Informático.

Software Es la parte lógica que dota al equipo físico de capacidad para realizar cualquier tipo de trabajo, tiene su origen en ideas y procesos desarrollados por el elemento humano, plasmado en un soporte determinado del hardware. Desde un punto de vista legal, el bien jurídico tutelado será la propiedad intelectual.

Criptografía Ocultación de la información mediante cifrado.

Internet Red de datos ideada para transmitir imagen y voz.

Los virus informáticos Que son? pequeños programas de computadora que tienen la capacidad de autoduplicarse y parasitar otros programas. Una vez difundidos, los virus se activan bajo determinadas circunstancias y en general, provocan algún daño o molestia.

El virus informático tiene tres características principales: produce daño, es autorreproductor y es subrepticio.

Es dañino porque es un programa que, cuando se lo ejecuta comienza a consumir recursos. El accionar es subrepticio porque el usuario no percibe su presencia.

Los virus se clasifican según el tipo de entidad ejecutable que utilizan para ejecutarse y propagarse (infectar un sistema a ir de un sistema a otro) en: Virus del sector de arranque de los disquetes y Virus de archivos ejecutables.

Caballos de Troya Se difunden disfrazados de programas útiles, bajo la apariencia de versiones mejoradas, o en un atache de un e-mail (es decir un archivo en un correo electrónico)

Gusano "Worm" es un programa similar al virus, pero que a diferencia de éste no requiere infectar a otro programa, ya que se difunde en forma autónoma de computadora a computadora.

Chat El término anglosajón chat se utiliza para denominar a una conversación online en tiempo real que se establece entre dos o más personas.

Protocolo Un protocolo de comunicación es la manera de comunicarse que tiene una computadora con otra, cuando se están transmitiendo datos entre sí.

FUENTES DE CONSULTA

1. Ayala, Claudia, "*Graves Patologías de Adultos que Abusan de Menores*", en Universal Gráfico, p 13. 06/06/01

2. Aguayo Quezada Sergio, "La Charola: Una historia de los servicios de inteligencia en México", 2001 ed., Grijalbo, 2001

3. Fernández Calvo, Rafael. *Glosario Básico de Internet - ATI* [en línea]. Versión HTML .1.1 José Ramón Yeste y Alonso Álvarez García, colaboradores. Asociación de Técnicos de Informática. 1995. consulta 19/julio/2006

4. García Luna, Genaro, *Contra el Crimen, ¿Por qué 1,661 Corporaciones de Policía no Bastan?, Presente, Pasado y Futuro de la Policía en México*, pp170

5. Marín Carlos, *"Manual de Periodismo*", ed., Debolsillo, 2006, pp 351

6. López Ruiz, Miguel, *Elementos para la Investigación, Metodología y Redacción*, Universidad Nacional Autónoma de México, UNAM, 1998, pp289

7. Real Academia Española. *Diccionario de la lengua española.* Real Academia Española. 20. ed., Madrid: Espasa-Calpe, 1984. 2 v.

8. Téllez Valdez, Julio. *Derecho Informático*. Editorial McGraw Hill, 282 p

9. Toussaint, Florence, *Crítica de la Información de masas*, ed., Trillas, México

10. Discurso del Director de CISEN Eduardo Medina-Mora Icaza, durante la presentación de los Resultados del Proceso de Evaluación del CISEN, julio 19 del 2001.

11. Boletín UNAM-DGCS-239 20 de Abril de 2007

12.http://www.coparmex.org.mx/contenidos/publicaciones/pag7/2001/nov01/nov01htm, consulta (29/06/2006)

13.http://www.lacrisis.com.mx/cgi-bin/criscgi/DisComuni.cgi?colum22%7C20040220004750 (consulta 2/08/2006)

14. WWW.INDICEPOLITICO.COM
http://www.sre.gob.mx/dgomra/oea/remja.htm (consulta 14/01/2007)

15.archivo.elnuevodiario.com.ni/2004/enero/26-enero 2004/nacional/nacional3.html (consulta 04/02/07)

16. http://www.funglode.org (consulta 27/03/2007)

17. Symantec Corporation. 2007. http://www.symantec.com (consulta 05/08/07)

18. Sociedad Internet de México. 2007. www.isocmex.org.mx (consulta 14/10/2007)

19. Asociación Mexicana de Internet. 2007. www.amipci.org.mx (consulta 14/10/2007)

20. Organización para la Cooperación y el Desarrollo Económico (OCDE) http://www.oecd.org/department/0,2688,en_2649_34267_1_1_1_1_1,00.html (consulta 20/05/2007)

21. Manejo del Comercio Electrónico (ECSG)http://www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html (consulta 27/03/2007)

22. Red Internacional de Protección al Consumidor y Aplicación de la Ley (ICPEN) http://www.icpen.org/ (consulta 14/10/2007)

23. http://www.enterate.unam.mx/Articulos/2006/enero/robo.htm 14 (02/07/2006)

24. Levene, R. (nieto) y Chiaravalloti, A., Delitos Informáticos, LL,1998-E-1228 / LL,1998-F-976. (consulta 14/10/2007)

25. http://www.lazarillo.com/latina/a/02hemilce.htm (consulta 05/08/2007)

26. Observatorio Bibliográfico del Derecho de la Economía. http:// www.iusimpresa.com (consulta 14/10/2007)

27. Columna Indicador Político, Carlos Ramírez, El Financiero on Line, 20 julio 2007

28. www.seguridadidl.org.pe/destacados/2006/03-02c.doc (consulta 05/08/2007)

29. CIMA NOTICIAS, PERIODISMO CON PERSPECTIVA DE GÉNERO www.cimacnoticias.com/noticias/06feb/s06022808.html (consulta 10/03/2007)

30. www.cibersivo.com/vtexto/desplieganota.cgi?nota=/noticiero/notas/2003-173-2034.txt (consulta 19/06/2006)

31.www.seguridad.unam.mx/eventos/datos/ev16/semi19/mat.20.pon37.semi19.pdf (consulta 19/06/2006)

32. Revista Red de Abril 2007 http://www.red.com.mx/index.php

33. http://www.portaldeabogados.com.ar (consulta 17/07/06)

34. http://www.bibliojuridica.org/ (consulta 19/06/2006)

35. http:/www.cem.itesm.mx/dacs/publicaciones/ (consulta 19/06/2006)

36. http://congreso.seguridad.unam.mx/ (consulta 05/06/07)

37. http:/www.copianos.com (consulta 19/06/2006)

38. http://www.delitosinformaticos.com.mx/ (consulta 19/06/2006)

39. http://www.derecho.org (consulta 17/05/2006)

40. http://digitaldesign.bariloche.net.ar/ (consulta 19/06/2006)

41. http://www.enterate.unam.mx/ (consulta 09/11/07)

42. http://es.wikipedia.org/

43. http://www.geocities.com/

44. http://www.gsi.dit.upm.es/

45. http:/www: indiana.edu/ iupress. (consulta 19/06/2006)

46. http://inicia.es/de/pazenred/delin1.htm (consulta 19/06/2006)

47. http://www.monografias.com/

48. http://www.onnet.es (consulta 05/05/06)

49. http://sapiens.ya.com/terrorista87k (16/03/2007)

50. http://www.secom.gov.ar/municipios (consulta 19/06/2006)

51. http://sitio.acis.org.co/ (consulta 15/08/06)

52. http://www.ssp.gob.mx/

53. http://tiny.uasnet.mx/

54. http://www.unam-cert.unam.mx

55. http://www.mastermagazine.info/termino/4232.php (consulta 18 enero 2008)

56. http://www.cem.itesm.mx/dacs/publicaciones/logos/espejo/2002/octubre.html

57. Revista Contaduría Pública Los delitos informáticos y el cómputo forense
autor Andrés Velázquez, CISSP, BS7799, CSIRT viernes, 01 de julio de 2005
http://www.mattica.com/articulo_detalle.php?id=51 (consulta 17/01/08)

58. "Roberto", Policía Cibernético

59. "Eduardo", Policía Cibernético

60. Policía Federal Preventiva, Secretaría de Seguridad Pública (SSP)