Universidad Autónoma del Estado de Hidalgo

Instituto de Ciencias Sociales y Humanidades

Área Académica de Derecho y Jurisprudencia

SISTEMATIZACIÓN DE LOS TIPOS PENALES FEDERALES SUSCEPTIBLES DE SER CONCRETADOS POR MEDIOS INFORMÁTICOS

Proyecto terminal de carácter profesional que, para obtener el grado de Maestro en Derecho Penal y Ciencias Penales presenta:

Javier Omar Montoya Piña

Director:

Doctor José Luis Gómez Tapia

Pachuca de Soto, Hidalgo Julio de 2013

Al Gran Arquitecto del Universo,

a mi Madre, a mi Padre que me

guía desde el cielo, a mis hermanos

por su fundamental apoyo,

Para ti Meztli, la razón que motiva

mi vida, sonrisa que ilumina mi camino

y origen de mi felicidad, que otorga

el impulso e inspiración al

que hacer de cada día…

Vivimos en una sociedad profundamente

dependiente de la ciencia y la tecnología

y en la que nadie sabe nada de estos temas.

Ello constituye una fórmula segura para el desastre.

(Carl Sagan)

ÍNDICE

RESUMEN

Esta investigación se concreta en analizar la legislaciones nacionales e internacionales, las cuales tienen relación o contemplan tipos penales susceptibles de ser cometidos por medios informáticos, verificar la ausencia de elementos de estos delitos en la legislación nacional planteando el estado de la cuestión de este fenómeno, lo que han hecho otros países en este rubro, así como nuevas estrategias de protección para hacer frente a las nuevas formas o variantes de delitos, lo cual favorecería en mucho el combate a la delincuencia, pues en lo que a informática se refiere no deben existir en México tantas lagunas jurídicas o falta de información al respecto, como hasta la fecha, demostrar los posibles delitos y variables de estos, que se pueden dar a través del manejo de una computadora o las TICS, identificar las incongruencias y divergencias entre la legislación nacional e internacional, a fin de proponer los ejes rectores que permitan cumplir con su teleología al Derecho Penal Nacional en esta materia.

En este Proyecto se realiza un análisis de la legislación mexicana en general, además de verificar tipicidades y atipicidades en materia de Delitos Informáticos. Si bien es cierto, en algunas de las legislaciones no son tipificados como tales pero si se encuadran en conductas ilícitas que crean un menoscabo en la víctima u ofendido de estas acciones, ya sea en su persona o patrimonio.

Se efectúa un ejercicio de derecho comparado en este tema, para verificar las leyes e instrumentos internacionales y demostrar las que han brindado las mejores soluciones de cada país y al final proponer ser parte de los instrumentos internacionales o tomar un modelo de ley para adaptarlas a la legislación nacional existente. Los llamados delitos informáticos o delitos a través de medios informáticos, son una nueva forma de criminalidad que están ocasionando graves problemas y se necesita buscar soluciones, pues hoy en día es insuficiente la normativa para su combate y por lo tanto su prevención. Es esencial legislar en el tema para mantener la integridad de los sistemas informáticos y penalizar el acceso ilícito cuyos fines son la producción de diversos delitos.

Javier Omar Montoya Piña

Universidad Autónoma del Estado de Hidalgo, 2013.

ABSTRACT

The purpose of this research is to analyze specific national and international law, to verify the absence of specific elements of these crimes in national legislation, and to raise the state of affairs of this phenomenon. Also what other countries have done in this area, and new strategies to protect against new alternatives prepared or variants of crimes, which would greatly enhance the fight against crime. As far as information is concerned, there should not be so many loopholes in Mexico or lack of information, as to date. Demonstrating the potential of these offenses and variables that can be given through the management of a computer or other technologies, to identify inconsistencies and discrepancies between national and international law; in order to propose the guiding principles that would meet with it's responsibility to national criminal law in this area.

In this project, an analysis of Mexican law in general, in addition to verifying their existence or nonexistence on Cybercrime. Because, some of these laws are not classified as such, therefore these people being ignorant of this situation, suffer the illicit behaviors that create an interference for the victim by these actions, either in his person or property.

It is essential to investigate into one comparative law in this area, to check the laws and international instruments, and demonstrate the laws that have provided the best solutions for each country, and eventually propose to be part of the international instruments to take a model law to adapt to existing national legislation.

The so-called computer crimes or offenses through information technology, are a new form of crime that are causing serious problems and need solutions, because today there is insufficient knowledge of different ways to fight them legally.

It is essential to legislate on the subject to maintain the integrity of computer systems and penalize the illegal access, which purpose is to produce various offenses.

INTRODUCCIÓN

En la actualidad es imprescindible el uso constante de las tecnologías de la información y la comunicación, ellas están omnipresentes y cada vez es mayor la tendencia para el intercambio de la mismas, el uso de estas herramientas ha incluido el manejo de aplicaciones para ser utilizada por el común de la gente, sin embargo a la par de ello han surgido acciones ilícitas por conocedores del tema, causando daños de una forma nueva y critica.

Actividades realizadas por medio de ordenadores y tecnologías de información y comunicación cuya principal herramienta es internet, que se han vuelto cada vez más frecuentes y sofisticados, evidentemente trayendo consecuencias de afectación a la esfera jurídica de las personas, por citar un dato cada segundo 18 adultos son víctimas de ciberdelitos; es decir, más de un millón y medio de víctimas cada día en todo el mundo.

Encontrar posibles soluciones, respuestas e información del tema es un reto importante, en México no existen instrumentos jurídicos al respecto que proporcionen medidas de protección para garantizar la seguridad en el uso de las tecnologías de la información mencionadas, excluyendo evidentemente la aplicación de medidas de salvaguarda y protección a los usuarios de las mismas.

La presente investigación se origina a partir de la aparición de nuevas tendencias de criminalidad, las cuales van de la mano del uso de la tecnología que crece a pasos acelerados y propiciando las condiciones para cometer conductas ilícitas cuyas consecuencias y realidades repercuten en el desarrollo del derecho. México aún no cuenta con mecanismos efectivos legislativos y en específico con la unificación de legislaciones, así como de acciones o programas en el rubro de la política criminal para frente a este problema.

En este diseño de investigación se analizaron los conceptos inherentes a los delitos informáticos como se les ha estado llamando a nivel Latinoamérica y España, así como el de cibercriminalidad, un concepto anglosajón que se ha tomado de manera global en la mayoría de los países, y se explica el por qué se ha optado también por llamarles delitos cometidos a través de medios

informáticos. Es indispensable conocer los antecedentes sociológicos de este tema respecto a internet, cuyo uso nivel internacional ha sido la llave del crimen organizado, que ha podido actuar eliminando distancias y fronteras, analizando como esta tecnología ha ido evolucionando hasta que consecuentemente pueda encontrarse a la mano de cualquier persona en el planeta, y no así, como anteriormente, siendo solo las organizaciones gubernamentales de primer mundo quienes tenían acceso a éste.

En México, los primeros en utilizar internet fueron las Universidades de manera local y gradualmente éstas, lograron utilizarlo a nivel internacional con Universidades extranjeras.

Otro aspecto importante que se aborda, es el de las redes sociales; donde se examinan tanto tendencias internacionales como nacionales, sobre el uso o principales actividades que se les da, así como el alcance por edad y género.

De igual manera para la elaboración de este trabajo, se estudiaron las iniciativas de ley existentes a la fecha, además de las reformas o adiciones al Código Penal Federal, tanto de las diferentes comisiones de la Cámara de Diputados y la de Senadores, inclusive por fracciones legislativas de cada uno de los partidos y las propias del Ejecutivo Federal.

Al no existir una ley específica, y tomando en cuenta que las que se encuentran actualmente abordan sólo algunos temas relacionados con los delitos informáticos, podemos concluir que no son suficientes para determinar la totalidad de casos o circunstancias que la justicia debe resolver, es por ello que en un acierto para resolver estos vacíos, se han introducido una serie de diversas jurisprudencias o tesis aisladas que tratan de resolver estas lagunas jurídicas, en este proyecto se mencionaran las más importantes al respecto.

En el contexto Internacional existen países que tienen un gran adelanto en materia de cibercriminalidad, incluso algunos cuyo avance es de décadas en el tema, que sirven de modelo para que en México se tomen medidas pertinentes y necesarias al respecto. En esta investigación se mencionan los países en cuya legislación ya existe una ley específica referente a los delitos informáticos. Siguiendo la metodología, para su mejor estudio fueron divididos en las

siguientes familias: Common Law, Romano-Germánica, jurídico Asiática jurídico socialista y la Supranacional.

Así mismo existen organismos Internacionales como el G8, la ONU, la Unión Internacional de Telecomunicaciones, el Consejo de Europa, la OCDE, la APEC, la Commonwealth, la Liga Árabe y la Organización de Estados Americanos que han estado muy activos en relación a la creación de instrumentos internacionales que ayuden a la pugna contra la cibercriminalidad y a razón de estos instrumentos los países que forman parte de los Organismos antes mencionados, fungen como signatarios de los mismos , sirviéndoles de patrones para la creación de sus leyes en su respectivo país o, en menor medida, para la toma de determinaciones de modificación en sus legislaciones penales.

En México la política criminal o programas del gobierno sobre este es casi nula y de la poca información existente, se aprecia un desconocimiento del tema; sin embargo, es trascendente considerar los puntos aprobados por la LX Quincuagésima Quinta Legislatura en diciembre de 2006, por la Cámara de Diputados, relativos a los procedimientos de prevención de riesgos en el uso de internet, en donde se abordan aspectos como la creación de una Coordinación de Delitos Electrónicos, su monitoreo y prevención.

La policía cibernética en México es un organismo dependiente de la Secretaría de Seguridad Pública Federal que se ha encargado de monitorear sitios de internet y cerrar aquellos principalmente de pornografía infantil, inclusive algunos estados del país han creado su propia policía cibernética, cuyo inconveniente hasta el momento, es que se encuentra limitada en su proceder, ya que no existe un ordenamiento legal que le de facultades para actuar al margen de este.

A través del uso de las herramientas informáticas se pueden llevar a cabo un sinfín de conductas que pueden tener un propósito delictivo, las cuales no pueden ser encuadradas a un tipo penal por la complejidad o el sin número de acciones en su realización, los bienes jurídicos protegidos en donde recae la conducta; algunas de estas conductas se encuentran en los llamados *códigos*

maliciosos los cuales tienden al menoscabo del patrimonio o el daño personal; los principales códigos o los más utilizados en los últimos tiempos serán abordados en esta investigación, de igual forma se examinará, como algunos de estos códigos maliciosos pueden ser utilizados para cometer delitos ya tipificados en el Código Penal Federal.

En el desarrollo de la investigación como uno de los principales temas, se concreta en la creación de una Ley General de Delitos Informáticos, para lo cual se toman en cuenta legislaciones nacionales que consideran algunos aspectos generales referentes a los delitos informáticos, como son: La Ley Federal de Telecomunicaciones, Ley de la Propiedad Industrial, Ley de Instituciones de Crédito, Ley de Seguridad Nacional, Ley Federal contra la Delincuencia Organizada y la reciente Ley federal de Protección de Datos Personales en Posesión de Particulares.

De igual forma, se sistematizaron los puntos principales que abordan algunos estados de la República Mexicana contenidos en sus Códigos Penales, donde adicionan o inclusive se crean títulos referentes a los delitos informáticos; cabe mencionar que se estudiaron los que hasta el momento cuentan con ello, ya que la tendencia de todos los estados se encamina hacia la creación de un capitulo referente a estos temas, para protegerse jurídicamente en espera de la creación de una ley general.

En la última parte se hace un análisis personal del delito informático en relación a sus hipótesis normativas, para poder explicar el nexo que se articula con la disposición en caso de existir y a su vez, con estos elementos poder crear el tipo así como el análisis de cada uno de sus elementos constitutivos del mismo.

Al final se plantean una serie de propuestas en las que se proyectan acciones que debe llevar a cabo el Gobierno Federal, que se deben de tomar en cuenta para el combate de los delitos informáticos, así como los principales elementos a considerar para la elaboración de una Ley General de Delitos Informáticos en México.

JUSTIFICACIÓN

El motivo por el cual se optó este objeto de estudio, obedece fundamentalmente a que la tecnología y la globalización son temas no solo de Conocimiento general, si no también temas que se han vuelto en la práctica, de naturaleza esencial para los seres humanos, además, que así como la tecnología cambia constantemente, el derecho debería estar preparado para crear elementos que permita dar una protección eficaz contra la criminalidad informática, que presupone ante todo que las víctimas conozcan los riesgos potenciales que dañen su persona o patrimonio dentro del ambiente informático así como sus formas de encubrimiento.

Esta serie de conductas ilícitas a través de medios electrónicos o herramientas informáticas son difíciles de probar y por obvias razones no se pueden perseguir ni castigar aunado a la falta de la correcta tipificación. Se debe lograr una correcta tipificación de los delitos informáticos y electrónicos en la legislación mexicana no solo en su función punitiva sino también en su función preventiva.

El desarrollo del Internet y la proliferación de la tecnología informática han creado nuevas oportunidades para aquellos que participan en actividades ilegales. La tecnología y la comunicación en línea no sólo ha producido un aumento en la incidencia de la actividad delictiva, sino que también ha dado lugar a la aparición de algunas variedades de los delitos ya existentes, es importante que todo sistema jurídico incluyendo el mexicano, adopte medidas necesarias para garantizar que la legislación sea la adecuada para afrontar los retos planteados por esta clase de delitos. Estamos es tiempo para adoptar medidas pertinentes para resolver tales eventos antisociales, ya sea mediante la adopción de una ley específica o mediante la modificación del Código Penal Federal y de las legislaturas locales.

El principal problema que existe en México, no es necesariamente la falta de tipificación de estos delitos, es más bien, la falta de conocimiento de todas las acciones ilícitas que se pueden llevar a cabo con el uso indebido de los medios informáticos, lo que imposibilita la persecución y castigo de los autores en forma

efectiva. Aunado a esto las autoridades no poseen el nivel de conocimiento y experiencia requerido en estas áreas, ni la capacidad para desarrollar actividades de investigación, persecución y recopilación de pruebas digitales y electrónicas para la persecución de estos delitos. Por lo que, todo tipo de acción contra los delincuentes informáticos, quedaría prácticamente en las manos de organizaciones privadas o las llamadas policías cibernéticas, que apenas se están creando en México, que descubren una acción ilícita, y al no ser ésta considerada como delito, la sanción se vuelve más administrativa que penal.

Es necesario estructurar una propuesta legislativa que contenga los elementos necesarios para la creación de una Ley general contra delitos informáticos, así mismo sugerir los cambios necesarios al Código Penal Federal acerca de delitos informáticos, así como integrar los elementos específicos que otras normas existentes en México contemplan.

México debería tener una sólida estructura y los medios adecuados para combatir los delitos informáticos, ya que actualmente existen legislaciones que tipifican algunas conductas, las cuales pueden ser adaptadas en relación a delitos que tienen que ver con la informática, directamente con la propiedad intelectual, acceso ilegal a dichos sistemas de información, alteración, daño, modificación o que se provoque pérdida de información contenida en estos, entre otros.

En la mayor parte de las legislaturas locales existe una heterogeneidad de variables, se toman otros aspectos en relación con este tipo de delitos, pero son demasiado escuetos.

La principal característica de estas conductas, es que la mayoría aún no están tipificadas como tales dentro de las leyes de algunos países como México y por lo tanto no son sancionadas.

Si no se pone atención en este tema como país, se quedará atras del derecho internacional y a nivel nacional existen varios delitos que podrían quedar impunes como los delitos contra las personas, contra la propiedad, contra la moral, contra el Estado y otros que se contemplarán en esta investigación.

CAPÍTULO I

ANTECEDENTES

1. APROXIMACIÓN TEÓRICO-CONCEPTUAL DE LOS DELITOS INFORMÁTICOS

Para poder definir delito informático, es necesario conocer previamente algunos términos considerados indispensables de manera general para empezar a establecer un panorama más amplio al respecto; cabe hacer mención que existen puntos encontrados en relación al mismo término, ya que algunos escritores creen que el concepto de "delito informático" no debe de considerarse como tal, ya que para ser considerado delito debe estar la conducta ilícita tipificada o positivada en alguna legislación, lo cual hasta el momento no ocurre en México, sin embargo, existen delitos que pueden realizarse con una computadora o algún otro dispositivo tecnológico, conductas ilícitas que se encuentran tipificadas en algunas legislaciones Federales y que por lo tanto se consideraría más viable el término "Delitos cometidos a través de medios informáticos".

Si bien es cierto en su acepción etimológica, la palabra delito deriva del verbo latino *delinquere*, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley. En este caso, abandonar la ley.[1]

Autores de la Escuela Clásica como Francisco Carrara, define al delito como la infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, y que resulta de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso.[2]

En lo que respecta al término informática, este concepto fue acuñado por Philipe Dreyfus mediante la contracción de información y automática, que la

[1] Pina Vara, Rafael, *Diccionario de Derecho*, México, Porrúa, 2004, p 219.

[2] Carrara, Francisco, *Programa de Derecho Criminal parte general*, Bogotá, Editorial Temis, volumen I, p. 43.

define como la ciencia del tratamiento automático o automatizado de la información, primordialmente mediante las computadoras.[3]

El convenio sobre la ciberdelincuencia celebrado en Budapest, el 23 de noviembre de 2001 por los miembros del Consejo de Europa define al Sistema Informático como *todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa*.

Así mismo, define a los datos informáticos como *cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función.*

La Ley Federal de Derechos de Autor en México en su Artículo 101, define de manera clara y precisa un programa de computación como: la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

A) CONCEPTO DE DELITO INFORMÁTICO

Después de haber analizado conceptos referentes a lo que es delito y la informática a continuación se expresan definiciones de diversos autores u organismos que manejan el concepto de Delito informático literalmente:

Para Jorge Esteban Cassou Ruiz por delito informático, suele entenderse toda *aquélla conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático*.[4]

Organismos internacionales como la OCED, lo define *como cualquier conducta, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos.*

[3] Fix Fierro, Héctor, *Informática y documentación jurídica*, México, UNAM, 1990, pp. 44 y 45.

[4] Revista del Instituto de la Judicatura Federal, Cassou Ruíz, Jorge Esteban, *Delitos Informáticos en México.* Poder judicial de la federación. México, D.F. 2009, P. 207

Para Julio Téllez Valdez, los delitos informáticos son aquéllas *actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables.*[5]

El mismo autor establece como característica de dichos antijurídicos que son conductas delictivas de cuello blanco, porque se requieren conocimientos técnicos; son acciones ocupacionales por realizarse cuando el sujeto activo labora, y son acciones de oportunidad pues se aprovecha la ocasión o el universo de funciones y organizaciones de un sistema tecnológico y económico.

Cabe destacar que se considera necesario precisar en relación a los elementos del delito; (para especificar en lo particular a lo que el delito informático se refiere); así, según Enrique Díaz-Aranda,[6] en los cuatro sistemas del delito que fueron desarrollados por la dogmática penal alemana, como lo son el clásico, neoclásico, finalista y funcionalista.[7]

En relación a la función de la conducta típica, cuando el legislador penal identifica los bienes fundamentales para la sociedad y considera que ciertas conductas los afectan gravemente, siendo el Derecho Penal el único medio eficaz para evitar su comisión, en ese momento realizan un ejercicio de abstracción para crear tipos penales (conformados por uno o varios artículos contenidos en una o varias leyes penales).[8] En este caso la creación de los tipos

---

[5] *http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf*

[6] Díaz-Aranda Enrique, *Teoría del delito*, México, Straf 2006, , p. 203.

[7] En el sistema clásico se analizaba el tipo objetivo (conformado por todos los elementos perceptibles a través de los sentidos) al cual se adicionaron los elementos normativos en el sistema neoclásico (aquellos que requieren de una valoración normativa), enseguida se procedía al análisis de la antijuridicidad y, una vez constatada la ausencia de causas de justificación, se proseguía con el examen de la culpabilidad, en particular el dolo. En el sistema final de acción, el análisis del delito se inicia con el tipo objetivo (elementos objetivos y normativos) y el tipo subjetivo (dolo o culpa) seguido de la antijuridicidad y, por último, la culpabilidad; en otras palabras, el examen del dolo se realizaba en la primera categoría o escalón: el tipo, y después se pasaba al análisis de la antijuridicidad y la culpabilidad. El sistema Funcionalista propone un estudio dogmático del delito estrechamente relacionado a la política criminal, donde la función de la pena y la función del derecho penal respondan a una praxis social que permita consolidar la estructura social.

[8] Si la conducta típica se describe en un solo artículo estamos en lo que la doctrina denomina tipos cerrados, mientras que los tipos abiertos son aquellos supuestos en los que se necesita recurrir a varios artículos para establecer la descripción de la conducta típica. Cfr. Welzel, Hans, *El nuevo sistema del derecho penal (una introducción a la doctrina de la acción finalista)*, Trad. José Cerezo Mir, Barcelona, Ariel, 1961.

penales para la prevención y castigo de los delitos informáticos o cualquier hecho ilícito a través de alguna tecnología de información y comunicación.

B) CIBERCRIMEN

En los países anglosajones se maneja el término de *cibercrimen* el cual hace alusión a la cibernética y el crimen, término que aún se encuentra en la mesa de debate en cuanto a legislación de muchos países del mundo se refiere incluyendo a México, sin embargo a partir del atentado del 11 de Septiembre de 2001 contra las Torres Gemelas en la ciudad de Nueva York en los Estados Unidos de Norteamérica, el cual fue planeado y ejecutado a través del uso y aprovechamiento de las Tecnologías de la Información y Comunicaciones, así como a la amenaza global de terrorismo digital dirigido al ataque de sistemas financieros, sistemas de defensa, bases de datos, difusión de virus, entre otros factores, hace que se trabaje de manera seria y globalizada en la generación y aplicación de leyes enfocadas a castigar conductas delictivas cometidas mediante la utilización de equipos de cómputo y sistemas de comunicación ya sea como fin o como medio.

2. ANTECEDENTES SOCIOLÓGICOS

A) EXTRANJEROS

LA INTERNET RESEÑA HISTÓRICA[9]

La Agencia de Proyectos de Investigación Avanzada (ARPA) se inició en el Departamento de Defensa de los Estados Unidos en los últimos años de la década de los cincuenta para investigar los campos de ciencia y tecnología militar. El objetivo de la propuesta era plantear una red que tuviera la máxima resistencia ante cualquier ataque enemigo.

Se suponía que una red de comunicaciones, por si misma, no era fiable debido a que parte de ella podría ser destruida durante un ataque bélico.

En 1968 el Laboratorio Físico Nacional en Inglaterra estableció la primera red de prueba basada en estos principios. En el mismo año, el primer diseño

[9] Linkses, *La Historia de Internet, www.mundoscibernetico.com*

basado en estos principios de envío de paquetes de información, realizado por Lawrence. Roberts, fue presentado en la ARPA. La red se llamó ARPANET.

Al año siguiente, el Departamento de Defensa dio el visto bueno para comenzar la investigación en ARPANET. El primer nodo, fue la Universidad de California en Los Ángeles. Estos sitios (como denominamos a los nodos) constituyeron la red original de cuatro nodos de ARPANET. Los cuatro sitios podían transferir datos en ellos en líneas de alta velocidad para compartir recursos informáticos.

El comienzo de la década de los setenta vio el crecimiento de la popularidad del correo electrónico sobre redes de almacenamiento y envío. En 1971, ARPANET había crecido hasta 15 nodos con 23 ordenadores hosts[10] (centrales). En este momento, los hosts comienzan a utilizar un protocolo de control de redes, pero todavía falta una estandarización. En 1972 Larry Roberts de DARPA decidió que el proyecto necesitaba un empujón. Organizó la presentación de ARPANET en la Conferencia Internacional sobre Comunicaciones por Ordenador.

En 1972 Bolt, Beranek v Newman (BBN) produjeron una aplicación de correo electrónico que funcionaba en redes distribuidas como ARPANET. El programa fue un gran éxito que permitió a los investigadores coordinarse y colaborar en sus proyectos de investigación y desarrollar las comunicaciones personales. Las primeras conexiones internacionales se establecieron en la Universidad *College London*, en Inglaterra. y en el *Royal Radar Establishment*, en Noruega junto con los ahora 37 nodos en EE.UU. La expansión era muy fácil debido a su estructura descentralizada.

[10] El término El término inglés *host* significa *anfitrión,* sentido con el cual se le interpreta en informática: equipo anfitrión.
http://www.conacyt.gob.mx/comunicacion/revista/193/Articulos/DNS/Ligas/Enlosorigenes01.html
Un host, literalmente anfitrión, es un ordenador directamente conectado a una red y que efectúa las funciones de un servidor, y alberga servicios, como correo electrónico, grupos de discusión Usenet, FTP, o World Wide Web accesibles por otros ordenadores de la red, *http://www.pergaminovirtual.com.ar/definicion/Host.html*

En 1974 se estableció el *Transmission Control Protocol* (TCP), creado por Vinton Cerf y Bob Kahn que luego fue desarrollado hasta convenirse en el *Transmission Control Protocol/Internet Protocol* (TCP/IP).

TCP convierte los mensajes en pequeños paquetes de información que viajan por la red de forma separada hasta llegar a su destino donde vuelven a reagruparse. IP maneja el direccionamiento de los envíos de datos.

En julio de 1975 ARPANET fue transferido por DARPA a la Agencia de Comunicaciones de Defensa.

El crecimiento de ARPANET hizo necesario algunos órganos de gestión: el Internet *Configuration Control Board* fue formado por ARPA en 1979. Más tarde se transformó en el Internet *Activities Board* y en la actualidad es el Internet *Architecture Board of the Internet Society.*

ARPANET en sí mismo permaneció estrechamente controlado por el DoD hasta 1983 cuando su parte estrictamente militar se segmentó convirtiéndose en MILNET. La *"European Unix Network"* (EuNet), conectado a ARPANET, se creó en 1982 para proporcionar servicios de correo electrónico y servicios Usenet a diversas organizaciones usuarias en los Países Bajos, Dinamarca, Suecia e Inglaterra.

En 1984 el número de servidores conectados a la red había ya superado los 1,000 Dado que el software de TCP/IP era de dominio público y la tecnología básica de Internet (como ya se denominaba esta red internacional extendida) era algo anárquica debido a su naturaleza, era difícil evitar que cualquier persona en disposición del necesario hardware (normalmente en universidades o grandes empresas tecnológicas) se conectase a la red desde múltiples sitios.

En 1986, la *National Science Foundation* (NSF) de EE.UU. inició el desarrollo de NSFNET que se diseñó originalmente para conectar cinco superordenadores. Su interconexión con Internet requería unas líneas de muy alta velocidad. Esto aceleró el desarrollo tecnológico de INTERNET y brindó a los usuarios mejores infraestructuras de telecomunicaciones. Otras agencias de la Administración norteamericana entraron en Internet, con sus inmensos recursos informáticas y de comunicaciones: NASA y el Departamento de Energía.

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

En 1989 el número de servidores conectados a Internet alcanza ya los 100,000 En este mismo año, se inauguró también la primera conexión de un sistema de correo electrónico comercial a Internet (MCI y Compuserve). En 1990 redes de diversos países como España, Argentina, Austria, Brasil, Chile, Irlanda, Suiza y Corea del Sur se conectaron también a NSFNET.

En 1991 se retiraron las restricciones de NFS al uso comercial de INTERNET. Ese mismo año también se Conectaron más países a la NSFNET incluyendo: Croacia, Hong Kong, República Checa, Sudáfrica, Singapur, Hungría, Polonia, Portugal, Taiwan y Túnez.

En 1992 el número de servidores conectados a INTERNET sobrepasaba la cifra de un millón de servidores. En ese año, la Sociedad de INTERNET (ISOC) se formó para promocionar el intercambio global de información. La *Internet Architecture Board* (IAB), fue reorganizada para llegar a formar parte del ISOC.

Como acontecimiento clave en la historia reciente de Internet, también en 1992 se desarrolló la *World Wide Web* en el Laboratorio Europeo de Física en Suiza. Esta tecnología provocó un drástico cambio en la apariencia en el sentido y en el uso de INTERNET.

En 1993 el número de servidores INTERNET sobrepasa los 2,000,000 también NSF patrocina la formación de una nueva organización, ínterNIC, creada para proporcionar servicios de registro en Internet y bases de datos de direcciones. El conocido navegador WWW *“Mosaic”* se desarrolló en el *National Center for Supercomputing.*

El número de servidores de Internet alcanza los 3,800,000 en 1994. Las primeras tiendas Internet empiezan a aparecer junto con "emisores" de radio on-line.

En 1995 había más de 5 millones de servidores conectados a Internet. La espina dorsal de NSFNET empezaba a ser sustituido por proveedores comerciales interconectados.

Hoy en día Internet está formada, no solamente de restos de la ARPANET original, sino que también incluye redes como la Academia Australiana de Investigación de redes (AARNET), la *NASA Science Internet* (NSI), la Red Académica de Investigación Suiza (SWITCH), por no mencionar las miles de redes de mayor o menor tamaño de tipo educativo y de investigación.

La velocidad de crecimiento de Internet en los primeros años de la década de los noventa ha sido espectacular: se podría decir casi salvaje. Se extiende casi a la misma velocidad que los ordenadores personales en los años ochenta.

La Administración norteamericana sigue apoyando en gran medida a la comunidad de Internet, debido, sin duda, a que ésta era en su origen un programa de investigación respaldado federalmente, y ha llegado a ser una parte importante de la infraestructura de investigación académica e industrial estadounidense.

Los ataques segmentados, las amenazas en las redes sociales, la seguridad de los dispositivos móviles y la proliferación de herramientas de ataque son las principales tendencias en el panorama actual de amenazas.[11]

MOUNTAIN VIEW, California, 13 de abril de 2011 **–** Symantec Corp. (Nasdaq: SYMC) anunció los resultados de la XVI edición del "*Informe sobre las Amenazas a la Seguridad en Internet",* el cual muestra un volumen masivo de más de 286 millones de nuevas amenazas el año pasado, acompañado de nuevas mega tendencias en el ambiente de amenazas.

El informe destaca el aumento dramático en frecuencia y sofisticación de los ataques dirigidos a las empresas.

2010: El Año de los Ataques Dirigidos Ataques específicamente dirigidos como *Hydraq y Stuxnet* representaron un creciente riesgo a las empresas en

[11] Symantec, Informe sobre las Amenazas de Seguridad en Internet (ISTR por sus siglas en inglés) se deriva de datos recopilados por decenas de millones de sensores de Internet, investigación de primera mano y monitoreo activo de comunicaciones de hackers, y proporciona una visión global del estado de seguridad en Internet. El período del estudio del Volumen XVI del Informe abarca de enero de 2010 a diciembre de 2010.

2010. En este año los atacantes lanzaron ataques focalizados contra un conjunto de empresas que cotizan en la bolsa, corporaciones multinacionales y organismos gubernamentales, así como un número sorprendente de empresas más pequeñas. En muchos casos, los atacantes investigaron a las víctimas clave de cada empresa y luego utilizaron ataques personalizados de ingeniería social para ingresar a las redes de las víctimas.

Mientras que los ataques específicos de alto perfil durante 2010 intentaban robar la propiedad intelectual o causar daños físicos, muchos ataques focalizados engañaron a los individuos para obtener información personal. Por ejemplo, el informe reveló que las filtraciones de datos ocasionadas por *hackeo* generaron en promedio que más de 260,000 identidades fueran expuestas por fugas o filtraciones en 2010, lo que correspondió aproximadamente a cuatro veces más que cualquier otro incidente.

Stuxnet y Hydraq, fueron dos de los eventos cibernéticos con mayor visibilidad en 2010, representan verdaderos incidentes de actividad de ataques cibernéticos y fundamentalmente cambiaron el panorama de las amenazas. La naturaleza de las amenazas se ha modificado al pasar de ataques a cuentas bancarias individuales a ataques a la información e infraestructura física de las naciones o estados", dijo Stephen Trilling, Vicepresidente Senior de Tecnología de *Symantec Security Technology y Response.*

Las redes sociales: Un Terreno Fértil para los Cibercriminales Las plataformas de redes sociales seguirán creciendo en popularidad y esta popularidad ha atraído un gran volumen de malware. Una de las principales técnicas de ataque utilizada en sitios de redes sociales implicó el uso de URL abreviadas. En circunstancias típicas y legítimas, estas URL abreviadas son utilizadas para compartir eficazmente un enlace en un correo electrónico o en una página web en lugar de una dirección web complicada o muy larga. El año pasado, los atacantes publicaron millones de estos enlaces abreviados en sitios de redes sociales para engañar a las víctimas y cometer ataques de *phishing* y *malware*, lo que aumentó exitosa y considerablemente el porcentaje de infecciones.

El informe reveló que los atacantes aprovecharon enteramente las funcionalidades de canales de noticias suministradas por sitios populares de redes sociales para distribuir masivamente los ataques. En un escenario típico, el atacante ingresa a una cuenta de red social atacada y publica un enlace abreviado en un sitio Web malintencionado en el área de la víctima. El sitio de redes sociales luego distribuye automáticamente el enlace a canales de noticias de amigos de la víctima, propagando el vínculo potencialmente a cientos o miles de víctimas en minutos. En 2010, el 65 por ciento de enlaces maliciosos en canales de noticias observados por Symantec utilizó URL abreviados. De éstos URLS, el 73 por ciento fue visitado 11 veces o más y 33 por ciento recibió entre 11 y 50 clics.

Las herramientas de ataque se centran en Java: En 2010, el uso de kits de herramientas de ataque, programas de software que pueden ser utilizados por novatos y expertos para facilitar el lanzamiento de ataques generalizados en computadoras en red, siguió propagándose. Estos kits de herramientas atacan cada vez más vulnerabilidades del popular sistema Java, lo que correspondió al 17 por ciento de todas las vulnerabilidades que afectaron los *plug-ins*[12] de navegador en 2010. Dado que Java es una tecnología popular multiplataforma y compatible con diferentes navegadores, Java es un blanco atractivo para los atacantes.

El kit de herramientas Phoenix fue responsable de la actividad de ataques en la Web en 2010. Este kit, así como muchos otros, incorpora ataques contra vulnerabilidades de Java.

El número de ataques diarios basados en la Web aumentó un 93 por ciento en 2010 con respecto a 2009. Ya que dos tercios de toda la actividad de amenazas en la Web observada por Symantec se atribuye directamente a kits de ataques, así que éstos son probablemente responsables de gran parte de este incremento.

[12] Un plug-in (conector) es un módulo de código que el navegador obtiene de un directorio especial del disco y lo instala como una extensión de sí mismo. Tanenbaum A. S. Redes de computadoras. Pearson, México, 2003.

B) NACIONALES
LA INTERNET EN MÉXICO. RESEÑA HISTÓRICA

En 1986, el Campus Monterrey del Tecnológico de Monterrey (ITESM) ya recibía, por medio de líneas conmutadas, la información electrónica que circulaba a través de la red BITNET. El 15 de junio de 1987, el ITESM Campus Monterrey estableció una conexión de carácter permanente hacia esa importante red de información electrónica. Posteriormente en Octubre de ese mismo año, la Universidad Nacional Autónoma de México también se conectó a la red BITNET.

El 28 de febrero de 1989, el Tecnológico de Monterrey Campus Monterrey se convirtió en la primera institución mexicana que logró establecer un enlace a Internet, a través de una línea analógica privada de cinco hilos de nueve mil 600 bits por segundo.

El acceso a Internet se estableció por medio de un enlace hacia la Escuela de Medicina de la Universidad de Texas, en San Antonio, Estados Unidos (UTSA). El Campus Monterrey estableció el primer nodo de Internet en México y en consecuencia lógicamente dispuso del primer *name server*[13] para el dominio .mx.[14]

La UNAM fue la segunda institución que consiguió establecer un acceso a Internet, conformando un segundo nodo entre el Instituto de Astronomía –ubicado en la Ciudad de México– y el Centro Nacional de Investigación Atmosférica (NCAR) –en Boulder, Colorado, Estados Unidos–. Ese enlace digital se estableció vía satélite a 56 Kbps. La UNAM y el Tecnológico de Monterrey Campus Monterrey entonces mantenían un enlace común a través de la red de la información BITNET, mediante líneas analógicas privadas.

A finales de la década de los ochenta y principios de los noventa, las principales instituciones de educación superior en México adoptaron las medidas

[13] Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. Mayor información en Glosario dentro de Pharming.

[14] Fundación Manuel Buen Día, Apuntes académicos para una historia de internet en México, en: *http://www.mexicanadecomunicacion.com.mx/fmb/foromex/apuntes.htm*

necesarias para establecer alguna ruta de acceso hacia las redes de información electrónica.

A principios de la década de los noventa, RED-MEX, organismo integrado por instituciones académicas, ya discutía políticas, estatutos y procedimientos con los cuales se proponía regular el desarrollo de las redes de comunicación electrónica en México. Sin embargo, esa institución nunca consiguió incidir significativamente en el desarrollo de Internet en México.

Por tal motivo, el 20 de enero de 1992, en la Universidad de Guadalajara y por iniciativa de varias universidades –Sistema ITESM, Universidad de Guadalajara, Universidad de las Américas, ITESO, Colegio de Postgraduados, LANIA, CIQA, Universidad de Guanajuato, Universidad Veracruzana, Instituto de Ecología, Universidad Iberoamericana e Instituto Tecnológico de Mexicali–, se creó un nuevo organismo que se encargaría de coordinar los esfuerzos de las instituciones de educación superior interesadas en propiciar y contribuir al desarrollo de Internet en México: MEXnet.

El 1o. de junio de 1992, MEXnet estableció una salida digital de 56 kbps al Backbone de Internet. Entre 1989 y 1993, las universidades operaron como únicos proveedores de acceso a Internet. La primera institución pública que consiguió establecer un enlace a la supercarretera fue el Consejo Nacional de Ciencia y Tecnología (Conacyt), el 18 de enero de 1993, a través del Centro Nacional de Investigación Atmosférica (NCAR), en Boulder, Colorado, Estados Unidos. Ese año también se enlazó a Internet el Instituto Tecnológico Autónomo de México (ITAM), y la Universidad Autónoma Metropolitana (UAM) logró articular el primer “NAP” consiguiendo intercambiar información entre dos diferentes redes de información electrónica.

En 1994 se fusionaron las redes de información electrónica de MEXnet y de Conacyt gracias a lo cual nació la Red Tecnológica Nacional (RTN) cuyo enlace (E1) alcanzó dos Mbps. Ese mismo año, con la plena consolidación mundial de la WWW –la cual, con el correo electrónico, hoy es la herramienta de comunicaciones más empleada en Internet, dieron inicio las actividades

comerciales a través de Internet. También en ese año algunas empresas gestionaron los primeros dominios .com.mx.

A partir de 1995 dio inicio lo que puede considerarse como la segunda etapa del desarrollo de Internet en México. En octubre de ese año, el número de dominios com.mx ascendió a 100, rebasando por primera vez y de forma irreversible el número de dominios edu.mx, asignados a las instituciones educativas. Así, un mes después se anunció la creación del Centro de Información de Redes de México (NIC-México), instancia responsable de administrar y coordinar los recursos de Internet en México.

C) LAS REDES SOCIALES

Actualmente el fenómeno de las redes sociales ocupa un lugar importante en los principales usos del internet, pues este tipo de comunicación además de no tener frontera y mucho menos limitantes en distancia y tiempo, no distingue clases sociales, culturales e inclusive edades, lo cual deja en un punto muy vulnerable, sobre todo a quienes no están familiarizado con ello o no tienen los conocimientos básicos para el manejo o las posibles consecuencias del mal uso de una red social, lo cual puede llevar a ser víctima de una serie de delitos sin darse cuenta de ello y mucho menos saber la verdadera identidad del activo del delito.En su forma más simple, una red social es un mapa de todos los lazos relevantes entre todos los nodos estudiados. Se habla en este caso de redes "sociocéntricas" o "completas". Otra opción es identificar la red que envuelve a una persona (en los diferentes contextos sociales en los que interactúa); en este caso se habla de "red personal".

La red social también puede ser utilizada para medir el capital social (es decir, el valor que un individuo obtiene de los recursos accesibles a través de su red social).

MÉXICO Y LATINOAMÉRICA[15]

Para el 2011 el número de internautas a nivel mundial alcanzó los 1,374 millones, representando un crecimiento de 10%. Latinoamérica alcanzó un crecimiento del 14%, significando 118 millones de internautas respecto al mismo periodo de 2010.

México es segundo lugar de participación de audiencia en internet con 19%.

En el 2010 el número de internautas en México alcanzó los 34.9 millones.

A nivel mundial las visitas a Redes Sociales significaron un incremento del 22%, siendo las tres principales Redes Sociales visiitadas: Facebook, Twitter y Windows live profile.

Los visitantes Latinoamericanos en Redes Sociales significaron poco más de 115 millones de visitas. Las tres principales Redes Sociales más visitadas en Latinoamérica son: Facebook, Windows live Profile y Orkut.

El 86% de los Internautas Mexicanos visitan al menos un sitio de entretenimiento al mes y dedican 3.4 horas semanales en este tema.

El Internauta Mexicano dedica 10.6 horas al mes en sitios de video On line, colocándose en el primer lugar a nivel Latinoamérica.

El 61% de los Internautas en México accesan al menos a alguna Red Social, las mujeres acceden en mayor proporción que los hombres.

Las Redes Sociales más conocidas y utilizadas en México son: Facebook[16], Twitter[17]y Windows live profile.[18]

Es importante hacer mención de la llegada de Google plus[19], que es una red social con más aplicaciones multimedia y un acceso fácil que permite tener una mejor interacción entre usuarios, además de contar con todas las herramientas de Google, red social que ha puesto a temblar a Facebook.

---

[15] Juárez, Renato *Research* Director Elogia e Ivan Marchant *Country Manager Comscore. Las Redes sociales en México y Latinoamérica 2001,* Asociación Mexicana de Internet, elaborado por VP Investigación de Mercados, *http://www.amipci.org.mx/*

[16] *http://www.facebook.com*

[17] *http://www.twitter.com*

[18] *http://explore.live.com/windows-live-profile*

[19] *http:// www.plus.google.com*

Los Usos que el Internauta Mexicano le da a las Redes Sociales son: Comunicarse con amigos y/o familiares, seguimiento y opinión de contenidos sobre cultura, deportes y entretenimiento, de la misma manera seguimiento y opinión de las últimas noticias tanto nacionales como internacionales.

Casi el 40% de los Internautas en México se encuentran de acuerdo con la Publicidad dentro de las Redes Sociales, en contraste del 17% que les disgusta.

4 de cada 10 internautas han visto publicidad respecto a política dentro de las Redes Sociales.

3. ANTECEDENTES LEGISLATIVOS NACIONALES (INICIATIVAS DE LEY)

FECHA	**QUIEN LA PRESENTA**
7 de octubre de 2004	Grupo Parlamentario del PRI (LIX Legislatura)
Iniciativa que reforma el Código Penal Federal en materia de pornografía infantil, corrupción de menores, comunicación y correspondencia, revelación de secretos y acceso ilícito a sistemas y equipos de informática, falsificación de documentos en general, amenazas y revelación de datos personales, delitos en contra de las personas en su patrimonio; el Código Federal de Procedimientos Penales En el párrafo tercero del artículo 202, radica básicamente en imputar como conducta delictiva la reproducción de dicho material, sobre todo cuando dicho acto se realiza mediante la ejecución que se haga de los archivos de datos de una red pública o privada de telecomunicaciones o de sistemas de cómputo o electrónicos. "…estaría considerando *v. gr*. a todo individuo, que sin su consentimiento y por cuestión de haber leído un mensaje de correo electrónico no solicitado o *spam*, de cuyo contenido se anexa una video grabación o fotografía, o bien, se describan en su texto a manera de publicidad anuncios en los que se exhiba a una o varias personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas	

que no tienen capacidad para resistirlo. El delito de pornografía en agravio de cualquiera de esos sujetos pasivos, es decir, que el simple acto de *download* de una imagen o texto en el que encuentre una mínima referencia a la Pornografía Infantil, constituye en sí mismo un acto de *pedofilia*.

FECHA	**QUIEN LA PRESENTA**
30 de marzo de 2005	El Poder Ejecutivo Federal a la cámara de Diputados (LIX Legislatura)

Iniciativa de decreto que reforma y adiciona diversas disposiciones de la Ley Federal contra la Delincuencia Organizada, del Código Penal Federal, del Código Federal de Procedimientos Penales y de la Ley Orgánica del Poder Judicial de la Federación.[20]

La Iniciativa del Ejecutivo Federal, pretende exceptuar como delito a las comunicaciones privadas, las grabaciones o registro de sonidos o imágenes que realicen agentes infiltrados, informantes o testigos, así como víctimas u ofendidos, que participen directamente en la comunicación de que se trate, mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, y que dicha comunicación se relacione con miembros de la delincuencia organizada.

FECHA	**QUIEN LA PRESENTA**
29 de Junio de 2005[21] y miércoles 6 de julio de 2005.[22]	Grupo parlamentario del PRD (LIX Legislatura)

Iniciativa que adiciona un Capítulo al Título Vigésimo, Libro Segundo, del Código Penal Federal, con objeto de tipificar los delitos de inserción y divulgación de datos personales falsos.

[20] Gaceta Parlamentaria, número 1720-III, miércoles 30 de marzo de 2005, *http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/mar/Anexo-III-30mar.html.*

[21] Gaceta Parlamentaria, número 1789, lunes 4 de julio de 2005, *http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/jul/20050704.html.*

[22] Gaceta Parlamentaria, número 1793, viernes 8 de julio de 2005, *http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/jul/20050708.html.*

Iniciativa que adiciona un artículo 202 bis al Código Penal Federal y reforma la fracción V del artículo segundo de la Ley Federal contra la Delincuencia Organizada, con el objeto de tipificar el delito de utilización o facilitación de medios de comunicación para obtener contacto sexual con personas menores de 18 años de edad. La Iniciativa que reforma el Código Penal Federal, en materia de Delitos Informáticos, a través de ella, sugiere se adicionen los artículos 246 Bis, 254 Quáter, 381 Ter y 389 Ter, con objeto de tipificar los delitos de falsificación informática, robo informático, fraude informático y oferta informática engañosa.[23]

FECHA	**QUIEN LA PRESENTA**
21 de febrero de 2006.	Grupo parlamentario del PRI (LIX Legislatura)
Proyecto de decreto para reformar y adicionar el artículo 201 Bis del Código Penal Federal, para quedar como sigue: Artículo 201 Bis. Al que procure o facilite por cualquier medio que uno o más menores de dieciocho años, con o sin su consentimiento lo(s) obligue o induzca(n) a realizar actos pornográficos, de exhibicionismo, lascivos, obscenos o sexuales para videograbarlos, fotografiarlos o mostrarlos a través de medios impresos, electrónicos, archivo de datos, Internet o cualquier otro mecanismo similar, con o sin interés de lucro, se le impondrá de cinco a quince años de prisión y de mil a cinco mil días multa….	

FECHA	**QUIEN LA PRESENTA**
07 de Marzo de 2006.	Grupo parlamentario del PAN (LIX Legislatura)
Proyecto de decreto Artículo Único. Se adiciona un Capítulo III al Título Quinto del Libro Segundo, denominado "Uso Indebido de la Red de Telecomunicaciones en lo Referente a la Pornografía", así como un artículo 177 Bis, ambos del Código Penal Federal, para quedar como sigue: Capítulo III Uso Indebido de la Red de Telecomunicaciones en lo Referente a la	

[23] Gaceta Parlamentaria, número 1804, lunes 25 de julio de 2005, *http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/jul/20050725.html*.

Pornografía. Artículo 177 Bis. A quien, con el fin de lucro o sin él, y haciendo uso de cualquier instrumento, medio o equipo informático, electrónico o de cualquier otra naturaleza, transmita, otorgue el acceso, envíe o distribuya a través de la red de telecomunicaciones imágenes, medios audiovisuales o sus representaciones digitales de actos a que hacen referencia los artículos 200 y 201 Bis del Código Penal Federal, se le impondrá de cinco a diez años de prisión y de mil a dos mil días multa.

FECHA	**QUIEN LA PRESENTA**
29 de Noviembre de 2011.	Grupo parlamentario del PVEM

Iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones al Código Penal Federal, en Materia de Delitos en contra de medios o sistemas Informáticos o cometidos mediante el uso o empleo de los mismos. Capítulo I Revelación de Secretos Artículo 211 Bis. Se impondrán las mismas penas que refiere el párrafo anterior a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información, conversaciones o mensajes de texto, imágenes o archivos de voz, contenidos en sistemas o equipos informáticos, obtenidos a través de mecanismos distintos a la intervención de comunicación privada, mediante el empleo de aparatos o dispositivos electrónicos fijos o móviles o a través de la suplantación de identidad. Capítulo II Acceso Ilícito a Sistemas y Equipos de Informática Artículo 211 Bis 1. Se aplicará una pena de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización acceda, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática que no estén protegidos por algún mecanismo de seguridad o también sin autorización acceda a dichos sistemas o equipos de informática o mediante cualquier mecanismo que de manera próxima o remota les cause un daño. En los casos en que el daño provocado por el acceso o la modificación no autorizados obstaculice o disminuya la capacidad de funcionamiento del sistema o equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes. 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 seis meses a dos años de prisión y de cien a trescientos días multa.

La pena aplicable será de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización conozca o copie información contenida en sistemas o equipos de informática no protegidos por algún mecanismo de seguridad. Artículo 211 Bis 2. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad o también sin autorización acceda a dichos sistemas o equipos informáticos o mediante cualquier mecanismo que de manera próxima o remota les cause un daño, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización, conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad o también sin autorización acceda a dichos equipos o medios o mediante cualquier mecanismo les cause un daño, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. En los casos en que el daño provocado por el acceso o la modificación no autorizados o por cualquier mecanismo empleado obstaculice o disminuya la capacidad de funcionamiento del sistema o equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes "…

FECHA	**QUIEN LA PRESENTA**
29 de Noviembre de 2011.	Grupo parlamentario del PVEM Diputados Juan José Guerra Abud y Rodrigo Pérez-Alonso González
La presente iniciativa propone adicionar y reformar diversos artículos al Código Penal Federal en materia de Delitos Informáticos, a fin de adecuar las disposiciones del orden jurídico a las exigencias que impone el avance tecnológico y la condición social actual de nuestro país, en materia de dichos ilícitos. [24]Titulo Noveno Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática. Capítulo I Revelación de Secretos Artículo 211 Bis. A quien revele,	

[24]Gaceta Parlamentaria No. 61, *http://gaceta.diputados.gob.mx/Gaceta/61/2011/nov/20111129-V.html*

divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa. Se impondrán las mismas penas que refiere el párrafo anterior a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información, conversaciones o mensajes de texto, imágenes o archivos de voz, contenidos en sistemas o equipos informáticos, obtenidos a través de mecanismos distintos a la intervención de comunicación privada, mediante el empleo de aparatos o dispositivos electrónicos fijos o móviles o a través de la suplantación de identidad. Capítulo II Acceso Ilícito a Sistemas y Equipos de Informática Artículo 211 Bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Se aplicará una pena de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización acceda, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática que no estén protegidos por algún mecanismo de seguridad o también sin autorización acceda a dichos sistemas o equipos de informática o mediante cualquier mecanismo que de manera próxima o remota les cause un daño. En los casos en que el daño provocado por el acceso o la modificación no autorizados obstaculice o disminuya la capacidad de funcionamiento del sistema o equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes. 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 seis meses a dos años de prisión y de cien a trescientos días multa. La pena aplicable será de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización conozca o copie información contenida en sistemas o equipos de informática no protegidos por algún mecanismo de seguridad. Artículo 211 Bis 2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad o también sin autorización acceda a dichos sistemas o equipos informáticos o mediante

cualquier mecanismo que de manera próxima o remota les cause un daño , se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización, conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad o también sin autorización acceda a dichos equipos o medios o mediante cualquier mecanismo les cause un daño, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. En los casos en que el daño provocado por el acceso o la modificación no autorizados o por cualquier mecanismo empleado obstaculice o disminuya la capacidad de funcionamiento del sistema o equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes. Artículo 211 Bis 4. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas establecidas en los párrafos anteriores se incrementarán hasta en dos terceras partes y se impondrán sin perjuicio de las que resulten aplicables por la comisión de otros delitos al que realice, para beneficio propio o de cualquier tercero, las conductas que describen los párrafos anteriores con la finalidad de realizar o encubrir las operaciones con recursos de procedencia ilícita a que se refiere el párrafo primero del artículo 400 Bis de este ordenamiento. Artículo 211 Bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a

dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. Las penas establecidas en los párrafos primero y segundo de este artículo se incrementarán hasta en dos terceras partes y se impondrán sin perjuicio de las que resulten aplicables por la comisión de otros delitos al que realice, para beneficio propio o de cualquier tercero; las conductas que describen los párrafos anteriores con la finalidad de realizar o encubrir las operaciones con recursos de procedencia ilícita a que se refiere el párrafo segundo del artículo 400 Bis de este ordenamiento. Artículo 211 Bis 6. Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código. Artículo 211 Bis 7. Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno, salvo en los casos que se disponga otra pena. Titulo Decimoctavo. Delitos contra la Paz y Seguridad de las Personas.

Estas iniciativas permiten concluir que desde el año 2004 se ha pretendido desarrollar medidas respecto de la seguridad informática, cuyo propósito es mantener la integridad de las tecnologías y sistemas de información; de igual forma, legislar sobre las conductas de reproducción y uso de los mismos que tiene como finalidad el producir la conducta ilícita, una vez cometida ésta, encontrarse en posibilidad de penalizarla.

Cabe hacer mención de que existe un reducido grupo de iniciativas respecto del tema; motivo por el cual, es imprescindible contar con una legislación al respecto, mediante la creación de un nuevo ordenamiento jurídico, o bien, integrar modificaciones al ya existente que contemple el tema de derecho cibernético, delitos cibernéticos y uso de tecnologías de información y comunicación.

De ahí la relevancia de contar con un dicho ordenamiento jurídico para implantar esquemas de seguridad informática que penalice las prácticas ilícitas que se llevan a cabo en materia de pornografía infantil, uso de datos personales

y delincuencia organizada, por citar algunos de los delitos cometidos con mayor frecuencia a través de las *TICs*.

Las iniciativas citadas en párrafos anteriores no representan una opción para encontrarnos en posibilidades de sancionar o penalizar, toda vez que la última iniciativa de ley en la materia contempla adiciones a tipos penales ya existentes; no así la creación de ley particular aplicable a la materia o un capítulo exclusivo para los delitos informáticos.

4. JURISPRUDENCIAS Y TESIS AISLADAS

Debido al avance constante y sobre todo veloz de la tecnología, así como las consecuencias que con ello conlleva para la aparición de nuevas formas de cometer delitos a través de esta, es necesario crear instrumentos legales para la defensa de estas conductas o medios que de manera general que permitan la protección del daño o menoscabo en nuestro patrimonio o persona, mientras esto no suceda seguirán emitiéndose jurisprudencias y tesis aisladas que ayuden a ocultar las deficiencias de la legislación en materia de delitos informáticos.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL CUARTO CIRCUITO.[25] FRAUDE COMETIDO MEDIANTE EL USO DE COMPUTADORAS. Si el inculpado asentó en la computadora instalada en el banco un depósito ficticio para ser abonado en la cuenta de ahorros que abrió a nombre de su coacusado, es evidente que el empleo de la computadora por el inculpado resultó un medio de comisión del fraude en esta época de la electrónica, pues al crear una falsa concepción de la realidad, con el propósito de alcanzar un beneficio económico, determinó la existencia del engaño constitutivo de dicho delito.

[25] Queja 39/2005. Cervezas Cuauhtémoc Moctezuma, S.A. de C.V.. Ponente: José Carlos Rodríguez Navarro. Secretaria: Rebeca del Carmen Gómez Garza. 4 de mayo de 2005. Unanimidad de votos.

TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO.[26] PRUEBA DE INSPECCIÓN. DEBE DESECHARSE CUANDO LOS PUNTOS PROPUESTOS PARA SU DESAHOGO PUEDAN SER COMPROBADOS A TRAVÉS DE LA DOCUMENTAL, ENTENDIDA COMO LA INFORMACIÓN GENERADA O COMUNICADA QUE CONSTE EN MEDIOS ELECTRÓNICOS O EN CUALQUIER OTRA TECNOLOGÍA, QUE PUEDE SER REPRODUCIDA, NO SOLAMENTE EN PAPEL SINO TAMBIÉN EN ALGÚN DISQUETE O DISCO ÓPTICO. La base de datos existente en el sistema de cómputo de alguna dependencia oficial, constituye, en sentido amplio, una documental, atendiendo a que el artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, por disposición de su artículo 2o., segundo párrafo, señala que se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIAS PENAL Y ADMINISTRATIVA DEL VIGÉSIMO PRIMER CIRCUITO.[27] INFORMACIÓN PROVENIENTE DE INTERNET. VALOR PROBATORIO. El artículo 188 del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, en términos de lo previsto en el diverso artículo 2o. de este ordenamiento legal, dispone: "… reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquiera otra tecnología; ahora bien, entre los medios de comunicación electrónicos se encuentra "internet", que constituye un sistema mundial de diseminación y obtención de información en diversos ámbitos y, dependiendo de esto último, puede determinarse el carácter oficial o extraoficial de la noticia que al efecto se recabe, y como constituye un adelanto de la ciencia, procede, en el aspecto normativo, otorgarle valor probatorio idóneo.

[26] Amparo directo 344/78. Rogelio Mendoza Reséndiz. . Ponente: Víctor Manuel Franco. La publicación no menciona la fecha de resolución del asunto. Unanimidad de votos.

[27] Queja 39/2006. Inversiones Raf, S.A. de C.V Ponente: Martiniano Bautista Espinosa. Secretario: Mario Alejandro Nogueda Radilla. . 29 de junio de 2006. Unanimidad de votos.

TERCER TRIBUNAL COLEGIADO DEL QUINTO CIRCUITO.[28] INTERNET. ES UNA MEDIDA PERTINENTE PARA INVESTIGAR EL DOMICILIO DE LA TERCERA PERJUDICADA SI SE TRATA DE UNA EMPRESA CUYOS DATOS SE LOCALICEN POR ESE MEDIO. Según la fracción II del artículo 30 de la Ley de Amparo, si no consta en autos el domicilio del tercero perjudicado, la autoridad que conozca del amparo dictará las medidas que estime pertinentes para investigar su domicilio. "…Por su parte, el artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, reconoce como prueba la información generada o comunicada a través de medios electrónicos.." Por lo tanto, una de las medidas pertinentes que puede dictar la autoridad federal para localizar el domicilio de la parte tercera perjudicada, si se trata de una empresa cuya localización no conste en autos, es la de efectuar su búsqueda por internet a través de las diversas páginas que ofrecen dicho servicio, donde basta introducir el nombre de la empresa que se pretende localizar y en breve se despliega información de la que puede obtenerse la forma para contactar con dichas empresas y en algunos casos también proporcionan sus domicilios.

SÉPTIMO TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO.[29] REVELACIÓN DE SECRETOS. EL DELITO PREVISTO EN EL ARTÍCULO 211 BIS DEL CÓDIGO PENAL FEDERAL, ES DE PELIGRO Y DE RESULTADO. Del citado precepto se advierte que el delito de revelación de secretos corresponde a una mezcla de la categoría de los denominados delitos de peligro, en una parte, y en otra, se inscribe dentro de la clase de los de resultado, ya que el elemento normativo "o en perjuicio de otro", se establece como disyuntiva del también elemento normativo "indebidamente"; lo cual significa que a falta de éste, para que se configure el delito, debe darse aquel requisito de perjuicio como necesaria existencia de un daño, de un menoscabo o

[28] Amparo en revisión 257/2000. Bancomer, S.A., Institución de Banca Múltiple, Grupo Financiero. .Ponente: Epicteto García Báez. 26 de junio de 2001. Unanimidad de votos.

[29]Queja 19/2009 Disidente: Manuel Ernesto Saloma Vera. Ponente: Julio César Vázquez-Mellado García. Secretario: Benjamín Garcilazo Ruiz. 21 de mayo de 2009. Mayoría de votos.

detrimento en los bienes morales o materiales del ofendido, por revelación, divulgación o utilización de la información o imágenes obtenidas en una intervención de comunicación privada. Es decir, se considerará conducta ilícita el solo hecho de revelar, difundir o utilizar indebidamente la información, pero también se admite como ilícito una forma de comisión material, al prever el posible perjuicio a alguien por dicha conducta.[30]

REVELACIÓN DE SECRETOS. EL ARTÍCULO 211 BIS DEL CÓDIGO PENAL FEDERAL QUE TIPIFICA ESE DELITO, NO VIOLA LA GARANTÍA DE EXACTA APLICACIÓN DE LA LEY PENAL CONTENIDA EN EL TERCER PÁRRAFO DEL ARTÍCULO 14 DE LA CONSTITUCIÓN FEDERAL. Conforme a la garantía de exacta aplicación de la Ley Penal prevista en el citado precepto constitucional. "… En congruencia con lo anterior, el artículo 211 bis del Código Penal Federal, al tipificar el delito de revelación de secretos señalando que a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada … no viola la citada garantía constitucional en virtud de que el vocablo "indebidamente", empleado en dicho precepto legal, no provoca confusión; en primer lugar, porque es posible precisar su significado a través de su concepto gramatical y, en segundo, porque su sentido puede fijarse desde el punto de vista jurídico y determinar cuándo la conducta es indebida para poder considerarse delictuosa…"[31] .

El material resulta insuficiente, si bien en cuanto a criterios jurisprudenciales ha existido un avance vertiginoso, la legislación de la materia aplicable no cuenta con tal denominación respecto al tema.

Situación alarmante toda vez que, atendiendo a los principios generales del derecho *"Nullum crimen sine lege", "Nulla poena sine crimine"* estas conductas

[30] Amparo en revisión 534/2005. Ponente: Juan N. Silva Meza. Secretario: Manuel González Díaz. 22 de junio de 2005. Cinco votos.

[31] Amparo en revisión 534/2005. Ponente: Juan N. Silva Meza. Secretario: Manuel González Díaz. 22 de junio de 2005. Cinco votos.

ilícitas se llevan a cabo al margen de la ley, y no pueden ser penalizadas en su totalidad como un conjunto de acciones tendientes a la producción del delito mediante conductas dolosas creadas por agentes que cuentan con un conocimiento especializado del tema.

Es indispensable dar al tema la importancia jurídica correspondiente, ya que con los insuficientes criterios jurisprudenciales anteriormente citados, no es posible cubrir la totalidad de los casos que a diario se presentan y de los cuales existe una casi nula incidencia de denuncia, porque no pueden ser formalmente punibles, toda vez, que la ley no los contempla, aunado al desconocimiento de la gente en la materia y la poca denuncia de estos delitos realizados a través de los medios informáticos en mención.

CAPÍTULO II

LOS DELITOS INFORMÁTICOS EN EL PLANO INTERNACIONAL

1.- LEYES EXTRANJERAS QUE PRESCRIBEN LOS DELITOS INFORMÁTICOS

En relación a la afinidad de las legislaciones es sumamente importante, ya que un gran número de países fundamenta su régimen de asistencia judicial mutua en el principio de la doble incriminación, según el cual un delito debe ser considerado como tal tanto en el Estado que solicita la asistencia como en el que la presta.[32]

La realidad de México en relación a los delitos informáticos es nueva, y se han llevado a cabo una serie de instrumentos internacionales mejor llamados acuerdos de colaboración o convenios, los cuales no obligan a dar cumplimiento cabal de lo plasmado en ellos, además de existir una serie de legislaciones ya sean locales o federales que tipifican algunos delitos informáticos, pero no hay en si una ley concreta al caso, como en otros países, por lo que a continuación se hace un análisis de derecho comparado de los países que al parecer han tenido un avance en la creación de legislaciones y que permiten como se ha actuado en relación a algunos casos de importante relevancia.

En 1986, la aprobación de la ley de privacidad de comunicaciones electrónicas *(Electronic Communication Privacy Act,* por sus siglas en Ingles*)* en Estados Unidos marcó la primera vez que específicamente se había promulgada una pieza importante de legislación para el mandato de restricciones en el uso de equipos. Fue un momento histórico, no sólo para ese país, sino para todo el mundo. En los años que siguieron tras el paso de la ECPA, muchas agencias federales desde el FBI y el servicio secreto comenzaron a aplicar este y otros actos legislativos, tratando de acabar en la nueva ola de delitos informáticos.

---

[32] En lo que respecta al principio de la doble incriminación en las investigaciones de delitos cibernéticos, véanse el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos
Revista Internacional de Política Criminal, Núms. 43 y 44
Publicación de las Naciones Unidas, Núm. de venta S.94.IV.5), p.269
Documento de antecedentes de Stein Schjølberg y Amanda Hubbard titulado *"Harmonizing national legal approaches on cybercrime"*, p.5.

Mucho ha sido escrito y hecho para mejorar la viabilidad de represión de delitos electrónicos. El FBI tiene ahora una red de escuadrones de delitos informáticos. El departamento de Justicia ha establecido un conjunto de directrices en el que se esbozan procedimientos para aprovechar y buscar equipos. Incluso la población general estadounidense en su conjunto es ahora más educada sobre delitos informáticos, y por lo general muchos saben qué hacer para protegerse a sí mismos.

Lo que se pierde en este marco legal, sin embargo, que es el Internet, así como los delitos de Internet se extienden mucho más allá de las fronteras de los Estados Unidos. De acuerdo con InterGov internacional, 39 por ciento del tráfico de Internet se genera fuera de los Estados Unidos. Además, una Comisión de las Naciones Unidas de 1991 sobre delincuencia y justicia penal llegó a la conclusión de que en la encuesta de 3000 sitios de extensiones de dirección Virtual en decenas de países, más de 72 por ciento comunicaron un incidente de seguridad dentro de los últimos 12 meses. Claramente, la aplicación de la ley en la frontera electrónica no es sólo un problema estadounidense. [33]

A) FAMILIA JURÍDICA COMMON LAW

Australia

La Ley de Telecomunicaciones de 1991 y las secciones básicamente añadidas 74 y 76 del Código Penal australiana. Sección 74, describe las definiciones de transportista y datos.

El Gobierno de Australia ha presentado nuevas leyes con las que combatir de manera más eficaz la delincuencia en Internet[34], al hilo de los últimos ciberataques contra empresas multinacionales e instituciones públicas, como Google, el Fondo Monetario Internacional y el Senado de Estados Unidos.

En una ocasión, la red informática del Parlamento se vio afectada por uno de estos ataques. "La creciente amenaza cibernética significa que ninguna nación por sí sola puede superar eficazmente este problema y la cooperación

[33] J. Katz PhD David L. Carter PhD and Adra, "*Computer Crime : An Emerging Challenge for Law Enforcement*," 12/96, *http://www.fbi.gov/leb/dec961.txt*

[34] Reuters | EP | Camberra Actualizado miércoles 22/06/2011

internacional es esencial", añade el fiscal. Más requisito de almacenamiento. Estas leyes, ya aprobadas por el Parlamento, permitirán que la Policía y los servicios de Inteligencia obliguen a las empresas de telecomunicaciones a mantener en sus archivos información relevante.

Austria

La Ley de reforma del Código Penal de 22 de diciembre de 1987 contempla los siguientes delitos: Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas. Estafa informática (148).

Canadá

Su integración económica con los Estados Unidos ha creado una red informática y la comunidad de Internet muy dependiente a la de su vecino país del sur, junto con esta tecnología, sin embargo, también han llegado delitos informáticos tanto de Estados Unidos, así como desde el interior. Canadá, ha observado muy de cerca la proliferación de delitos informático y no ha tardado en la aplicación de medidas legislativas para corregir tal proliferación para que no le afecte, junto con una aplicación bien definida y una estructura de mando han dado a Canadá una tasa de éxito casi inigualable en el trato con la piratería. El Gobierno canadiense ha sido muy agresivo en aplicación de la legislación de los delitos informáticos. Existen básicamente dos secciones del Código Penal canadiense, secciones 342.1 y 430 que lidian más con delitos informáticos. Sección 342.1 está dividida en dos partes. En Canadá la definición de los Delitos informáticos se ha tomado de la comunidad internacional Convenio sobre la Ciberdelincuencia que se produjo el 23 de noviembre de 2001. Canadá ha contribuido, y es signatario, a este convenio internacional de los delitos que implican el uso de los ordenadores: los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, los delitos relacionados con la informática, delitos relativos al contenido, los delitos relacionados con infracciones de derechos de autor y derechos conexos, y la

responsabilidad auxiliar. La Ley de Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos son: el acceso ilegal, la intercepción ilegal, la interferencia de datos, la interferencia del sistema, mal uso de los dispositivos. Los delitos relacionados con la informática son: falsificación y el fraude relacionados con la informática, delitos relacionados con Pornografía infantil, los relativos a la violación de los derechos de autor y derechos conexos, y los derechos digitales, los delitos de responsabilidad auxiliar incluyen cosas como la tentativa, la complicidad y la responsabilidad corporativa. El robo, la falsificación de tarjetas de crédito y el uso no autorizado del equipo está regulado por la Sección 342. La privacidad está regulada por el artículo 184 y la suplantación de la sección 403, también algunos de los crímenes están reguladas con la Ley C-46.

Estados Unidos

Es importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya, etcétera y en que difieren de los virus. Define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudente la sanción fluctúa entre una multa y un año en prisión.

Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

Puede hallarse un ejemplo de este enfoque legislativo en los § 517(a) y (b) del 17 U.S.C. (Código de los Estados Unidos).

Mediante la creación de un régimen de protección, la DMCA exceptúa de responsabilidad a los proveedores de ciertos servicios por violaciones de derechos de autor cometidas por terceros. En este contexto, es importante en

primer lugar poner de relieve que no todos los proveedores están abarcados en la limitación. Las limitaciones de responsabilidad se aplican únicamente a proveedores de servicio y proveedores de sistemas de almacenamiento especial[35].

CÓDIGO DE ESTADOS UNIDOS[36]. La sección 1030. Fraude y otras actividades conexas relacionadas con las computadoras.(A) El que a sabiendas acceso a una computadora sin autorización o excediendo el acceso autorizado, y por medio de dicha conducta con la información obtenida que ha sido determinado por el Gobierno de Estados Unidos en virtud de una Orden Ejecutiva o los estatutos que requieren una protección contra el uso no divulgación por razones de defensa nacional o las relaciones exteriores, o cualquier otra información restringida.

Reino Unido

Básicamente son dos leyes relativas a la utilización de equipo superior que han sido aprobados por el Gobierno británico, estas son la ley de protección de datos de 1984 y la ley de uso indebido de equipo de 1990. La primera trata generalmente de la adquisición y uso de datos personales, mientras que la segunda ley define los procedimientos y sanciones que rodean la entrada no autorizada en los equipos.

[35] 17 U.S.C. § 512(b).

[36] Sección de Delitos Informáticos y Propiedad Intelectual, *http://www.justice.gov/criminal/cybercrime/*

CAPÍTULO DE LA LEY DE LA POLICÍA Y LA JUSTICIA 2006 MODIFICA LA LEY DE USO INDEBIDO DE ORDENADORES[37]

El acceso no autorizado a material informático: "Una persona culpable de una ofensa bajo esta sección será responsable, (a) en juicio sumario en Inglaterra y Gales, de prisión por un término no superior a 12 meses o una multa que no exceda el máximo legal, o ambas; (b) por condena sumaria, en Escocia, a una pena de prisión no superior a seis meses o una multa que no exceda el máximo legal o tanto, (c) en caso de condena en la acusación, a una pena de prisión no superior a dos años o una multa, o ambas ". Para la sección 3 de la Ley de 1990 (modificación no autorizada de material informático) es sustituido "tres actos no autorizados con la intención de perjudicar, o con temeridad en cuanto a alterar, el funcionamiento del equipo, etc.

B) FAMILIA JURÍDICA ROMANO-GERMÁNICA

Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos: Espionaje de datos (202 a), Estafa informática (263 a) Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271, 273) Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.

Sabotaje informático (303 b. Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

[37] Las enmiendas entraron en vigor nuevas el 1 de octubre de 2008, *http://www.legislation.gov.uk/ukpga/2008*

Utilización abusiva de cheques o tarjetas de crédito (266b).

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

El gobierno de Alemania en 20 de septiembre 2006 propuso un nuevo proyecto de Ley Sobre el Delito Cibernético con el objetivo de cerrar las lagunas restantes. En su Código Penal vigente[38] penaliza todas aquellas conductas ilícitas respecto al manejo de datos de espionaje, alteración de los datos y el sabotaje informático.

Italia

La legislación de ese tipo está contenida en la sección de código italiano 547, que fue aprobada en diciembre de 1993 como parte de un proyecto de ley más grande, básicamente fueron doce puntos en el proyecto de ley. Cuatro de los puntos de tratan de la posesión, alteración o destrucción de sistemas de datos o equipo. Otros cuatro establecen sanciones para el acceso no autorizado o pirateado en sistemas y posterior intercepción de comunicaciones, que conllevan una pena máxima de seis años. Los cuatro últimos puntos fueron más diversos en su naturaleza, uno analiza el crimen interceptar una transmisión electrónica, otro prohíbe la difusión de virus informáticos en la red, la tercera hace ilegal la posesión de dispositivos para interceptar o interrumpir las comunicaciones, el punto final es probablemente el más intrigante, el cual establece penas más duras para la divulgación de información a otro sin buena causa.[39]

[38] Texto completo *http://www.gesetze-im-internet.de/stgb/index.html*

[39] Italian Computer Crime Law, *http://www.clarence.com/home/diritto/Comment2.htm*

El Senado del Parlamento italiano el 27 de febrero (2008) y aprobada ratificada la Convención sobre el Delito Cibernético[40].

Del Código Penal el artículo 615 ter: El acceso no autorizado a una computadora o sistemas de telecomunicaciones:

España

La Ley de servicios de la sociedad de la información y del comercio electrónico[41] tiene como objeto la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica.

El artículo 2 de la Ley 34/2002 de 11 de Julio, de servicios de la sociedad de la información y de Comercio Electrónico establece el ámbito de aplicación subjetivo de la ley a los prestadores de servicios establecidos en España.

Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático. Tales como el acceso fraudulento a un sistema de elaboración de datos (462-2) y el Sabotaje informático (462-3).- Así como el uso de documentos informatizados falsos (462-6). La ratificación del Consejo de Europa sobre la ciberdelincuencia se hizo el 10 de enero de 2006.

Venezuela

En el año 2001 se promulgó la Ley Especial contra los delitos Informáticos por Asamblea Nacional de la República Bolivariana de Venezuela. De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información, De los Delitos Contra la Propiedad, De los delitos contra la privacidad de las personas y de las comunicaciones, De los delitos contra niños, niñas o adolescentes, De los delitos contra el orden económico, argumentados en cinco capítulos respectivamente.[42]

[40] Texto completo *http://www.ictlex.net/wp-content/s2012.pdf*

[41] Texto completo *http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf*

[42] Ley Especial sobre los Delitos Informáticos de Venezuela de 2001, texto completo *http://www.tsj.gov.ve/legislacion/ledi.htm*

C) FAMILIA JURÍDICA ASIÁTICA

Japón

En efecto a partir del 03 de febrero 2000 mediante la Informática Ley de Acceso no autorizado. Además se cuenta con el Convenio sobre Ciberdelincuencia, firmado desde 2004 por 31 países, exige a las partes criminalizar el acceso no autorizado a sistemas informáticos, el almacenamiento de pornografía infantil o la vulneración de derechos de autor.

Tokio.- El Parlamento japonés aprobó hoy una ley que criminaliza la creación y distribución de virus informáticos, pese a las voces críticas que sostienen que podría infringir el derecho constitucional que garantiza la privacidad en las comunicaciones. Las autoridades niponas han tenido problemas para investigar ataques cibernéticos contra oficinas gubernamentales, corporaciones o individuos ante la ausencia de una ley nacional específicamente trazada para castigar la creación de virus y otros actos que dañen redes informáticas.

Con la aprobación de la ley, el Gobierno nipón tiene la intención de suscribir definitivamente el Convenio sobre Ciberdelincuencia que, pese a ser aprobado por el Parlamento en 2004, no fue oficialmente ratificado ante la ausencia de normas de ámbito local en este terreno.

D) FAMILIA JURÍDICA SOCIALISTA

China

Sin duda llegará un punto donde China debe establecer normas para regular su creciente electrónica y la industria informática. Sólo cabe esperar que esa legislación no dé como resultado la persecución opresiva de la población.[43]

El Ministerio de Industria de la Información (Departamento de Políticas, Leyes y Reglamentos) es una de las principales instituciones en la reforma de la ley vigente desde 1996.

[43] China Field of Electronic Frontier Foundation, *http://www.eff.org/pub/Global/China/*

Derecho Penal de la República Popular de China (14 de marzo de 1997) establece lineamientos para el uso de una computadora para el fraude financiero, robo, corrupción, malversación de fondos públicos, el robo de secretos de Estado, o de otros delitos castigados conforme a las disposiciones pertinentes de esta ley.

E) FAMILIA JURÍDICA SUPRANACIONAL

Unión Europea

Los poderes de la Unión Europea son limitados cuando se trata de legislar en la esfera del derecho penal. En efecto, la Unión sólo tiene la posibilidad de armonizar el derecho penal de los Estados Miembros en esferas especiales, tales como la protección de los intereses financieros de la Unión Europea y el ciberdelito[44].

En 1999 la Unión Europea lanzó la iniciativa "eEurope", adoptando la Comunicación de la Comisión Europea "e-Europa – Una sociedad de la información para todos". En 2000 el Consejo Europeo adoptó un "Plan de Acción e-Europa" detallado y pidió que se tradujese a la práctica antes de fines de 2002.

En 2001 la Comisión Europea publicó una Comunicación que versaba sobre la creación de una sociedad de la información más segura, mejorando la seguridad de las estructuras de la información y luchando contra el ciberdelito[45].

Tras participar en el Consejo de Europa y en los debates del G8, la Comisión reconoce la complejidad y dificultad que plantean las cuestiones de procedimiento jurídico. En la decisión mencionada se toma nota de que el Convenio sobre la Ciberdelincuencia del Consejo de Europa se concentra en la armonización de las disposiciones del derecho penal sustantivo tendentes a proteger los elementos de las infraestructuras.

---

[44] En cuanto a la legislación en materia de delito cibernético abuso de la informática y la reden los países de la UE, véase: Baleri / Somers / Robinson / Graux / Dumontier, Manual de Procedimientos Legales del uso indebido de la red de ordenadores en los países de la UE de 2006.

[45] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y El Comité de las Regiones - Creación de una Sociedad de la Información más segura mediante la mejora de la seguridad de las infraestructuras de información 26.1.2001, COM (2000) 890.

En cada una de las familias existe un avance por cuanto hace a legislación, preponderando la penalización del acceso ilegal a información gubernamental o de uso exclusivo del Estado o Gobierno como es el caso de los Estados Unidos Norteamericanos, Reino Unido, Japón y China; a la par en países como Italia, Alemania y España se ha logrado legislar sobre el acceso no autorizado a datos informáticos entre particulares, penando estas conductas ilícitas llevadas a cabo con el propósito de delinquir.

Con ello se logra una regulación de los bienes informáticos, la protección de datos personales, la protección de la información exclusiva para el uso del Gobierno, garantizando leyes que contienen prohibiciones, limites derivados de ordenamientos en su mayoría en materia penal que contienen conductas previstas y sancionadas, previniendo este tipo de conductas ilícitas y conflictos sociales derivados de ellas.

En México el Capítulo II Segundo, Titulo IX Noveno del Código Penal Federal del "Acceso ilícito a sistemas y equipos de informática" protege y penaliza la información gubernamental, financiera y de seguridad pública restringida del Estado, cito "artículo 211 bis 2: "Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán …"; sin tomar en cuenta la protección a la seguridad del manejo de información por parte de los particulares.

2. ORGANISMOS E INSTRUMENTOS INTERNACIONALES EN MATERIA DE COMBATE DE LOS DELITOS INFORMÁTICOS

El crimen organizado ha ido en aumento operando con ataques masivos a empresas, instituciones públicas o de manera individual a niveles internacionales de manera rápida sirviéndose de la aparición y mayor alcance, así como de los beneficios del internet, que nulifica la barrera de espacio y tiempo entre los países.

Esto se debe al hecho de que las lagunas en la legislación internacional y regional siguen siendo todavía mayores, por lo que es difícil hacer un seguimiento eficaz a los delincuentes. El principal problema es la falta de armonización internacional en materia de legislación los delitos cibernéticos. La Investigación y el enjuiciamiento son difíciles, si la clasificación de los delitos varía de país a país. Algunos de los esfuerzos para hacer frente a este reto se han realizado, y aunque muy valiosa, que siguen siendo insuficientes. El Internet es una herramienta de comunicación internacional y por lo tanto, cualquier solución para asegurarlo debe buscarse a nivel mundial.

El G8[46]

En 1997 el Grupo de los Ocho (G8) estableció un Subcomité[47] sobre delitos de alta tecnología, cuyo objetivo era luchar contra el ciberdelito[48]. Durante la

[46] El Grupo de los Ocho (G8) se compone de ocho países: Canadá, Francia, Alemania, Italia, Japón, Gran Bretaña, Estados Unidos y la Federación Rusa. La Presidencia del grupo que representa a más del 60% de la economía mundial.

[47] La idea de la creación de cinco subgrupos - entre ellos, uno en delitos de alta tecnología -fue para mejorar la aplicación de las cuarenta recomendaciones adoptados por los Jefes de Estado del G8 en 1996.

[48] El establecimiento del Subgrupo (también descrito como el Subgrupo del "Grupo de Lyon") continuó los esfuerzos del G-8 (en ese momento todavía G7) en la lucha contra el crimen organizado, que se inició con el lanzamiento del Grupo de Expertos de Alto Nivel sobre los Crímenes Organizados (el "Grupo de Lyon") en 1995. En la cumbre de Halifax en 1995 del G8 expresaron:"Reconocemos que el éxito final requiere que todos los gobiernos establezcan medidas efectivas para prevenir el blanqueo de capitales procedentes del tráfico de drogas y otros delitos graves. Para llevar a cabo nuestros compromisos en la lucha contra la delincuencia organizada transnacional, hemos establecido un grupo de expertos de alto nivel con un mandato temporal para ver los arreglos existentes para la cooperación tanto bilateral como multilateral, para identificar lagunas importantes y las opciones para mejorar. coordinación y proponer acciones concretas para colmar esas lagunas". Ver: Declaración del Presidente, la Cumbre del G-7 en Halifax, 17 de junio de

reunión del G8, celebrada en Washington D.C., Estados Unidos, los Ministros de Justicia y del Interior del G8 adoptaron **Diez Principios y un Plan de Acción de diez puntos para combatir el delito de alta tecnología**. Los Jefes de Estado apoyaron ulteriormente estos principios, entre los cuales cabe citar lo siguiente:

"No puede haber refugios para aquellos que utilizan de forma abusiva las tecnologías de la información; todos los Estados interesados habrán de investigar la comisión de delitos internacionales de alta tecnología, así como el enjuiciamiento de sus autores, con independencia del cual sea el país en el que se hayan producido los correspondientes daños, entre otros."

En 1999 el G8 especificó la actuación que tenía prevista para luchar contra el delito de alta tecnología en la Conferencia Ministerial sobre la **Lucha contra el Delito Transnacional celebrada en Moscú, Federación de Rusia**[49]. Los participantes en el G8 expresaron su preocupación acerca de delitos tales como la pornografía infantil, así como sobre la posibilidad de rastrear las transacciones y el acceso transfronterizo para almacenar datos. En el comunicado publicado con motivo de la Conferencia se consignan varios **principios sobre la lucha del ciberdelito**, que figuran actualmente en una serie de estrategias internacionales.

Uno de los logros prácticos de las tareas efectuadas por varios Grupos de Expertos ha sido la preparación de una **red internacional de contactos las 24 horas del día y 7 días por semana**, red que exige que los países participantes establezcan coordinadores de las investigaciones transnacionales que se realicen, coordinadores que deberán estar accesibles las 24 horas del día y 7 días por semana[50].

1995 para más información, véase: UIT sobre Ciberseguridad Global Agenda / Grupo de Alto Nivel de Expertos, Informe Global Estratégico de 2008, p.ina 17, *http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.*

[49] Comunicado de la Conferencia Ministerial de los países del G-8 sobre la lucha contra la delincuencia organizada transnacional", Moscú, 19 a 20 octubre de 1999.

[50] La idea de una red 24/7 ha sido recogida por una serie de enfoques internacionales en la lucha contra la ciberdelincuencia. Un ejemplo es el artículo 35 de la Convención sobre el Delito Cibernético: (1) Cada Parte designará un punto de contacto disponible las veinticuatro horas, siete días a la semana base, a fin de garantizar la prestación de asistencia inmediata con el objetivo de las investigaciones o procedimientos relativos a delitos relacionados con la informática sistemas y datos, o para la obtención de pruebas en formato electrónico de una infracción penal. Dicha asistencia incluirá la facilitación, o, si lo permite su legislación y práctica nacionales, directamente a la realización de las siguientes medidas: a) la prestación de asesoramiento

En 2004, los Ministros de Justicia y del Interior del G8 expidieron un comunicado en el que señalaron que había que considerar la necesidad de crear **capacidades mundiales para combatir la utilización delictiva de Internet**[51].

Una vez más el G8 tomó nota del Convenio sobre la Ciberdelincuencia del Consejo de Europa.

Organización de las Naciones Unidas

En **el 8º Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente (celebrado en La Habana, Cuba, del 27 de agosto al 7 de septiembre de 1990),** la Asamblea General de Naciones Unidas adoptó una Resolución que tenía por objeto la legislación contra el ciberdelito[52]. Basándose en esta Resolución (Resolución 45/121 (1990)), las Naciones Unidas publicaron en 1994 un **Manual sobre la prevención y el control de delitos informáticos**[53].

En 2000 la Asamblea General aprobó **una Resolución sobre la lucha contra la utilización de la tecnología de la información con fines delictivos**, que presenta cierta semejanza con el Plan de Acción de Diez Puntos adoptado por el G8 en 1997[54].

En 2002 la Asamblea General aprobó otra **Resolución sobre la lucha contra la utilización de la tecnología de la información con fines delictivos**[55] en la que se señalan los métodos existentes en el plano internacional para combatir el ciberdelito y se destacan varias soluciones, por citar algunas :

---

técnico; b) la conservación de los datos de conformidad con los artículos 29 y 30; c) la obtención de pruebas, el suministro de información jurídica, y la localización de los sospechosos.

[51] G8 Comunicado de Justicia e Interior, Washington DC, 11 de mayo de 2004.

[52] A/RES/45/121 aprobada por la Asamblea General de la ONU el 14 de diciembre de 1990. El texto completo de la resolución h*ttp://www.un.org/documents/ga/res/45/a45r121.htm*

[53] Manual de las Naciones Unidas para la Prevención y el Control de los delitos informáticos (publicación de las Naciones Unidas, N E.94.IV.5), *http://www.uncjin.org/Documents/EighthCongress.html.*

[54] A/RES/55/63. El texto completo de la resolución *http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf*

[55] A/RES/56/121.

El texto completo de la resolución,
http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf.

elaborar leyes y políticas nacionales y al adoptar prácticas para luchar contra la utilización de la tecnología de la información con fines delictivos, etc.

En **el 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, organizado en Bangkok, Tailandia, en 2005**[56], se aprobó una Declaración en la que se destacaba la necesidad de unificar el combate contra el ciberdelito. Señalando "*la práctica de los instrumentos vigentes y la preparación de medidas nacionales y el desarrollo de la cooperación internacional en el ámbito penal, de modo tal que se tome en consideración el fortalecimiento y la ampliación de medidas, en particular, contra el ciberdelito…"*

Asimismo, en el sistema de las Naciones Unidas se han aprobado Decisiones, Resoluciones y Recomendaciones sobre temas relacionados con el ciberdelito y entre las cuales, cabe citar por su importancia, las siguientes:

• **La Comisión de Prevención del Delito y Justicia Penal (Oficina de las Naciones Unidas[57] contra la Droga y el Delito**)

• En 2004 el Consejo Económico y Social de las Naciones Unidas[58] adoptó una **Resolución sobre cooperación internacional para prevenir, investigar, enjuiciar y castigar el fraude, la utilización delictiva y la falsificación de identidad y delitos afines**[59]. En 2007 el Consejo adoptó una **Resolución sobre cooperación internacional para impedir, investigar, enjuiciar y castigar el fraude económico y los delitos de usurpación de identidad conexos**[60].

---

[56] "Las sinergias Declaración y respuestas: alianzas estratégicas en materia de Prevención del Delito y Justicia Penal", http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

[57] La Comisión de Prevención del Delito y Justicia Penal (CCPCJ) fue creado en 1991.Se trata de un órgano subsidiario del Consejo Económico y Social.

[58] Las Naciones Unidas Consejo Económico y Social (ECOSOC) es un órgano principal de coordinación económica, social y relacionados con trabajar y servir como foro central para examinar las cuestiones económicas y sociales. Para más información, consulte: *http://www.un.org/ecosoc/*

[59] Resolución del ECOSOC 2004/26 Cooperación internacional en la prevención, investigación, enjuiciamiento y castigo del fraude, el uso indebido e ilícito y falsificación de identidad y otros delitos relacionados, http://www.un.org/ecosoc/docs/2004/Resolution% 202004-26.pdf.

[60] ECOSOC 2007/20 Resolución sobre la cooperación internacional en la prevención, investigación, enjuiciamiento y castigo de el fraude económico y los delitos relacionados, *http://www.un.org/ecosoc/docs/2007/Resolution 202007-20.pdf*.

En 2004 el Consejo adoptó una **Resolución sobre la venta de drogas ilícitas a través de Internet** en la que se contemplaba expresamente el fenómeno relacionado con un delito cibernético[61].

Unión Internacional de Telecomunicaciones[62]

Como organismo especializado del sistema de las Naciones Unidas, la Unión Internacional de Telecomunicaciones (UIT) desempeña un cometido rector en lo que concierne a la normalización y el desarrollo de las telecomunicaciones, así como a los diferentes aspectos de la ciberseguridad. Entre otras actividades, la UIT hizo las veces de organismo rector de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) que se organizó en dos fases, la primera en Ginebra, Suiza (2003) y la segunda en Túnez, Túnez (2005). En la Cumbre gobiernos, formuladores de políticas y expertos de todo el mundo intercambiaron ideas y experiencias acerca de la forma más adecuada de abordar las cuestiones que empezaba a plantear el desarrollo de una sociedad de la información mundial, lo que incluía la definición de normas y leyes compatibles.

Los resultados de la Cumbre se consignan en **la Declaración de Principios de Ginebra, el Plan de Acción de Ginebra, el Compromiso de Túnez y la Agenda de Túnez para la Sociedad de la Información.**

C5. Creación de confianza y seguridad en la utilización de las TICS

La confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información; los gobiernos, en cooperación con el sector privado, deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TIC.

El delito cibernético se discutió, igualmente, en la segunda fase de la CMSI, organizada en Túnez en 2005. En la Agenda de Túnez para la Sociedad de la

[61] Resolución del ECOSOC 2004/42 a la venta por Internet de drogas lícitas a las personas a través de Internet, *http://www.un.org/ecosoc/docs/2004/Resolution% 202004-42.pdf*

[62] La Unión Internacional de Telecomunicaciones (UIT) con sede en Ginebra, fue fundada como la Unión Telegráfica Internacional en el año 1865. Se trata de un organismo especializado de las Naciones Unidas. La UIT cuenta con 191 Estados Miembros y más de 700 Miembros de Sector y Asociados.

Información[63] se hacía hincapié en la necesidad de promover la cooperación internacional para combatir el ciberdelito

En 2007, el Secretario General de la UIT, destacó la importancia de la cooperación internacional en lo que respecta a la lucha contra el ciberdelito y anunció el lanzamiento de la Agenda sobre Ciberseguridad Global de la UIT[64]. La Agenda contiene siete objetivos clave, basados, a su vez, en cinco pilares estratégicos[65], entre otros, la elaboración de estrategias para la formulación de legislación modelo contra el ciberdelito. Los objetivos precitados como " *Preparar estrategias que promuevan el desarrollo de una legislación modelo sobre ciberdelito, definir estrategias…"*

Consejo de Europa[66]

En 1989, el Comité Europeo para Asuntos Delictivos adoptó el "Informe de Expertos sobre el delito cibernético"[67], en el que se analizaban las disposiciones de derecho penal sustantivas que exigía la lucha contra nuevos tipos de delitos electrónicos, incluido el fraude cibernético y la falsificación cibernética. Reunido en 1989, el Comité de Ministros adoptó una Recomendación[68], en que se destacaba concretamente la índole internacional del ciberdelito:

De conformidad con el Artículo 15.b *del "..considerando que el delito cibernético suele tener carácter transfronterizo…".*

Entre 1997 y 2000 el Comité celebró diez sesiones en Plenaria y su Grupo de Redacción de composición abierta organizó otras quince ordinarias. El Pleno

[63] CMSI Agenda de Túnez para la Sociedad de la Información, 2005, h*ttp://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0*

[64] Consulte *http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.*

[65] Los cinco pilares son los siguientes: Medidas jurídicas, las medidas técnicas y de procedimiento, las estructuras organizativas, desarrollo de capacidades, De Cooperación Internacional. Consulte:*http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.*

[66] El Consejo de Europa, con sede en Estrasburgo y fundada en 1949, es una organización internacional que representa a 47 miembros Estados de la región europea. El Consejo de Europa no debe ser confundido con el Consejo de la Unión Europea y la Unión Europea.

[67] Nilsson en Sieber, "Crimen tecnologías de la información", p.576.

[68] Recomendación n º R (89) 9, adoptada por el Comité de Ministros el 13 de septiembre de 1989 en la reunión de la 428ª de Ministros Diputados.

adoptó el Proyecto de Convenio en la segunda parte de su sesión de abril de 2001[69].

En abril de 2009 habían firmado el Convenio sobre la Ciberdelincuencia 46 Estados[70] y 25 Estados[71] lo habían ratificado. Países tales como Argentina, Pakistán, Filipinas, Egipto, Botswana y Nigeria han redactado ya partes de su legislación con arreglo al Convenio. Si bien dichos países no han firmado aún el Convenio, apoyan el proyecto de armonización y normalización propuesto por los redactores del Convenio. Actualmente, se reconoce que el Convenio es un importante instrumento internacional para luchar contra el ciberdelito y como tal ha recabado el apoyo de diferentes organizaciones internacionales.

Algunos de los países en los que se protege apreciablemente el principio de libertad de expresión señalaron con preocupación que si se incluían disposiciones en el Convenio que violaran la libertad de expresión, no podrían firmar el Convenio[72]. De ahí que estas cuestiones se integrasen en un Protocolo separado. En octubre de 2008 habían firmado el Protocolo Adicional 20 Estados[73] y 13 Estados[74] lo habían ratificado.

---

[69] El texto completo de la Convención 185 (Convención sobre el Delito Cibernético), el Protocolo adicional I y la lista de firmas y ratificaciones, *http://www.coe.int*

[70] Albania, Armenia, Austria, Azerbaiyán, Bélgica, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, República Checa, Dinamarca, Estonia Finlandia, Francia, Georgia, Alemania Grecia, Hungría, Islandia, Irlanda, Italia, Latvia, Lituania, Luxemburgo, Malta, Moldova, Países Bajos Montenegro, Noruega, Polonia, Portugal, Rumania, Serbia, Eslovaquia, Eslovenia, España, Suecia, Suiza, Antigua República Yugoslava de Macedonia, Ucrania, Reino Unido, Canadá, Japón, Sudáfrica, Estados Unidos.

[71] Albania, Armenia, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Estonia, Finlandia, Francia, Alemania, Hungría, Islandia, Italia, Letonia, Lituania, Países Bajos, Noruega, Rumania, Serbia, Eslovaquia, Eslovenia, la ex República Yugoslava de Macedonia, Ucrania, Estados Unidos.

[72] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, Informe sobre la Economía de 2005, UNCTAD/SDTE/ECB/2005/1

[73] Albania, Armenia, Austria, Bélgica, Bosnia y Herzegovina, Croacia, Chipre, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Islandia, Letonia, Lituania, Luxemburgo, Malta, Moldavia, Países Bajos, Montenegro, Noruega, Polonia, Portugal, Rumania, Serbia, Eslovenia, Suecia, Suiza, la ex República Yugoslava, República de Macedonia, Ucrania.

[74] Albania, Armenia, Bosnia y Herzegovina, Croacia, Chipre, Dinamarca, Francia, Letonia, Lituania, Noruega, Eslovenia, la Ex República Yugoslava, Macedonia, Ucrania.

Dada su óptica de mejorar la protección de menores contra la explotación sexual, el Consejo de Europa preparó un nuevo Convenio en 2007[75]. Uno de los objetivos esenciales del Convenio es unificar las disposiciones de derecho penal encaminadas a proteger a los menores contra la explotación sexual.

Organización de Cooperación y Desarrollo Económicos[76]

En 1983 la Organización de Cooperación y Desarrollo Económicos (OCDE) inició un estudio sobre la posibilidad de emprender una armonización internacional del derecho penal vigente para abordar el problema que representaba el delito cibernético[77]. La OCDE publicó en 1985 un Informe que analizaba la legislación vigente y formuló propuestas para combatir el ciberdelito866. En 1990 el Comité de Políticas de Información, Informática y Comunicación (ICCP) creó un Grupo de Expertos para preparar un conjunto de directrices de seguridad de la información, que se terminaron de redactar en 1992 y fueron adoptadas ese año por el Consejo de la OCDE. En 2001 un segundo Grupo de Expertos, que actualizó las directrices. En 2002 una nueva versión de las directrices de seguridad de los sistemas y redes de información en el marco de una cultura de seguridad de la OCDE se adoptaron como Recomendación del Consejo de la OCDE[78]. Las directrices contienen nueve principios complementarios como *sensibilización, responsabilidad, respuesta ética, democracia, evaluación de riesgos diseño e implementación en materia de seguridad, gestión de la seguridad y revaluación.*

---

[75] Consejo de Europa - Consejo de Europa sobre la Protección de los Niños contra la Explotación Sexual y Sexual Abuso (CETS No. 201).

[76] La Organización para la Cooperación y el Desarrollo fue fundada 1961. Cuenta con 30 Estados miembros y se basa en París. Más información, *http://www.oecd.org*

[77] Schjolberg / Hubbard, armonización de los enfoques Jurídico Nacional sobre el Delito Cibernético, 2005, p.ina 8, en:
http://www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf

[78] Aprobada por el Consejo de la OCDE en su sesión 1037a, el 25 de julio de 2002. El 2002Directrices de la OCDE para la Seguridad de Sistemas de Información y Redes: Hacia una cultura de seguridad, *http://www.oecd.org/document/42/0, 3343, en_2649_34255_15582250_1_1_1_1, 00.html*

Foro de Cooperación Económica Asia-Pacífico[79]

En 2002 los dirigentes del Foro de Cooperación Económica Asia-Pacífico (APEC) publicaron una declaración sobre la lucha contra el terrorismo y la promoción del crecimiento, para dar aplicación a leyes detalladas sobre el ciberdelito y desarrollar capacidades nacionales e investigación de los delitos cibernéticos873. Los dirigentes se comprometieron a: intentar promulgar en octubre de 2003 un conjunto detallado de leyes sobre ciberseguridad y ciberdelito.

Los dirigentes del APEC hicieron un llamamiento para promover una cooperación más estrecha entre los funcionarios que participan en la lucha contra el ciberdelito[80]. En 2005 el APEC organizó la Conferencia sobre Legislación en materia de Ciberdelito[81].

En la Declaración adoptada por los Ministros de Comunicaciones e Información del APEC reunidos en Bangkok, Tailandia, en 2008, se destacaba la importancia de proseguir la colaboración contra el ciberdelito[82].

[79] La región de Asia-Pacific Economic Cooperation (APEC) es un grupo de países del Pacífico se ocupan de la mejora de la vínculos económicos y políticos que tiene 21 miembros.

[80] "También hacemos un llamado para una cooperación más estrecha entre los agentes del orden público y las empresas en el campo de la seguridad de la información y la lucha contra la delincuencia informática. " Declaración de los Líderes de APEC sobre la lucha contra el terrorismo y promover el crecimiento, Los Cabos, México, 26 de octubre.

[81] Delitos informáticos Legislación y capacidad de ejecución de proyectos de construcción 3 ª Conferencia de Expertos y el Seminario de Capacitación, APEC de Telecomunicaciones y el Grupo de Trabajo de Información, 32 ª reunión, 5-9 de septiembre de 2005, Seúl, Corea.

[82] Los Ministros afirmaron en la declaración "su llamado a continuar la colaboración y el intercambio de información y experiencias entre las economías miembros a que apoyen un entorno TIC seguro y de confianza como una respuesta eficaz para garantizar la seguridad contra las ciberamenazas, los ataques maliciosos y el spam", consultar: *http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.*

La Commonwealth[83]

Habida cuenta de la creciente importancia del ciberdelito los Ministros del Interior de la Commonwealth decidieron constituir un Grupo de Expertos para preparar un marco jurídico que permitiera luchar contra el ciberdelito, basándose en el Convenio sobre la Ciberdelincuencia del Consejo de Europa. Para definir este enfoque de armonización legislativa en el seno de la Commonwealth y fomentar la cooperación internacional se tuvo presente, entre otras cosas, el hecho de que dicho enfoque requeriría la adopción de no menos de 1 272 tratados bilaterales en el marco de la Commonwealth para abordar la cooperación internacional sobre el particular. El Grupo de Expertos presentó su Informe y recomendaciones en marzo de 2002[84]. En la fecha ulterior de dicho año se presentó el proyecto de Ley Modelo sobre el ciberdelito y los actos delictivos afines.

La Liga Árabe y el Consejo de Cooperación del Golfo[85]

Varios países de la Región Árabe han tomado ya medidas nacionales y adoptado diferentes enfoques para luchar contra el ciberdelito, o se encuentran preparando legislación al respecto. Entre estos países, cabe citar: Pakistán, Egipto y Emiratos Árabes Unidos. El Consejo de Cooperación del Golfo[86] recomendó en una Conferencia celebrada en 2007 que los países del Consejo de Cooperación del Golfo intentasen definir un enfoque común en el que se tomaran en consideración diferentes normas internacionales[87].

---

[83] Es una organización compuesta por 54 países independientes y semi-independientes que, con la excepción de Mozambique y Ruanda, comparten lazos históricos con el Reino Unido. Su principal objetivo es la cooperación internacional en el ámbito político y económico, y desde 1950 su membresía no implica sumisión alguna hacia la corona británica.

[84] Ver: *http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/ 7BDA109CD2-5204-AA77-4FAB-86970A639B05% 7D_Computer% 20Crime.pdf (Anexo 1)*

[85] La Liga de Estados Árabes es una organización regional, actualmente con 22 miembros.

[86] Bahrein, Kuwait, Omán, Qatar, Arabia Saudita y los Emiratos Árabes Unidos.

[87] Transacción no oficiales de las recomendaciones de la Conferencia sobre la lucha contrala ciberdelincuencia en los países del CCG, 18 de Junio de 2007, Abu Dhabi: 1.- Llamar a la adopción de un tratado por el Consejo de Cooperación del Golfo (CCG), inspirado por el Consejo de Europa Convenio sobre la Ciberdelincuencia, que se amplió posteriormente a todos los países árabes. 2.- Llamar a todos los países del CCG a adoptar la lucha contra el delito cibernético leyes inspiradas en el

Organización de los Estados Americanos[88]

Desde 1999 la Organización de los Estados Americanos (OEA) ha venido ocupándose activamente de la cuestión del ciberdelito en la región. Entre otras cosas, la Organización ha celebrado una serie de reuniones dentro del mandato y alcance de la **Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA)**.[89]

En 2000, los Ministros de Justicia o Ministros o Procuradores Generales de las Américas abordaron el tema que representaba el ciberdelito y convinieron en una serie de recomendaciones. Estas recomendaciones, entre las cuales cabe citar las siguientes, fueron reiteradas en la reunión de 2003[90]:

• Que se apoye el examen de las recomendaciones efectuado por el Grupo de Expertos Gubernamentales en su reunión inicial, como contribución de la REMJA a la elaboración de la **Estrategia Comprensiva Interamericana de la OEA para combatir amenazas a la ciberseguridad cibernética, señalada en la Resolución de la Asamblea General de la OEA AG/RES. 1939 /XXXIII-O/03),** y pedir al Grupo que, a través de su Presidente, siga apoyando la preparación de la Estrategia.

Los Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA) han celebrado siete reuniones hasta la fecha[91]. Las reuniones más recientes fueron las organizadas en Washington D.C., Estados Unidos, en abril de 2006 y abril de 2008. Entre las recomendaciones formuladas en la reunión de 2006 pueden citarse las siguientes:

---

modelo de la Ley de Delito Cibernético Emiratos Árabes Unidos. 3) Llamar a la adopción de leyes en relación con las cuestiones de procedimiento, tales como convulsiones, inspección e investigación otros procedimientos especiales para este tipo de delitos.

[88] La Organización de Estados Americanos es una organización internacional con 34 Estados miembros activos. Ver: *http://www.oas.org/documents/eng/memberstates.asp*

[89] Consultar *http://www.oas.org/juridico/english/cyber.htm* y el informe final de la quinta reunión de la REMJA, que contiene la lista completa de los informes, los resultados de la sesión plenaria y las conclusiones y recomendaciones *http://www.oas.org/juridico/english/ministry_of_justice_v.htm*

[90] La lista completa de recomendaciones *http://www.oas.org/juridico/english/ministry_of_justice_v.htm*

[91] Las conclusiones y recomendaciones de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas y el Delito Cibernético: *http://www.oas.org/juridico/english/cyber_meet.htm*

• Que prosiga el fortalecimiento de la cooperación con el Consejo de Europa. Asimismo, que se sigan realizando esfuerzos **para fortalecer los mecanismos de intercambio de información y cooperación con otras organizaciones internacionales en la esfera del ciberdelito, tales como las Naciones Unidas, la Unión Europea, el Foro de Cooperación Económica Asia-Pacífico, la OCDE, el G8, la Commonwealth e INTERPOL, para que los Estados Miembros de la OEA aprovechen los progresos alcanzados en dichos foros.**

• Que los Estados Miembros establezcan unidades especializadas para investigar el ciberdelito e identificar a las autoridades que se encargan de la coordinación a este respecto.

Estas recomendaciones fueron reiteradas en la reunión de 2008:

• Que las Secretarías del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Trabajo sobre Ciberdelito, sigan realizando actividades permanentes de coordinación y cooperación para garantizar la implementación de la Estrategia Comprensiva Interamericana de la OEA para combatir amenazas a la seguridad cibernética, adoptada por la Asamblea General de la OEA en la **Resolución AG/RES. 2004 (XXXIVO/04).**

AMERICA LATINA Y MEXICO

Por lo que respecta a América Latina, Costa Rica es el único país que cuenta con presencia internacional en el tema, mediante la adhesión en el **Convenio sobre la Ciberdelincuencia hecho en Budapest el 23 de noviembre de 2001**[92], siendo invitado por El Comité de Ministros del Consejo de Europa[93], de conformidad con su artículo 37.

[92] *http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF*

[93] México participa como observador desde el 1° de diciembre de 1999.

México no ha signado ninguno de los instrumentos mencionados en el tema solo ha servido como observador, motivo por el cual no cuenta con los instrumentos jurídicos para aplicarlos al caso concreto.

Este convenio es considerado como el estándar mundial en esta materia, lo que ha cerrado la posibilidad de que se elabore un Convenio Interamericano sobre Delitos Informáticos, como se sugirió en Foro Legislativo en Materia de Delitos Cibernéticos llevado a cabo en la Ciudad de México en el año 2004.

Es indispensable que México participe como miembro activo en las comunidades citadas, en virtud de que el no contar con la facultad para aplicar algún convenio en la materia representa la perdida valiosa de integración al consenso internacional en la persecución de las nuevas formas de delincuencia ejecutadas a través de los medios informáticos.

CAPÍTULO III

POLÍTICA CRIMINAL EN MÉXICO SOBRE EL COMBATE DE DELITOS INFORMÁTICOS (PROGRAMAS DE GOBIERNO)

1. POLÍTICA DEL PODER EJECUTIVO FEDERAL 2006-2012

En el Plan Nacional de Desarrollo 2007-2012 establece una está estructurado en cinco ejes rectores:

1. Estado de Derecho y seguridad.
2. Economía competitiva y generadora de empleos.
3. Igualdad de oportunidades.
4. Sustentabilidad ambiental.
5. Democracia efectiva y política exterior responsable.

EJE 1. ESTADO DE DERECHO Y SEGURIDAD

En este eje, el titular del poder ejecutivo propuso una reforma que fortalezca los cimientos del Estado de Derecho, ampliando el impacto social del Poder Judicial, mejorando sus respuestas a las demandas de los ciudadanos y aumentando la eficiencia y eficacia de todas las instituciones involucradas en el sistema de justicia. Dentro de ello se planteó la información e inteligencia.

INFORMACIÓN E INTELIGENCIA

Se articuló un sistema de homologación de información para el intercambio, en tiempo real, de datos de audio, video y texto sobre el crimen, estadísticas delictivas y registro del personal de seguridad pública. El intercambio fluido y oportuno de información entre los cuerpos de policía para la prevención del delito y una adecuada coordinación de esfuerzos en su combate. Interrelacionar e interconectar los sistemas de información y de telecomunicaciones de las corporaciones policiales en los tres órdenes de gobierno, para generar métodos uniformes de actuación, información, reporte y archivo localizados en bases de

datos de acceso común, facilitará las investigaciones, operativos conjuntos y generación de inteligencia policial compartida.

Lo cual se llevó a cabo mediante la implementación de la llamada "estrategia 7.1 y 7.2".

ESTRATEGIA 7.1. Desarrollar e implementar sistemas de información y comunicaciones de alta tecnología para el combate a la delincuencia.

Se consolidó el Sistema Único de Información Criminal para concentrar y compartir datos relevantes del fenómeno delictivo en bases de datos completas y eficaces, como los registros de automóviles y armas, perfiles de delincuentes y sus modos de operación. Se desarrolló también una red de interconexión que permita la transmisión de datos, voz e imagen para que esta información pueda compartirse oportunamente, disponer de sistemas de comunicación avanzados con plataformas tecnológicas compatibles.

ESTRATEGIA 7.2. Se generó, fortaleció y coordinó a los sistemas de inteligencia en el Gobierno Federal.

En materia de información se utilizaron estrategias para que las diferentes instituciones avanzaran en su labor de generar inteligencia.

El anterior Gobierno Federal promovió el fortalecimiento de los centros y sistemas de inteligencia para que apoyaran la profesionalización de la investigación en el combate a la delincuencia y el crimen organizado, así como en la mejora de la averiguación previa del proceso penal.

PREVENCIÓN CONTRA EL DELITO CIBERNÉTICO[94]

La Secretaría de Seguridad Pública realiza actividades enfocadas a alertar a los niños y padres de familia sobre los riesgos que existen de ser víctimas de un delito a través del uso de la Internet. Por medio de pláticas a los padres de

[94] Tercer Informe de la Secretaría de Seguridad Pública, *Prevención contra el delito cibernético,* 31 de Agosto de 2009, p.61.
http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/550126//archivo

familia y del rally “Aprende a Cuidarte”, se le explica a la población los riesgos que existen entre el Internet, como medio de comunicación e información, con actividades delictivas como el robo de identidad, la pornografía infantil, el abuso de menores y el narcomenudeo .Debido al impacto que ha tenido el programa se amplió su cobertura a alumnos de todos los grados escolares y se imparte tanto en escuelas como en espacios públicos, así como a miembros de organizaciones sociales interesadas en replicar los mensajes de prevención.

Como parte de las acciones que se llevan a cabo dentro de este programa, se participó en el “Séptimo Parlamento de las Niñas y los Niños 2009”, celebrado el 2 de abril. En respuesta a la invitación de la Comisión de Atención a Grupos Vulnerables de la Cámara de Diputados, se formó un comité de trabajo integrado por miembros de dicha Comisión, Telmex, Google, “Navega Protegido” (Microsoft) y la SSP, para promover entre los alumnos la seguridad a través de Internet.

Se capacitó a 387 multiplicadores, quienes reportaron un efecto multiplicador a 2,059 personas;- se ha trabajado en los estados de Aguascalientes, Baja California, Baja California Sur, Chiapas, Chihuahua, Colima, Guerrero, Hidalgo, Jalisco, México, Morelos, Nayarit, Puebla, Querétaro, Quintana Roo, San Luis Potosí, Sinaloa, Tabasco, Tamaulipas, Tlaxcala, Veracruz, Yucatán y el Distrito Federal.

Informe de Rendición de Cuentas de la APF 2006-2012[95]

El uso generalizado y masivo de medios electrónicos, en particular de teléfonos móviles y el internet, ha propiciado el incremento de los riesgos en la seguridad de los ciudadanos, por lo que este programa centró sus actividades en el desarrollo de habilidades y competencias para prevenir a la población infantil, juvenil y adulta sobre las prácticas incorrectas en el uso de estos medios de comunicación, así como de los delitos que pueden cometerse a través de ellos, como son los relacionados con el sector bancario, el comercio electrónico, el narcomenudeo, el maltrato infantil y el abuso sexual, entre otros. A través de este

[95] *http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/1172114//archivo*

programa, se realizaron 6,694 cursos, talleres y actividades lúdicas en las que participaron 465,512 personas.

En el citado informe y en el marco respectivo a las Tecnologías de la Información se cuenta con avances en el marco de la reforma estructural de la SSP a partir de 2010 se llevaron a cabo las acciones orientadas a proponer y ejecutar el desarrollo tecnológico de la Institución, en materia de recursos informáticos, telecomunicaciones y equipo especializado, para promover la optimización y estandarización de estos sistemas con un alto nivel de servicios e impulsar la implantación, operación y modernización de los sistemas administrativos vigentes o en proceso de incorporación, el SUIC, así como el sistema de la Plataforma México. Para en ese sentido contribuir y aplicar las estrategias, y objetivos que contempla el PND 2007-2012 y así como el PNSP 2008-2012 y el PSSP 2007-2012 como son: Establecer mecanismos y procesos que permitan conocer sistemáticamente las características y patrones del fenómeno delictivo en México; asegurar la disponibilidad de información confiable y oportuna; desarrollar e implementar sistemas de información y comunicaciones de alta tecnología para el combate a la delincuencia e incorporar tecnologías de información y telecomunicaciones a la función policial para crear interconexiones de bases de datos a nivel federal, estatal y municipal, asimismo, generar estrategias coordinadas de prevención y combate al delito.

2. POLICÍA CIBERNÉTICA

La Policía Cibernética de la Policía Federal Preventiva (PFP) ha detectado en México en los últimos meses la existencia de 10 comunidades de hackers, nueve de las cuales son nacionales y una italiana. [96]

Esas comunidades ofrecen técnicas para el ataque a sistemas computacionales vía internet e incluso distribuyen software programas de computación que sirven para los mismos propósitos.

[96] EL UNIVERSAL.mx, *En México hay 10 comunidades de hackers: Policía Cibernetica*, Jueves 12 de Junio de 2003, *http://www2.eluniversal.com.mx/pls/impreso/noticia.html?id_nota=97982&tabla=nacion*

Sin embargo, los fraudes comerciales y la pornografía en sus diversas modalidades son los principales ilícitos que ocurren en México vía internet, de acuerdo con informes del Grupo Interinstitucional de Combate a Delitos Cibernéticos DC México.

Además, México está reconocido como generador de ataques a sistemas computacionales y Estados Unidos es el primero en esta materia, de acuerdo con DC México. Apenas el mes pasado la PFP detectó 22 nuevos sitios de distribución y promoción de pornografía infantil, mismos que son soportados por conocidos portales tanto nacionales como internacionales, pero que tienen su origen, fundamentalmente, en México.

En los últimos nueve años la Policía Federal (PF) ha detectado y promovido la desactivación de 3 mil 284 sitios de pedofilia o pornografía en Internet. Según las cálculos de la corporación, por cada página se podría suponer la existencia de una red de compradores, interesados o consumidores. [97]

Puntualizó que esos sitios alojados en lo que se conoce como web hosting, pueden registrarse en cualquier parte del mundo bajo un formato que puede ser llenado con datos falsos, pues no pueden ser corroborados por ningún medio, por lo que resulta difícil precisar, geográficamente hablando, dónde se generan las páginas.

Respecto de cuántas redes de pedofilia o pornografía infantil ha detectado, la PF respondió que por cada sitio web detectado se podría suponer la existencia de una red de compradores, interesados o consumidores, los cuales de manera general pueden intercambiar archivos a cuentas de correo [...], así como también pueden subir o descargar imágenes, video, publicar comentarios y/o narraciones textuales relacionadas con el tema de pornografía infantil.

En 2010 los sitios web gubernamentales que se vieron afectados por *hackers* aumentaron 40 por ciento en comparación con 2009, al pasar de 240 a 321 casos.

---

[97] Castillo García, Gustavo *En 9 años la Policía Cibernética impulsó la desactivación de 3 mil 284 sitios pornográficos,* Periódico La Jornada Domingo 27 de febrero de 2011, p. 11.

Entre los casos más conocidos de estas afectaciones ilegales en fechas recientes, destaca lo ocurrido el 30 de enero, cuando justo el día de los comicios para elegir gobernador, diputados locales y alcaldes, el portal del gobierno de Guerrero fue alterado. “Los piratas informáticos colocaron el mensaje: ‘Ya no queremos más violencia en México’. Esto surge por la falta de seguridad que no encontramos los mexicanos y ya estamos artos (sic) de ver esto todos los días en la televisión”.

En junio de 2010, el aeropuerto capitalino y su página oficial fueron alteradas por *hackers* que protestaron por tener que registrar sus celulares y denunciaron la venta de números y propietarios en Internet.

En mayo, los piratas que se identificaron como *Gob* y *Suckean*, argentino y chileno, colapsaron la página del Senado mexicano, y colocaron imágenes de *El chavo del ocho,* antiguo personaje de la televisión comercial.

El 17 de noviembre de 2009, el periódico *El Heraldo de Chihuahua* informó que “decenas de páginas oficiales de gobierno, medios de comunicación, instituciones educativas y de empresas de distintos giros fueron vulneradas por un grupo de protesta, formado por expertos en seguridad informática.

El grupo reclamó [...] la ineptitud de los gobiernos para combatir la corrupción y el crimen organizado, dando una muestra de la fragilidad de las páginas de Internet, durante más de dos horas.

La Ciber Protesta Mexicana, como fue denominada por los integrantes del grupo atacante, comenzó antes de las 8 de la mañana, insertando en los portales oficiales textos e imágenes de reclamo, y terminó al filo de las 10 horas, cuando las páginas pudieron ser estabilizadas.

Los conteos de la PF a este respecto refieren que entre 2009 y 2010, por ejemplo, las páginas del GDF han sido alteradas más de 40 ocasiones; el portal del gobierno de Chiapas sufrió más de 30 ataques, mientras las páginas de entidades como Jalisco, estado de México, Sonora, Colima y Veracruz han sido vulneradas más de 20 ocasiones.

Los sitios oficiales de los estados de Guanajuato, Yucatán, Nayarit, Baja California, Baja California Sur, Michoacán, Querétaro, Morelos, Coahuila, Puebla,

Aguascalientes, Zacatecas, Tabasco, Hidalgo y Sinaloa también han sufrido ciberataques.

POLICÍA CIBERNÉTICA EN LOS ESTADOS

Para finalizar cabe hacer mención que también existen policías cibernéticas a nivel Estatal como es la Unidad de la Policía Cibernética de Jalisco (PCJ), que funciona desde el mes de Octubre de 2002,[98] Nuevo León, Yucatán, Coahuila y Sinaloa tienen lo propio.

Estados como Veracruz, tabasco, Querétaro, y Chihuahua trabajan en su creación e inclusive ya han sido aprobadas por sus congresos.

3. PUNTOS DE ACUERDO APROBADOS POR LA CÁMARA DE DIPUTADOS RELATIVOS A LOS PROCEDIMIENTOS DE PREVENCIÓN DE RIESGOS EN EL USO DE INTERNET[99]

Se propone el fortalecimiento de la Unidad de Investigación Cibernética y respuestas a los puntos requeridos por la Secretaría de Gobierno.

JUSTIFICACIÓN

Hoy existe en la Policía de Investigación una Unidad de Investigación Cibernética, misma que se implantó en diciembre de 2006, a la fecha tiene una estructura en diferentes funciones como lo son la investigación de delitos cometidos a través de la red, análisis y obtención de información digital de dispositivos electrónicos, laboratorio de análisis forense y de telefonía celular.

La Unidad de Investigación Cibernética auxilia al Ministerio Publico en la investigación y persecución de los delitos en donde se encuentre relacionada alguna tecnología de la información.

VISIÓN

A corto plazo establecer el área de Inteligencia Cibernética integrada por la Coordinación de Delitos Electrónicos (e-Crime), Coordinación Técnica de inteligencia, Coordinación de Monitoreo (CERT) , especializados en el combate

[98] *http://www.policiacibernetica.jalisco.gob.mx/index.html*

[99] Gaceta Parlamentaria, año XIV, número 3251-I, viernes 29 de abril de 2011

de los delitos, integrado por agentes de la Policía Investigadora del Distrito Federal, para auxiliar al Ministerio Público en la investigación y persecución de estos delitos.

A largo plazo se pretende establecer las bases necesarias para la creación de una fiscalía especializada en tecnologías de la información, que esté integrada por un Ministerio Público especializado en la materia, policía investigadora y peritos en informática, asimismo crear un SITE oficial para la investigación de estos delitos a nivel nacional, que facilite el intercambio y pronta procuración e impartición de justicia.

COORDINACIÓN DE DELITOS ELECTRÓNICOS (E-CRIME)

Auxiliará al Ministerio Publico en la investigación y persecución de los delitos relacionados con las tecnologías de la información, así como iniciar el proyecto CERT de monitoreo y conexión a través de la Red a nivel nacional.

COORDINACIÓN DE MONITOREO, RESPUESTA Y ANÁLISIS (CERT)

Es el inicio de la creación de una red para ciberpolicías a nivel nacional teniendo como matriz a la PFP, el término CERT proviene de las siglas en inglés *Computer Emergency Response Team*, y viene a definir a un equipo de personas dedicado a la implantación y gestión de medidas tecnológicas con el objetivo de mitigar el riesgo de ataques contra los sistemas de la comunidad a la que se proporciona el servicio.

COORDINACIÓN TÉCNICA DE INTELIGENCIA

Es la encargada de desarrollar tecnología para la etapa de la inteligencia operativa, utilizará la tecnología asignada para las vigilancias técnicas y obtención de información, (laboratorio de video, audio, fotografía, etcétera.)

DELITOS CONTRA EL MENOR. AMENAZAS Y EXTORSIONES. FRAUDES ELECTRÓNICOS Y OTROS

En esta área se atienden las investigaciones solicitadas a la Coordinación de Delitos Electrónicos, que estén relacionadas con alguna averiguación previa, con apoyo de las técnicas de investigación tecnológica y las herramientas necesarias realizará los informes correspondientes a las solicitudes durante la guardia. La función fundamental es la de investigar a fondo todos los hechos ilícitos que se cometen en la red tomando en cuenta que por medio de un dispositivo electrónico se pueden realizar tipos penales vigentes en el Código.

LABORATORIO DE RECOLECCIÓN Y EVIDENCIA DIGITAL. TELEFONÍA CELULAR. DISPOSITIVOS ELECTRÓNICOS

Cumple con la función de entender en la permanente observación, el registro y análisis de los casos de delitos (e irregulares) cometidos mediante tecnologías de la información y de las telecomunicaciones. Brindará los informes que resulten útiles para la investigación y persecución de tales hechos cuando resulten ilícitos con base en un método de recolección de evidencia digital.

MONITOREO, RESPUESTA Y ANÁLISIS CERT

CERT se encargará de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún ataque, aquí se dará seguimiento a la información recibida en el correo institucional por parte de las denuncias electrónicas o incidencias, así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo, para esto es necesario estar conectados a un servidor central que dará alojamiento IP a todas la ciberpolicías del país, permitiendo monitorear y compartir incidencias delictivas por jurisdicción, compartir bases de datos de pederastas a nivel internacional con una conexión vía web server a Microsoft.

ODINET Y ANÁLISIS

De los resultados obtenidos en el operativo de investigación en Internet, se realizará el análisis para su tratamiento y actualización de los modus operandi a través de la Red, enfocado principalmente a la explotación sexual infantil, fraudes electrónicos y otros, llevará estrecha relación con las aéreas encargadas de hacer las redes delincuenciales.

Se busca establecer un acuerdo de intercambio de información oficial mediante el uso de los servidores de correo institucional, por medio del cual la información solicitada pueda ser incluida en investigaciones oficiales, hay que recordar que la Suprema Corte de Justicia de la Nación reconoce plenamente el uso de la información mediante servidores de correo institucional para esto es necesario establecer un CERT único que contenga las bases de datos necesarias, además de un monitoreo de fraudes electrónicos y para detectar las conductas delictivas. Asimismo intercambio de freeware forense, al igual que promover, en el ámbito de competencias, la homologación en la capacitación entre las diferentes esferas de la justicia.

CAPÍTULO IV

ANÁLISIS DOGMÁTICO DE LOS DELITOS INFORMÁTICOS Y CONDUCTAS ILÍCITAS NO TIPIFICADAS, REALIZADAS CON HERRAMIENTAS INFORMÁTICAS Y DEMÁS MEDIOS ELECTRÓNICOS

1. LEGISLACIONES FEDERALES

CÓDIGO PENAL FEDERAL

CAPÍTULO II: ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

Artículo 211 bis 1: *Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrá de seis meses a dos años de prisión y de 100 a 300 días multa.*

Al que sin autorización conozca o copia información contenida en sistemas fue equipos de informática protegidos por algún mecanismo la, se le impondrá de tres meses a un año de prisión y de 50 a 150 días multa.

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

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

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

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

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

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

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

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

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

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

Artículo 211 bis 7: *Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.*[100]

Reformas al Código Penal Federal publicadas en el Diario Oficial de la Federación el 17 de mayo del año 1999.

[100] Agenda Penal Federal 2012, México 2012,Ediciones Fiscales ISEF.

Artículo 167.- *Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:*

VI. Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos.

Artículo 168-bis.- *Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho:*

I. Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas, o

II. Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas.[101]

Así mismo en los Artículos 424-bis, 424-ter y 368 se establece tipificación sobre la piratería informática, que a la letra dice:

Artículo 424-bis*.- Se impondrá prisión de 3 a 10 años y de 2,000 a 20,000 días multa, a quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.*

Igual pena para quienes, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o a quien fabrique con fin de lucro, un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Artículo 368.- Se equiparan al robo y se castigarán como tal:

II. El uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin

[101] *http://www.cddhcu.gob.mx/leyinfo/pdf/9.pdf*

derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.[102]

Es importante señalar que es común robar o desencriptar a través de software libre que se encuentre en internet o desbloquear las llaves o códigos de seguridad para poder usar una señal de cualquier modem de internet inalámbrico.

OBSERVACIONES

Los tipos penales anteriormente citados concuerdan con los planteados en países como España, Italia, Alemania, entre otros, mismos que hemos analizado en capítulos anteriores, respecto a ciertos elementos comunes aplicados a la protección de los sistemas de información de uso del Gobierno.

Por ultimo un avance significativo en materia de Propiedad Intelectual. Se encuentran tipificadas conductas como producción, reproducción, a través de sistemas de información, conductas llevabas a acabo mediante delitos como la piratería, entre otros.

[102] *http://info4.juridicas.unam.mx/ijure/tcfed/8.htm?*

A) CONDUCTAS TIPIFICADAS EN EL CÓDIGO PENAL FEDERAL[103] SUSCEPTIBLES DE SER COMETIDOS A TRAVÉS DE MEDIOS INFORMÁTICOS CON EL USO DE CÓDIGOS MALICIOSOS, CORREOS ELECTRÓNICOS, REDES SOCIALES Y PUBLICACIÓN DE PÁGINAS WEB.

DELITO	COMETIDO POR UN MEDIO INFORMÁTICO A TRAVÉS	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Espionaje	BUGWARE GUSANO (Computer Worm) PHARMING	Art. 127.- Al extranjero que, declarada la guerra o rotas las hostilidades contra México, tenga relación o inteligencia con el enemigo o le proporcione información, instrucciones o documentos o cualquier ayuda que en alguna forma perjudique o pueda perjudicar a la Nación Mexicana….”
	PHISHING SPYWARE	Art. 128.- Al mexicano que, teniendo en su poder documentos o informaciones confidenciales de un gobierno extranjero, los revele a otro gobierno, si con ello perjudica a la Nación Mexicana.”
		Art. 129.- Al que teniendo conocimiento de las actividades de un espía y de su identidad, no lo haga saber a las autoridades…”
Rebelión	REDES SOCIALES PUBLICACIÓN DE PÁGINAS WEB CORREOS ELECTRÓNICOS TROYANO	Art. 133.- Al funcionario o empleado público de los Gobiernos Federal o Estatales, o de los Municipios, de organismos públicos descentralizados, de empresas de participación estatal, o de servicios públicos, federales o locales, que teniendo por razón de su cargo documentos o informes de interés estratégico, los proporcione a los rebeldes
		Art. 135.- Al que: I.-En cualquier forma o por cualquier medio invite a una rebelión; II. Residiendo en territorio ocupado por el Gobierno: b) Mantenga relaciones con los rebeldes, para proporcionarles noticias concernientes a las operaciones militares u otras que les sean útiles.”

[103] Agenda Penal Federal 2012, Op. Cit., nota 100, p.63

DELITO	COMETIDO POR UN MEDIO INFORMÁTICO A TRAVÉS	DESCRIPCIÓN TÍPICA Y PUNIBILIDAD
Terrorismo	CORREOS ELECTRÓNICOS PUBLICACIÓN DE PÁGINAS WEB REDES SOCIALES	Art. 139.- Al que utilizando sustancias tóxicas, armas químicas, biológicas o similares, material radioactivo o instrumentos que emitan radiaciones, explosivos o armas de fuego, o por incendio, inundación o por cualquier otro medio violento, realice actos en contra de las personas, las cosas o servicios públicos, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad para que tome una determinación.
Sabotaje	REDES SOCIALES CORREOS ELECTRÓNICOS PUBLICACIÓN DE PÁGINAS WEB BOMBAS DE TIEMPO GUSANOS HOAXES BUGWARE MIRC VIRUS PHARMING ROOTSKITS TROYANO	Art. 140.- Al que dañe, destruya o ilícitamente entorpezca vías de comunicación, servicios públicos, funciones de las dependencias del Estado, organismos públicos descentralizados, empresas de participación estatal o sus instalaciones; plantas siderúrgicas, eléctricas o de las industrias básicas; centros de producción o distribución de artículos de consumo necesarios de armas, municiones o implementos bélicos, con el fin de trastornar la vida económica del país o afectar su capacidad de defensa.
Conspiración	PUBLICACIÓN DE PÁGINAS WEB REDES SOCIALES CORREOS ELECTRÓNICOS	Art. 141.- A quienes resuelvan de concierto cometer uno o varios de los delitos del presente Título y acuerden los medios de llevar a cabo su determinación.”

DELITO	COMETIDO POR UN MEDIO INFORMÁTICO A TRAVÉS	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
En Materia de vías de Comunicación y Correspondencia	SPYWARE TROYANO	Art. 167.- VI. Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos;
		Art. 168.- A quien sin derecho: Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas, o Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas.
Violación de Correspondencia	SPYWARE TROYANO	Art. 173.- Al que abra indebidamente una comunicación escrita que no esté dirigida a él, y Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido.”
	CORREOS ELECTRÓNICOS	Art. 176.- Al empleado de un telégrafo, estación telefónica o estación inalámbrica que conscientemente dejare de transmitir un mensaje que se le entregue con ese objeto, o de comunicar al destinatario el que recibiere de otra oficina, si causare daño, se le impondrá de quince días a un año de prisión o de 30 a 180 días multa.”
	REDES SOCIALES	Art. 177.- A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.”
Contra la Salud	PUBLICACIÓN DE PÁGINAS WEB CORREOS ELECTRÓNICOS REDES SOCIALES	Art. 194.- Al que: II. Aporte recursos económicos o de cualquier especie, o colabore de cualquier manera al financiamiento, supervisión o fomento para posibilitar la ejecución de alguno de los delitos a que se refiere este capítulo; y III. Realice actos de publicidad o propaganda, para que se consuma cualesquiera de las instancias comprendidas en el artículo anterior.

DELITO	COMETIDO POR UN MEDIO INFORMÁTICO A TRAVÉS	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Corrupción de Personas Menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo.	CORREOS ELECTRÓNICOS PUBLICACIÓN DE PÁGINAS WEB REDES SOCIALES SEXTING	Art. 200.- Al que comercie, distribuya, exponga, haga circular u oferte, a menores de dieciocho años de edad, libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter pornográfico, reales o simulados, sea de manera física, o a través de cualquier medio
Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo.	CORREOS ELECTRÓNICOS PUBLICACIÓN DE PÁGINAS WEB REDES SOCIALES SEXTING	Art. 202.- Quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos.
Lenocinio	CORREOS ELECTRÓNICOS PUBLICACIÓN DE PÁGINAS WEB REDES SOCIALES SEXTING CIBERTALKING	Art. 202.- II. Al que induzca o solicite a una persona para que con otra, comercie sexualmente con su cuerpo o le facilite los medios para que se entregue a la prostitución.
Amenazas	CORREOS ELECTRÓNICOS. REDES SOCIALES. PUBLICACIÓN DE PÁGINAS WEB. CIBERTALKING CIBERBULLYNG	Art. 282.- I. Al que de cualquier modo amenace a otro con causarle un mal en su persona, en sus bienes, en su honor o en sus derechos, o en la persona, honor, bienes o derechos de alguien con quien esté ligado con algún vínculo, y II. Al que por medio de amenazas de cualquier género trate de impedir que otro ejecute lo que tiene derecho a hacer.

DELITO	COMETIDO POR UN MEDIO INFORMÁTICO A TRAVÉS	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Robo	REDES SOCIALES BUGWARE PHISHING SPYWARE	Art. 367.- El que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley. I. El apoderamiento o destrucción dolosa de una cosa propia mueble, si ésta se halla por cualquier título legítimo en poder de otra persona y no medie consentimiento; y II. El uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.
Fraude	CORREOS ELECTRÓNICOS PUBLICACIÓN DE PÁGINAS WEB REDES SOCIALES PHISHING PHARMING	Art. 386.- El que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.
Extorsión	CORREOS ELECTRÓNICOS PUBLICACIÓN DE PÁGINAS WEB REDES SOCIALES CIBERBULLYNG	Art. 390.- Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial.
Operaciones con Recursos de Procedencia Ilícita	PHISHING	Art. 400 bis.- Al que por sí o por interpósita persona realice cualquiera de las siguientes conductas: adquiera, enajene, administre, custodie, cambie, deposite, dé en garantía, invierta, transporte o transfiera, dentro del territorio nacional, de éste hacia el extranjero o a la inversa, recursos, derechos o bienes de cualquier naturaleza, con conocimiento de que proceden o representan el producto de una actividad ilícita, con alguno de los siguientes propósitos: I. Ocultar o pretender ocultar, encubrir o impedir conocer el origen, localización, destino o propiedad de dichos recursos, derechos o bienes, o alentar alguna actividad ilícita.”

DELITO	COMETIDO POR UN MEDIO INFORMÁTICO A TRAVÉS	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Delitos en materia de Derechos de autor	CORREOS ELECTRÓNICOS PUBLICACIÓN DE PÁGINAS WEB REDES SOCIALES PHISHING	Art. 424 bis.- I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos. Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.
		Art.426.- I. A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, I. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

El empleo de técnicas y sofisticadas estrategias por quien tiene conocimiento de las tecnologías de las información como los usuarios de sistemas, hackers, intrusos, etc., para causar algún daño es una conducta que actualmente se encuentra tipificada, el legislador ha buscado encuadrar en figuras típicas como el robo, fraude, falsificación, estafa o sabotaje hasta el terrorismo a estas conductas realizadas por sujetos con conocimiento del tema.

El Estado no ha hecho caso omiso a esta problemática, y ha buscado proporcionar a través de los tipos descritos con anterioridad la seguridad a los sistemas de telecomunicaciones, y a los derechos de autor que constantemente sufren de ataques virtuales, legislando no solo en estas áreas sino también en lo

concerniente a la intervención de comunicaciones de la Ley de Seguridad Nacional.

Y por lo que respecta a los particulares a través de los tipos penales enumerados en los artículos 9, 17, 67 se pretende proporcionar una seguridad al acceso a datos personales del individuo.

B) LEGISLACIONES FEDERALES QUE PRESCRIBEN CONCEPTOS Y/O POSIBLES CONDUCTAS DELICTIVAS A TRAVÉS DE MEDIOS INFORMÁTICOS Y OTRAS TECNOLOGÍAS ADEMÁS DE SU PREVENCIÓN.

LEGISLACIÓN	ARTÍCULO	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Ley Federal de Telecomunicaciones	3	IV. Frecuencia: número de ciclos que por segundo efectúa una onda del espectro radioeléctrico; VIII. Red privada de telecomunicaciones: la red de telecomunicaciones destinada a satisfacer necesidades específicas de servicios de telecomunicaciones de determinadas personas que no impliquen explotación comercial de servicios o capacidad de dicha red; IX. Red pública de telecomunicaciones: la red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal; XII. Servicios de valor agregado: los que emplean una red pública de telecomunicaciones y que tienen efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida por algún usuario y que comercializan a los usuarios información adicional, diferente o reestructurada, o que implican interacción del usuario con la información almacenada;
	44	Los concesionarios de redes públicas de telecomunicaciones deberán: I. Llevar un registro y control separado de sus usuarios, tanto en la modalidad de línea contratada en plan tarifario, como en líneas de prepago, el cual contenga como mínimo los siguientes datos: Los concesionarios deberán conservar copias fotostáticas o en medios electrónicos de los documentos necesarios para dicho registro y control; así como mantener la reserva y protección de las bases de datos personales, las cuales no podrán ser usadas con fines diferentes a los señalados en las leyes; d. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad que permitan identificar con precisión los siguientes datos: 1. Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago; 2. Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia; 3. Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que

		se haya activado el servicio; 4. La ubicación digital del posicionamiento geográfico de las líneas telefónicas. La obligación de conservación de datos a que se refiere la presente fracción cesa a los doce meses, contados a partir de la fecha en que se haya producido la comunicación. Los concesionarios tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control; i. Entregar los datos conservados, al Procurador General de la República o Procuradores Generales de Justicia de las Entidades Federativas, cuando realicen funciones de investigación de los delitos de extorsión, amenazas, secuestro, en cualquiera de sus modalidades o de algún delito grave relacionado con la delincuencia organizada, en sus respectivas competencias.
	71	Las infracciones a lo dispuesto en esta Ley, se sancionarán por la Secretaría de conformidad con lo siguiente: A. Con multa de 10,000 a 100,000 salarios mínimos por: V. Interceptar información que se transmita por las redes públicas de telecomunicaciones,

LEGISLACIÓN	ARTÍCULO	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Código de Comercio	89	De los mensajes de Datos. En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones: 1. Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica. 2. Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante. 3. Destinatario: La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje. 4. Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario. 5. Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que

		produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio. 6. Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97. En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica. 7. Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa. 8. Intermediario: En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él. 9. Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología. 10. Parte que Confía: La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica. 11. Prestador de Servicios de Certificación: La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados. 12. Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos. 13. Titular del Certificado: Se entenderá a la persona a cuyo favor fue expedido el Certificado.

LEGISLACIÓN	ARTÍCULO	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Ley Federal de Derechos de Autor	13	Los derechos de autor a que se refiere esta Ley se reconocen respecto de las obras de las siguientes ramas: XI. Programas de cómputo;
	101	Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.
	102	Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.
	103	Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.

	104	Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares.
	105	El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando: I. Sea indispensable para la utilización del programa, o II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación. Artículo 106. El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir: I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma; II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante; III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.
	107	Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.
	108	Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.
	109	El acceso a información de carácter privado relativa a las personas contenidas en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.
	110	El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir: I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma; II. Su traducción, adaptación, reordenación y cualquier otra modificación; III. La distribución del original o copias de la base de datos; IV. La comunicación al público, y V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

	111	Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.
	112	Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.
	113	Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.
	114	La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

LEGISLACIÓN	**ARTÍCULO**	**DESCRIPCIÓN TIPICA Y PUNIBILIDAD**
Ley de la Propiedad Industrial	15	De las Patentes Se considera invención toda creación humana que permita transformar la materia o la energía que existe en la naturaleza, para su aprovechamiento por el hombre y satisfacer sus necesidades concretas.
	19	No se considerarán invenciones para los efectos de esta Ley: IV. Los programas de computación;
	223 bis	Al que venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa y con fin de especulación comercial, objetos que ostenten falsificaciones de marcas protegidas por esta Ley. Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en los artículos 223 y 224 de esta Ley.

LEGISLACIÓN	ARTÍCULO	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Ley de Instituciones de Crédito	112 Quáter	Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello: I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.
	113 Bis	A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de recursos o valores de los clientes de las instituciones de crédito, se le aplicará una sanción de tres a diez años de prisión y multa de quinientos a treinta mil días de salario.
	113 Bis 2	Serán sancionados los servidores públicos de la Comisión Nacional Bancaria y de Valores, con la pena establecida para los delitos correspondientes más una mitad, según se trate de los delitos previstos en los artículos 111 a 113 Bis y 114 de esta ley, que: I. Oculten al conocimiento de sus superiores hechos que probablemente pueda constituir delito; II. Permitan que los funcionarios o empleados de la institución de crédito alteren o modifiquen registros con el propósito de ocultar hechos que probablemente puedan constituir delito; III. Obtengan o pretendan obtener un beneficio a cambio de abstenerse de informar sus superiores hechos que probablemente puedan constituir delito;

LEGISLACIÓN	ARTÍCULO	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Ley de Seguridad Nacional	33	De las Intervenciones de Comunicaciones En los casos de amenaza inminente a los que se refiere el artículo 5 de esta Ley, el Gobierno Mexicano podrá hacer uso de los recursos que legalmente se encuentren a su alcance, incluyendo la información anónima.
	34	De conformidad con lo dispuesto por el párrafo noveno del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el Centro deberá solicitar en los términos y supuestos previstos por la presente Ley, autorización judicial para efectuar intervenciones de comunicaciones privadas en materia de Seguridad Nacional. Se entiende por intervención de comunicaciones la toma, escucha, monitoreo, grabación o registro, que hace una instancia autorizada, de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología.
	39	Una vez presentada la solicitud, el juez debe proporcionar acuse de recibo y emitir dentro de las veinticuatro horas contadas a partir de la solicitud, una resolución fundada y

		motivada en la que puede otorgar o negar la autorización solicitada. En caso de negarla, el juez señalará los motivos de su negativa y los requisitos que deben cubrirse para la procedencia de ésta. La intervención puede aplicarse a comunicaciones y emisiones privadas, realizadas por cualquier medio de transmisión, conocido o por conocerse, o entre presentes, incluyendo la grabación de imágenes privadas.
	40	El juez, al emitir la resolución que autorice la medida solicitada, en todo caso deberá precisar: I. Los datos de identificación del expediente en que se actúa; II. El tipo de actividad que autoriza; III. El lapso durante el cual se autoriza la medida; IV. En caso necesario, la autorización expresa para instalar o remover cualquier instrumento o medio de intervención, y V. Cualquier apreciación que el juez considere necesaria. De los Casos de Urgencia

LEGISLACIÓN	ARTÍCULO	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Ley Federal contra la Delincuencia Organizada	2	Cuando tres o más personas se organicen de hecho para realizar, en forma permanente o reiterada, conductas que por sí o unidas a otras, tienen como fin o resultado cometer alguno o algunos de los delitos siguientes, serán sancionadas por ese solo hecho, como miembros de la delincuencia organizada: I. Terrorismo, previsto en los artículos 139 al 139 Ter y terrorismo internacional previsto en los artículos 148 Bis al 148 Quáter; contra la salud, previsto en los artículos 194 y 195, párrafo primero; falsificación o alteración de moneda, previstos en los artículos 234, 236 Y 237; operaciones con recursos de procedencia ilícita, previsto en el artículo 400 Bis; y el previsto en el artículo 424 Bis, todos del Código Penal Federal; II. Acopio y tráfico de armas, previstos en los artículos 83 bis y 84 de la Ley Federal de Armas de Fuego y Explosivos; III. Tráfico de indocumentados, previsto en el artículo 138 de la Ley General de Población; IV. Tráfico de órganos previsto en los artículos 461, 462 y 462 bis de la Ley General de Salud; V. Corrupción de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo previsto en el artículo 201; Pornografía de personas menores de dieciocho años de edad o de personas…… VI. Trata de personas, previsto y sancionado en los artículos 5 y 6 de la Ley para Prevenir y Sancionar la Trata de Personas.
	16	Cuando en la averiguación previa de alguno de los delitos a que se refiere esta Ley o durante el proceso respectivo, el Procurador General de la República o el titular de la unidad especializada a que se refiere el artículo 8o. anterior,

		consideren necesaria la intervención de comunicaciones privadas, lo solicitarán por escrito al juez de distrito, expresando el objeto y necesidad de la intervención, los indicios que hagan presumir fundadamente que en los delitos investigados participa algún miembro de la delincuencia organizada; así como los hechos, circunstancias, datos y demás elementos que se pretenda probar. Las solicitudes de intervención deberán señalar, además, la persona o personas que serán investigadas; la identificación del lugar o lugares donde se realizará; el tipo de comunicación privada a ser intervenida; su duración; y el procedimiento y equipos para la intervención y, en su caso, la identificación de la persona a cuyo cargo está la prestación del servicio a través del cual se realiza la comunicación objeto de la intervención. Podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.

LEGISLACIÓN	ARTÍCULO	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Ley Federal de Protección de Datos en Posesión de Particulares	9	De los Principios de Protección de Datos Personales Artículo 9.- Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.
	17	El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera: II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata.
	67	De los Delitos en Materia del Tratamiento Indebido de Datos Personales. Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.
	68	Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.
	69	Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

2. LEGISLACIONES PENALES LOCALES QUE PRESCRIBEN CONCEPTOS Y/O POSIBLES CONDUCTAS DELICTIVAS A TRAVÉS DE MEDIOS INFORMÁTICOS Y OTRAS TECNOLOGÍAS ADEMÁS DE SU PREVENCIÓN.

LEGISLACIÓN PENAL LOCAL	ARTÍCULOS	DESCRIPCIÓN TIPICA Y PUNIBILIDAD
Aguascalientes	80 A, 175, 175 Bis, 175 Ter	Tipos penales protectores de la confidencialidad y la intimidad de la información.[104] Delitos contra la inviolabilidad del secreto y de los sistemas y equipos de informática Acceso ilícito a sistemas y equipos de informática A quien sin autorización o indebidamente, copie o accese a información contenida en sistemas o equipos de informática
Coahuila	281 Bis, 281 Bis 1, 281 Bis 2, 281 Bis 4	Delitos contra la seguridad en los medios informáticos. Sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de particulares. Hace mención también a circunstancias; asimismo sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de una entidad pública agravantes de los delitos anteriores, de igual forma establece: "..se entiende por: Sistema informático: todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos para generar, enviar, recibir, recuperar, procesar o almacenar información de cualquier forma o por cualquier medio. Dato informático o información: toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático."
Chiapas	439, 440, 441, 442	Acceso ilícito a sistemas de informática. Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo o sistema de seguridad o al que no tenga derecho a accesar. Al que, sin autorización accese, modifique, copie, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública protegida… Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, innecesariamente o en perjuicio de otro o del servicio público modifique, destruya o provoque pérdida de información… Al que estando autorizado para acceder a sistemas y

[104] Reformada su denominación, P.O. 1 de marzo de 2010.

		equipos de informática de alguna dependencia pública, sin autorización copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y de cien a trescientos días multa
Colima	240 Bis	Delito Informático[105] Se le impondrá una pena de seis meses a seis años de prisión y multa de trescientos a mil unidades al que de manera dolosa y sin derecho alguno, ni autorización de quien pueda otorgarlo conforme a la Ley, utilice o tenga acceso a una base de datos, sistemas o red de computadoras o a cualquier parte de la misma, con el firme propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información en perjuicio de otro.
Chihuahua	327 Bis, 327 ter, 327 Quarter, 327 Quinquies	Del uso y acceso ilícito a los sistemas y equipos informáticos y de comunicación[106] Al que diseñe, programe, fabrique, introduzca, importe, comercialice o distribuya programas de cómputo Al que valiéndose de equipos informáticos o de comunicación, utilice indebidamente, datos o información personal Las penas previstas en este Capítulo se incrementarán en una mitad cuando las conductas sean cometidas en contra de una entidad pública estatal o municipal.
Jalisco	143 Bis, 170 Bis	Al que sin autorización y de manera dolosa, copie, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática. Falsificación de medios electrónicos o magnéticos
Morelos	148 Quarter	De los Delitos Informáticos[107] Comete el delito informático, la persona que dolosamente y sin derecho:I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma…
Querétaro	159 Ter, 159 Quarter	Acceso ilícito a sistemas de informática[108] Al que sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos protegidos o no por algún sistema de seguridad… Al que sin autorización, por

[105] Adic. Dec. 294, aprob. 30 de abril de 2008.

[106] Capítulo adicionado con sus artículos 327 Bis, 327 Ter, 327 Quater y 327 Quinquies; mediante Decreto No. 344-2011 II P.O. publicado en el P.O.E. No. 93 del 19 de noviembre de 2011

[107] Adicionado P.O. 4844 de fecha 20 de octubre de 2010

[108] Adición P. O. No. 24, 22-Mayo-11

		cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos del Estado
Sinaloa	217	Delito Informático Comete delito informático, la persona que dolosamente y sin derecho: I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.
Tabasco	326 Bis, 326 Bis 1, 326 Bis 2	Delitos contra la seguridad en los medios informáticos y magnéticos[109], daño Informático, falsificación informática,
Tamaulipas	207 Bis, 207 Ter, 207 Quarter 207 Quinquies 207 Sexies	Acceso ilícito a sistemas y equipos de informática.[110] Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistema o equipo de informática Al que sin autorización conozca o copié información contenida en sistemas o equipos de informática de alguna dependencia pública Tipos penales señaldos sobre el acceso a sistemas y equipos de informática de dependencias publicas .
Veracruz	181	Delitos Informáticos Comete delito informático quien, sin derecho y con perjuicio de tercero: I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; o II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red…

[109] Reformado P.O. 6855 Spto. E 17-Mayo-2008

[110] Adición P.O. No. 154, del 25 de diciembre del 2001.

Partiendo del análisis de los tipos penales citados con anterioridad nos podemos percatar que se existen normas jurídicas en vigor con la finalidad de proteger el acceso a la confidencialidad e intimidad de la información como es el caso del Estado de Aguascalientes; o Estados como Chiapas, que incluso nos dan una definición de Sistema Informático, lo que representa un gran avance en la materia, y el Estado de Colima, nos proporciona un concepto de delito informático dirigido a la afectación patrimonial.

Sin embargo la brecha aun es grande, es necesario evidenciar que en el campo de derecho los conceptos informáticos a diario avanzan lo que deja desfasada a la norma jurídica, y por lo tanto la aplicación resulta inoperante.

.

CAPÍTULO V

ANÁLISIS DEL TIPO PENAL CONTENIDO EN EL ARTÍCULO 211 BIS 1 "ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA" DEL TITULO NOVENO CAPÍTULO II DEL CÓDIGO PENAL FEDERAL

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

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

1. BIEN JURÍDICO

Para Olga Islas Es el concreto interés individual o colectivo del orden social protegido en el tipo penal.[111]

Por consiguiente Edmund Mezger considera que este bien jurídico es, a la vez, el objeto de protección de la ley, o, considerado desde el punto de vista del delincuente, el objeto de ataque contra el cual se dirige el delito. El "bien jurídico" evidencia, con ello, el valor que posee para el individuo, como su portador directo, y para la sociedad como tal.[112]

También es importante destacar lo que señala Santiago Mir Puig, pues considera que el concepto de bien jurídico no se agota en la designación de un objeto aprehensible por los sentidos, sino que abarca a todos los procesos sociales cuya protección es necesaria para la subsistencia o funcionamiento de los sistemas sociales.[113]

---

[111] Islas de González Mariscal, Olga, *Análisis Lógico de los Delitos Contra la Vida*, 4ª. Edición, México, Trillas, 2004, p. 32.

[112] Mezger, Edmund, *Derecho Penal Parte General Libro de Estudio*, Argentina, Editorial Bibliografica Argentina, 1958, p. 155

[113] Mir Puig, Santiago, *Introducción a las bases del Derecho Penal*, 2ª. Edición , Argentina, Editorial B de F 2003, p. 144.

Es decir, el bien jurídico cumple una función esencial del derecho penal al establecer, a través de la protección de los bienes el mínimo ético social necesario para la convivencia en opinión de la mayoría, de tal manera, que es necesario un equilibrio entre la protección de la sociedad y la de los individuos.

De manera general el Bien jurídico protegido en cuestión sería, la **PROTECCIÓN DE LA INFORMACIÓN** ya que el artículo en cuestión cita: ***"modifique, destruya o provoque pérdida de información contenida en sistemas",*** aunque si bien es cierto, sabemos que a través de medios informáticos se pueden enumerar una serie de delitos cuyo bien jurídico esta enlazado concretamente a la conducta ilícita tipificada en el precepto legal.

Modificar, se refiere a cambiar una cosa sin alterar su naturaleza misma[114], ese cambio por obvias razones tendría que ser en detrimento de la información contenida en los sistemas informáticos, inutilizando la información contenida para un fin específico.

Destruir, proviene en su etimología del latín "destructĭonis", designando tanto el acto de arruinar o dañar en forma grave a algo o a alguien, como a la consecuencia o efecto de lo que queda arruinado, inservible o dañado[115], en este caso en la información contenida en sistemas, lo cual se refiere a un perjuicio o menoscabo que sufre el sujeto pasivo en su patrimonio, lo anterior aunado a la palabra *Pérdida*, que al igual que la destrucción es un daño o perjuicio de una cosa, en este caso de la información.

Conocer significa tener idea o noción de una persona o cosa, saber qué es o cómo es alguien o algo por haberlo visto, haber oído hablar de ello, haberlo estudiado, etc[116] es decir la información contenida en los sistemas informáticos. Y finalmente *copiar,* refiriéndose a transmitir o pasar a cualquier medio la información contenida en los sistemas.

Pablo Lucas Murillo considera que el derecho a la intimidad normalmente implica el poder jurídico de rechazar intromisiones ilegítimas en la esfera protegida, y correlativamente, determinar libremente y dentro de ella la propia

[114] *http://www.alegsa.com.ar/Definicion/de/modificar.php*

[115] *http://deconceptos.com/general/destruccion*

[116] *http://servicios.elpais.com/diccionarios/castellano/conocer*

conducta. E s un típico derecho de defensa. Conviene abandonar la referencia de la intimidad y enunciar un nuevo derecho (el derecho a la autodeterminación informativa), que tendría como objeto preservar la información individual (íntima y no íntima) frente a su utilización incontrolada arrancando, precisamente, donde termina el entendimiento convencional del derecho a la vida privada.[117]

Carlos Ruiz, distingue entre la intimidad física o clásica (libertad frente a toda intromisión sobre uno mismo, su casa, su familia, comunicaciones o relaciones) de la intimidad informativa (derecho a determinar cómo y en qué medida se puede comunicar a otros información sobre uno mismo).[118]

Al referirse a este caso concreto en que exista frente a la intromisión o acceso no autorizado una base de datos, sistemas o red de computadoras con que cuenta con o sin seguridad propiedad del sujeto pasivo.

Aunado ello, no debemos pasar desapercibos los bienes jurídicos como la vida, el desarrollo sexual, el patrimonio, etc., de los delitos que se pueden cometer una vez realizada la conducta de intromisión con la finalidad de producir un resultado ya tipificado como es el caso de la pornografía de menores a través de internet, entre otros.

2. SUJETO ACTIVO

Es toda persona que normativamente tiene la posibilidad de concretizar el contenido semántico de los elementos incluidos en el particular tipo penal.[119]

El actuar del sujeto activo está motivado por el ánimo de apoderarse, usar o conocer indebidamente la información contenida.

El Código Penal Federal prescribe que son personas responsables de los delitos los siguientes:

---

[117] Murillo de la Cueva, Pablo Lucas y Piñar Mañas, José Luis, *El derecho a la autodeterminación informativa*. Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 117.

[118] Ruiz Miguel, C arlos, *Protección de los datos personales automatizados*, Revista de Estudios Políticos (Nueva Época), Madrid, Centro de Estudios Constitucionales, núm. 84, abril-junio de 1994, p. 237.

[119] Islas de González Mariscal, Op. Cit. nota 111, p. 32.

Artículo 13.- Son autores o partícipes del delito:

I.- Los que acuerden o preparen su realización.

II.- Los que los realicen por sí;

III.- Los que lo realicen conjuntamente;

IV.- Los que lo lleven a cabo sirviéndose de otro;

V.- Los que determinen dolosamente a otro a cometerlo;

VI.- Los que dolosamente presten ayuda o auxilien a otro para su comisión;

VII.- Los que con posterioridad a su ejecución auxilien al delincuente, en cumplimiento de una promesa anterior al delito y

VIII.- los que sin acuerdo previo, intervengan con otros en su comisión, cuando no se pueda precisar el resultado que cada quien produjo.

Los autores o partícipes a que se refiere el presente artículo responderán cada uno en la medida de su propia culpabilidad.

En la descripción típica no se precisa como necesaria la concurrencia de dos o más personas, el delito por lo tanto es monosubjetivo aun cuando en forma contingente intervengan varios sujetos.[120] Si bien es cierto en este tipo de delitos también es dable la complicidad y es evidente que en estos tiempos esta conductas realizadas a través del ciberespacio pueden ser sujetas de asociaciones delictuosas detrás de estas, en relación a esto la Ley Federal contra la Delincuencia Organizada señala en su artículo 2: *"Cuando tres o más personas se organicen de hecho para realizar, en forma permanente o reiterada, conductas que por sí o unidas a otras, tienen como fin o resultado cometer alguno o algunos de los delitos siguientes, serán sancionadas por ese solo hecho, como miembros de la delincuencia organizada…"* Igualmente no se debe pasar por alto lo estipulado en el artículo 13 del código penal donde específica a los autores o participes del delito como los siguientes:

I.- Los que acuerden o preparen su realización.

II.- Los que los realicen por sí;

III.- Los que lo realicen conjuntamente;

[120] Castellanos Tena, Fernando, *Lineamientos Elementales de Derecho Penal*, 40ª. Edición, México, Porrúa, 2003, p. 283.

IV.- Los que lo lleven a cabo sirviéndose de otro;

V.- Los que determinen dolosamente a otro a cometerlo;

VI.- Los que dolosamente presten ayuda o auxilien a otro para su comisión;

VII.- Los que con posterioridad a su ejecución auxilien al delincuente, en cumplimiento de una promesa anterior al delito y

VIII.- los que sin acuerdo previo, intervengan con otros en su comisión, cuando no se pueda precisar el resultado que cada quien produjo.

Los autores o partícipes a que se refiere el presente artículo responderán cada uno en la medida de su propia culpabilidad.

Este Tipo penal no requiere una calidad específica debido a que no menciona una característica exigida y necesaria para los sujetos a quien va dirigido el deber.

Marcelo Huerta y Claudio Líbano dicen que es cierto que muchos de los delitos se cometen desde dentro del sistema por personas que habitualmente lo operan y que tienen autorizado los accesos (Insiders). Sin embargo, las tendencias modernas apuntan hacia el campo de la teleinformática a través del mal uso del ciberespacio y las supercarreteras de la información o redes de telecomunicaciones. Es decir, cada día gana más terreno el delito informático a distancia. (Outsiders).[121]

Aunque es importante hacer mención que existe quien considera que por estar la computación tan extendida cualquier persona que posea conocimientos mínimos de informática y tenga acceso a un ordenador, incluso desde su casa, puede realizar un delito informático. En tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.[122]

[121] Huerta Miranda, Marcelo Y Líbano Manzur Claudio, *Los Delitos Informáticos*, Chile, Editorial Jurídica Cono Sur,1998.

[122] Palazzi Pablo, Andres, *Delito Informático.* Buenos Aires Argentina, Editorial Ad Hoc S.R.L. 2000.

SUJETO ACTIVO INDETERMINADO: "Al que sin autorización modifique, destruya o provoque pérdida de información…"

"Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática…"

En concreto a este tipo penal tipificado en el Artículo 211 bis del Código Penal Federal no requiere una Calidad Especifica del Sujeto Activo, ya que no exige una característica en el Tipo hacía los sujetos a los que va dirigido el deber.

Así mismo el tipo no exige un número de sujetos necesarios para la realización de la conducta descrita en el tipo, es decir no requiere una Pluralidad Específica.

3. SUJETO PASIVO

Olga Islas lo define como el titular del bien jurídico protegido en el tipo. Es por ende, el elemento del tipo en el que se singulariza la ofensa inferida a la sociedad.[123]

Rodríguez Mourullo sostiene que es el titular directo del bien protegido por la norma y ofendido por la acción descrita en el tipo (el titular de la vida en el homicidio, el titular del derecho real de propiedad en la apropiación indebida, etc.).[124]

Respecto del sujeto pasivo, se habla de personas físicas o morales, cabe hacer mención que para que contemplar el sujeto pasivo en esta clase de delitos deberá cumplirse con una condición relevante, como es la de ser titular de información de carácter privado y confidencial en formato digital, de los sistemas o equipos de informática protegidos por algún mecanismo de seguridad y que dicha posea un valor relevante para el sujeto.

El sujeto pasivo es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él se puede conocer los diferentes ilícitos que

[123] Islas de González Mariscal, Olga, Op. Cit., nota 111, p. 41

[124] Rodriguez Mourullo, Gonzalo, *Derecho Penal. Parte General*, España, , Editorial Civitas S.A., 1978, p. 282

cometen los delincuentes informáticos, Los sujetos en quien recae el daño pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, entre otros, quienes utilizan sistemas automatizados de información, generalmente conectados unos a otros.

No se requiere calidad específica por lo que cualquiera puede ser sujeto pasivo, ni pluralidad específica pues no lo exige el tipo penal en mención.

Este tipo de delitos se caracterizan por la dificultad para descubrirlos y derivado de esto su probación y persecución, motivo por el cual no se denuncian por el sujeto pasivo, lo que agrava el conocimiento de las autoridades en las cifras de este tipo de delitos y por lo tanta la no adecuada planificación de medidas preventivas y sancionadoras a tales acciones ilícitas, aunado a esto contribuye la falta de preparación por parte de las autoridades, todo lo anterior trae como consecuencia que las estadísticas sobre este tipo de conductas contribuyan a la denominada cifra negra.

4. OBJETO MATERIAL

Amuchategui refiere que es la persona o cosa sobre el cual recae directamente el daño causado por el delito cometido o el peligro en que se colocó a dicha persona o cosa.[125]

Rodríguez Mourullo señala que es el objeto de acción, también llamado objeto material, es la persona, (objeto material personal) o cosa (objeto material real) sobre la que incide la acción descrita en el tipo. Por ejemplo la persona sobre la que recae la acción de matar. Objeto material y sujeto pasivo, aunque en el plano conceptual son siempre susceptibles de distinción, pueden coincidir de hecho. Sucede así, por ejemplo, en el Homicidio, en este caso objeto material y sujeto pasivo (titular del bien jurídicamente protegido) es la misma persona a quien se priva de la vida, es decir, sobre la que incide la acción letal... Hay delitos con

[125] Amuchategui Requena, Griselda, *Derecho Penal,* 3ª Edición, México, Oxford University Press, 2010, p.40.

pluralidad de objetos materiales...y hay por el contrario tipos que carecen de objeto material.[126]

En el caso del artículo en mención sería:

Sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad; sin embargo y mediante el análisis de esta conducta se presenta la imposibilidad de establecer que es un "mecanismo de seguridad" cuyo término no es definido y puede ser tomado desde diferentes aspectos, aunado a que este tipo penal no hace alusión a aquellos sistemas que no cuenten con mecanismos de este tipo; en materia de actividades bancarias, financieras contamos con la protección al acceso a este flujo de información no obstante y a pesar de encontrarse tipificado como tal, no se cuenta con los mecanismos o instrumentos idóneos que resulten eficaces para el apoyo de la defensa a los ataques a este sector, que resulta mayormente vulnerable dado el derrame económico que se desenvuelve diariamente con los diversos movimientos y transacciones bancarias entre usuarios de estos sistemas que generen un intercambio seguro.

Dentro de la Seguridad Informática se mencionan algunos tipos de mecanismos de seguridad según su función que desempeñen como los siguientes[127]:

- Control de acceso. Como nombre de usuario y contraseñas.
- Cifrado de datos (Encriptación). Es el proceso de intentar regenerar el mensaje desde el texto cifrado pero sin conocimiento de las claves de encriptacion. Esta es la tarea normal de los intrusos. Si el intruso o criptoanalista no puede determinar un mensaje desde el texto cifrado (sin

[126] Rodriguez Mourullo, Gonzalo, Op. Cit. Nota 124, p. 357

[127] Aguilera Purificación, *Seguridad Informática*, , España, Editorial Editex, 2010, p. 17

la clave), entonces el sistema de criptografiado es seguro [128]. El cifrado de datos fortalece la confidencialidad.

- Antivirus. Detectan e impiden la entrada de virus y otro software malicioso. En caso de infección tienen la capacidad de eliminarlos y corregir los daños que ocasionan en el sistema.
- Contrafuegos (firewall). Se trata de uno o más dispositivos de software, de hardware o mixtos que permiten, deniegan o restringen el acceso al sistema. Protege la integridad de la información.
- Firma digital. Se utiliza para la transmisión de mensajes telemáticos[129] y en la gestión de documentos electrónicos. Su finalidad es identificar de forma segura a la persona o al equipo que se hace responsable del mensaje o del documento. Protege la integridad y la confidencialidad de la información.
- Certificados digitales. Son documentos digitales mediante los cuales una entidad autorizada garantiza que una persona o entidad es quien dice ser, avalada por la verificación de su clave pública. Protege la integridad y la confidencialidad de la información.

5. LOS MEDIOS UTILIZADOS

Indeterminados; los adecuados y necesarios para desplegar la conducta de sin autorización modificar, destruir o provocar pérdida de información, conocer o copiar información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

Algunos de los medios para desplegar la conducta fueron citados anteriormente en el capítulo cuatro de este proyecto de investigación,

[128] http://sistemasoperativos.angelfire.com/html/6.8.html.

[129] En seguridad informática, código malicioso es un término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso. Esta definición incluye tanto programas malignos compilados, como macros y códigos que se ejecutan directamente, como los que suelen emplearse en las p.inas web (scripts). http://www.alegsa.com.ar/Dic/codigo%20malicioso.php

particularmente en el uso de códigos maliciosos[130] los cuales son programas de cómputo diseñados para hacer que los equipos de cómputo (móviles y fijos) realicen procesos o acciones distintas a las que fueron programados originalmente sin el consentimiento del usuario cuyos objetivos son:

a. Ataque a sistemas de archivos.

b. Ataque a sistemas operativos.

c. Ataque a sistemas de procesamiento.

d. Ataque a sistemas de comunicación.

e. Ataque a sistemas de almacenamiento.

f. Ataque a extensiones de archivo específicas.

g. Ataque a aplicaciones específicas.

6. CONDUCTA

Para Fernando Castellanos La conducta es el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito.[131]

Olga Islas lo define como el proceder finálistico descrito en el tipo, se constituye por una voluntad y un hacer algo, o una voluntad y un dejar de hacer algo (Acción u Omisión).[132]La conducta es siempre un acto voluntario que va dirigido a un fin.

Para Raúl Carrancá Trujillo y Raúl Carrancá Rivas establecen para este elemento del delito que lo primero para que el delito exista es que se produzca una conducta humana. La conducta es, así, el elemento básico del delito. Consiste en el hecho material, exterior, positivo o negativo, producido por el hombre. Si es positivo consistirá en un movimiento corporal productor de un resultado como efecto, siendo ese resultado un cambio o un peligro de cambio en el mundo

[130] Mayor información en Glosario.
[131] Castellanos Tena, Fernando, Op. Cit nota 120, p. 154.
[132] Islas de González Mariscal, Olga, Op. Cit. nota 111., p. 42

exterior, físico o psíquico. Y si es negativo, consistirá en la ausencia voluntaria del movimiento corporal esperado, lo que también causará un resultado.[133]

Para el caso del tipo penal en cuestión se trata de una acción o conducta positiva sin autorización por parte del sujeto activo, dando como resultado modificar, destruir o provocar pérdida de información, conocer o copiar información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

Es importante tomar en cuenta dentro de la conducta el sistema finalista de la acción, cuya característica principal es la atención en la finalidad que ha guiado la conducta del sujeto para la lesión del bien jurídico tutelado.[134] Autores como Moisés Moreno argumentan que: *La dirección de las normas a la finalidad, esto es a la voluntad de realización, es una condición de la posibilidad de que el derecho penal pueda cumplir su tarea.*[135]Para finalizar y sintetizar lo anteriormente expuesto y que engloba un concepto más preciso en relación al finalismo respecto a la conducta Welsel afirmo que: *El carácter finalista de la acción, se basa en que el ser humano, gracias a su saber causal, puede prever dentro de ciertos límites, las consecuencias posibles de su conducta; asignarse por tanto, fines diversos y dirigir su actividad conforme a un plan, a la realización de esos fines.*[136]

DOLO

Consiste en causar intencionalmente el resultado típico, con conocimiento y conciencia de la antijuridicidad del hecho.[137]

El Código Penal Federal define al Dolo de la siguiente manera:

---

[133] Carrancá y Trujillo, Raúl y Carrancá y Rivas, Raúl, *Derecho Penal Mexicano (Parte General).* Vigésima tercera edición, México, Editorial Porrúa 2007.p. 295.

[134] Díaz Aranda, Enrique, et al., *Problemas Fundamentales de Política Criminal y Derecho Penal,* México, UNAM, 2012. p.19

[135] Moreno Hernández, Moisés, *Modernas tendencias en la ciencia del derecho penal y la criminología*, Madrid, Universidad Nacional de Educación a Distancia, 2001, p. 603.

[136] Welzel, Hans, *El nuevo sistema del derecho penal. Una introducción a la doctrina de la acción finalista,* Barcelona, Ariel, 1964, y notas de Cerezo Mir, José, trad. De la 4ª. ed. alemana, Montevideo, Buenos Aires, B de F, p.41.

[137] Islas de González Mariscal, Olga, Op. Cit. nota 111., p. 45.

Artículo 9o.- Obra dolosamente el que, conociendo los elementos del tipo penal, o previendo como posible el resultado típico, quiere o acepta la realización del hecho descrito por la ley,

En este tipo penal se podría analizar por voluntad dolosa todas aquellas acciones y mecanismos de interferir sistemas de información mediante el despliegue de operaciones con conocimientos avanzados en el tema.

Este delito presupone una conducta dolosa, toda vez que el agente o sujeto activo cuenta con los conocimientos necesarios para poder manipular la información de cualquier ordenador y tiene toda la intención para hacerlo.

El sujeto activo actúa dolosamente, es decir, comprende el sentido formal de los elementos esenciales del tipo penal y quiere la realización de dichos elementos, quiere realizar la acción delictiva, en este caso modificar, destruir o provocar pérdida de información.

La acción dolosa para la configuración de cualquiera de los tipos posibles implica, al menos un acceso ilegítimo a equipos protegidos por algún mecanismo, violentándose los sistemas de seguridad.

7. TIPICIDAD

Se entiende por tipicidad la correspondencia unívoca, uno a uno, entre los elementos del tipo penal y los contenidos del delito; es decir que para cada elemento del tipo tiene que haber una porción de contenido del delito que satisfaga la semántica de aquel y para cada porción del contenido del delito tiene que haber un elemento del tipo que exija su concreción.[138]

Es importante hacer mención que en el Código Penal solo se encuentra Tipificado este delito dentro de los artículos 211bis 1 al 211bis 7, no obstante existen conductas que se pueden llevar a cabo a través de medios informáticos, las cuales encuadran perfectamente en una serie de delitos enumerados en capítulos anteriores.

[138] Islas de González Mariscal, Op. Cit. nota 111, p. 55

Por lo anteriormente planteado, se podría pensar que son los mismos tipos penales o acciones lesivas ya tipificadas, pero con diferente forma de realización, si ese fuera el caso, se necesitarían modificaciones relevantes para que la tipicidad pueda encuadrar perfectamente en el tipo correspondiente, subsanando de manera general tanto la nueva forma del tipo penal como la antes existente.

Es importante destacar el papel del juzgador para conocer si el elemento de tipicidad se encuentra totalmente comprobado, para dar un veredicto apegado a la ley, ya que podría ser difícil o hasta imposible, si los legisladores no establecen claramente los elementos del delito, para así evitarlos o en su momento castigarlos de tal manera que se pueda dar una total coexistencia de la conducta en la descripción del tipo penal con la Ley.

8. ANTIJURIDICIDAD.

Mezger la define como una acción es punible sólo si es antijurídica. La antijuridicidad, o, como se acostumbra decir en la actualidad, el injusto, es el presupuesto imprescindible de todo hecho punible. Sencillamente, que el delito constituye una violación del derecho, o sea que "contradice el derecho". Hoy, en virtud de la aversión que se tiene a conceptos rigurosos y cierta predilección por expresiones más vagas, se prefiere emplear, la palabra injusto (literalmente: no derecho), que determina el concepto, precisamente, con menor exactitud que la otra empleando ambas expresiones (antijuridicidad e injusto) como sinónimas.[139]

Díaz Aranda, menciona que la antijuridicidad se establece si la conducta prohibida es contraria al orden jurídico en general, y por ello al hecho típico y antijurídico se le denomina “injusto”. Por el contrario, si el hecho típico está amparado por alguna causa de justificación ya no hay delito.[140]

Como su nombre lo indica, es la contradicción de la conducta con el ordenamiento jurídico.

[139] Mezger, Edmund, Op. Cit, nota 112, p. 131

[140] Díaz-Aranda, Enrique, *Derecho Penal Parte General*, 2ª Edición, México, Porrúa, 2004 p. 301

La prohibición de una conducta no queda garantizada con el solo encuadramiento de la conducta en el tipo (tipicidad). Para la existencia de la antijuridicidad se requiere de dos requisitos:

1. La adecuación de una conducta a un tipo penal, es decir, la presencia de una acción típica.
2. Que la acción típica no esté amparada por una causa de justificación.

Para ser más específicos a continuación se hace mención de los elementos del Juicio de Antijuridicidad, los cuales consisten en hacer un examen que permita explicar por qué una acción es antijurídica:

a) Que se trate de una acción típica.
b) Que no exista ninguna causa de justificación.
c) Que exista plena desvaloración de la acción (Culpa o Dolo).
d) Que exista pleno desvalor del resultado (Resultado Material o resultado formal)[141].

9. CULPABILIDAD

Es la reprochabilidad del hecho[142] típico y antijurídico, es un juicio de reproche hacía el autor por haber obrado en contra de la norma, pudiendo haber obrado de acuerdo a ella.

Edmund Mezger define la culpabilidad como el conjunto de los presupuestos que fundamentan el reproche personal al autor por el hecho punible que ha cometido.[143]

Tiene dos elementos estructurales:

1. Imputabilidad.- Capacidad de comprensión de lo injusto de su actuar y de conducirse de acuerdo a esa comprensión.

[141] Plascencia Villanueva, Raúl, *Teoría del Delito,* Instituto de Investigaciones Jurídicas UNAM, México, 2004.
[142] Ebert Udo, *Derecho Penal Parte General,* Traducción Escudero Said, talleres Gráficos de la UAEH, México 2005 p. 112
[143] Mezger, Edmund, op. cit, nota 112., p. 131

2. Conocimiento de la Antijuridicidad.- Comprensión de lo antijurídico de la conducta y conciencia en el momento de la realización del acto de lo ilícito de su actuar.

El tipo penal en análisis reúne los dos elementos estructurales de la culpabilidad ya que se tiene la comprensión de su conducta y conciencia para modificar, destruir, provocar pérdida de información, conocer o copiar información contenida en sistemas o equipos de informática, además en este artículo esta reiterada la comprensión que lo está haciendo *"Sin autorización…"*

10. CLASIFICACIÓN DE LOS TIPOS PENALES

Al referir los tipos penales, es plausible elaborar una clasificación atendiendo a su estructura formal; en tal virtud, es factible agruparlos en: básicos, especiales, subordinados, elementales, compuestos, autónomos, en blanco, de daño, de peligro, abiertos o cerrados.[144]

a) Básicos. Conocidos igualmente como fundamentales, son aquellos en los que se describe de manera independiente un modelo de comportamiento humano y, por esa razón, se aplican sin sujeción a ningún otro. Por lo regular, estos tipos encabezan cada uno de los capítulos del Código y constituyen su espina dorsal;

b) Especiales. Los que además de los elementos propios del básico, contienen otros nuevos o modifican requisitos previstos en el tipo fundamental; por eso se aplican con independencia de éste.

c) Subordinados o complementados. Los que refiriéndose a uno básico o especial, señalan determinadas circunstancias o aspectos que cualifican la conducta, los sujetos o el objeto descrito en éstos; por esa razón no pueden aplicarse en forma independiente; su vida jurídica depende de la del tipo básico o especial al cual se refieren y los efectos de su aplicación sólo en el momento procesal de la imposición de la pena;

En sentido similar Castellanos Tena considera que los tipos penales pueden ser clasificados en: normales, anormales, fundamentales, básicos, especiales,

[144] Reyes Echandía, Alfonso, *Derecho penal*, Bogotá, Editorial Temis, 2002 , p. 112

complementados, autónomos, subordinados, casuísticos, amplios y de daño o de puesta en peligro.[145]

Tanto los tipos especiales como los subordinados pueden ser privilegiados o agravados; aquéllos prevén una sanción más leve que la de los básicos o los especiales, y éstos, una de mayor gravedad.

d) Compuestos. Los que describen una pluralidad de conductas, cada una de las cuales podría conformar un tipo distinto, aunque referido al mismo bien jurídico; se identifican sin mayor dificultad porque tienen varios verbos rectores.

e) Autónomos. Los que describen un modelo de comportamiento al cual puede adecuarse directa o inmediatamente la conducta del actor, sin que el intérprete deba aludir al mismo o a otro ordenamiento jurídico para completar su significado;

f) En blanco. Aquellos cuya conducta no está integralmente descrita en cuanto el legislador se remite al mismo o a otro ordenamiento jurídico para actualizarla o precisarla; mientras tal concreción no se efectúe, resulta imposible realizar el proceso de adecuación típica.

g) De daño o de puesta en peligro. Los primeros requieren para su concreción que el bien jurídico sea destruido o lesionado, y los de puesta en peligro sólo toman en consideración la posición de riesgo en la cual se coloca el bien jurídico.

h) Abiertos. Dentro de las leyes penales existen casos en los que el legislador adopta una concepción abierta en torno al tipo penal, es decir, la descripción sólo es comprensible a partir del complemento que realice otro texto legal; así, Jescheck considera que reciben el nombre de tipos abiertos aquellos preceptos penales en los que falta una guía objetiva para completar el tipo, de modo que en la práctica resultaría imposible la diferenciación del comportamiento prohibido y del permitido con la sola ayuda del texto legal, en atención a dicha consideración el autor rechaza la idea en torno a los tipos abiertos prefiriendo una concepción cerrada del tipo que no deje margen a maniobras derivadas de otros tipos penales, ya que de lo contrario le faltaría precisamente el carácter típico.

[145] Castellanos Tena, Fernando, *op cit nota 120*, p. 171

Esto significa que el tipo ha de contener todos, sin excepción, los elementos que contribuyen a determinar el contenido de injusto de una clase de delito.

Un ejemplo de tipo abierto es el previsto en el artículo 171 del CPF, que a la letra señala

: Artículo 171. Se impondrá prisión hasta de seis meses, multa hasta de cien pesos y suspensión o pérdida de derecho de usar licencia de manejador: [...]

II. Al que en estado de ebriedad o bajo el influjo de drogas enervantes cometa alguna infracción a los reglamentos de tránsito y circulación al manejar vehículos de motor, independientemente de la sanción que le corresponde si causa daños a las personas o a las cosas.

Como se puede apreciar, al momento concretarse el tipo penal es necesario rellenar su contenido con lo previsto los reglamentos de tránsito, lo cual supone al tipo con un contenido abierto que requiere ser complementado, cuestión que en el caso del artículo en comento ha propiciado que la doctrina los refiera como tipos penales en blanco, al remitir su contenido a una ley de carácter administrativo.

i) Cerrados. Son aquellos que resultan suficientes en todos y cada uno de sus elementos por sí mismos, ejemplo de estos tendríamos el previsto en el artículo 302. Comete el delito de homicidio: el que priva de la vida a otro.

De lo anterior, se puede observar cómo el tipo resulta plenamente satisfecho con lo dispuesto en el artículo 302, sin necesidad de recurrir en el caso del homicidio simple a otra consideración para completar.

En referencia al Tipo Penal objeto de estudio, se ubica en la siguiente clasificación:

Básico: ya que se describe de manera independiente un modelo de comportamiento humano: *“Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad…”*

“Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad…”

Autónomo: Describe un modelo de comportamiento al cual puede adecuarse directa o inmediatamente la conducta del actor, sin que el intérprete deba aludir al mismo o a otro ordenamiento jurídico para completar su significado.

De daño: Requieren para su concreción que el bien jurídico sea destruido o lesionado, "*modifique, **destruya** o provoque **pérdida de información** contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad…"*

Cerrado: Resulta suficiente en todos y cada uno de sus elementos por sí mismos.

11. CIRCUNSTANCIAS DE LUGAR, TIEMPO, Y OCASIÓN[146]

Referencia de Temporal: Es la condición de tiempo o lapso, descrita en el tipo, dentro de la cual ha de realizarse la conducta o producirse el resultado.

Referencia Espacial: Es la condición del lugar, señalada en el tipo, en que ha de señalarse la conducta o producirse el resultado.

Referencia de Ocasión: Es la situación especial requerida en el tipo, generadora de riesgo para el bien jurídico, que el sujeto aprovecha para realizar la conducta o producirse el resultado.

En este rubro cabe hacer mención que si bien es cierto el tipo penal no requiere una calidad específica, no obstante el sujeto activo presenta ciertas características que lo distinguen del común de los delincuentes, esto es, tiene habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos en donde se maneja información de carácter relevante, o bien cuenta con los conocimientos teóricos y prácticos respecto del uso de los sistemas informatizados.

El artículo 211 bis 1 del Código Penal Federal no especifica o condiciona alguna de las circunstancias anteriormente descritas.

[146] Islas de González Mariscal, Olga, Op. Cit. nota 111, p. 50

12. PUNIBILIDAD

Olga Islas refiere que la punibilidad es conminación de privación o restricción de bienes del autor del delito, formula por el legislador para la prevención general, y determinada cualitativamente por la clase de bien tutelado y cuantitativamente por la magnitud del bien y del ataque a este.[147]

La penalidad o punibilidad según Muñoz Conde es, una forma de recoger o elaborar una serie de elementos o presupuestos que el legislador por razones utilitarias, diversas en cada caso y ajenas a los fines propios del Derecho penal, puede exigir para fundamentar o excluir la imposición de una pena, la punibilidad, según sus defensores, tiene su razón de existir porque el injusto y la culpabilidad jurídico-penal no justifican por sí solos la pena; en todos los casos debe asegurarse además la necesidad práctica de hacer uso de la misma para la protección del orden social.[148]

En resumen entendemos que es la amenaza de una pena que establece la ley, para, en su caso, ser impuesta por el órgano jurisdiccional, de acreditarse la comisión de un delito.

Artículo 211 bis 1.- Primer Párrafo: "*Se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa."*

Segundo Párrafo: "Se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa."

[147] Islas de González Mariscal, Olga, Op. Cit. nota 111. p. 53

[148] Muñoz conde, Francisco, García Aran, Mercedes D*erecho Penal Parte General,* España, 8ª. Edición, Editorial Tirant lo Blanch, 2010, p. 459

CONCLUSIONES

Si bien es cierto, y ya analizado que en la legislación y jurisprudencia nacionales se hallan elementos para prevenir y castigar el uso indebido de medios informáticos y otras tecnologías, éstas no son suficientes pues además de que se encuentra dispersa, no se tiene el conocimiento de su existencia y sobre todo si esta se encuentra de manera específica en diferentes legislaciones, si a veces resulta difícil encontrar una conducta que se encuadre en un tipo penal en una sola ley como lo es el Código Penal Federal, cuanto y más laboriosa resultara la investigación o búsqueda de encuadrar un tipo que tiene relación con medios informáticos en varias o diferentes normas.

A medida que transcurre el tiempo el grado de complejidad y especialización de la tecnología y por obviedad de los propios delincuentes, se abre más el panorama y en términos coloquiales “el menú” para poder llevar a cabo conductas ilícitas a través de medios informáticos y otras tecnologías de manera global.

Quien resulta más vulnerable a ser víctima de este tipo de delitos son sobre todo quienes no poseen los conocimientos informáticos básicos a diferencia del sujeto activo. A lo largo de este proyecto se mencionó la falta de conocimiento en este tema en general por parte de la sociedad en materia de combate o protección de los delitos informáticos, aunado a esto, en México el gobierno federal, no ha considerado los delitos informáticos como una prioridad lo cual hará más difícil la lucha contra estas acciones ilícitas, aunado a esto se encuentran las crisis económicas a nivel mundial. Sobre todo en Europa, provocando una recesión general lo cual resulta un terreno prolífico para las actividades delictivas a través del internet y sacar provecho de la situación.

México no puede ser solo observador de los acuerdos o tratados internacionales en esta materia, se necesita tener un papel protagonista en esa materia y tomar en cuenta todas las acciones internacionales y medidas que en otros países han sido exitosas, pues en lo que respecta tan solo de América Latina, Venezuela, Chile y Colombia llevan una gran ventaja.

En la legislación Federal al parecer se camina al revés, pues es evidente que en las legislaciones locales se están tomando claras medidas en sus códigos, inclusive creando capítulos para el castigo de delitos informáticos, denominados como tales, a nivel Federal solo se hacen remiendas con las famosas adecuaciones a los artículos ya existentes como lo son en general los bis, ter, quarter, entre otros.

A pesar de que actualmente en el país se cuenta con la policía cibernética dependiente de la Secretaría de Seguridad Pública Federal y las de algunos estados, estos funcionan de manera preventiva o enmendadora y no en combate directo contra el crimen organizado en materia informática; debido al desconocimiento de la normatividad corporaciones como la anteriormente mencionada, no saben sus atribuciones que una ley de manera general les facultaría, así como sus limitantes para que no se violen los derechos tanto del sujeto activo como del probable responsable. Así mismo esta ley definiría al sujeto activo claramente como lo han hecho en algunas legislaturas estatales y por lo tanto teniendo bien definidos los elementos normativos, se encuadraría la conducta delictiva en un tipo penal especifico y existente en una ley y juzgar correctamente el delito del que podría ser objeto la víctima, además de evitar la consulta de otras legislaciones nacionales que en conjunto no reúnen todo lo necesario para castigar la conducta ilícita.

Es necesaria una legislación en Delitos Informáticos, ya que las nuevas tendencias hacía la tecnología da lugar a una serie de conductas ilícitas nuevas, las cuales no pueden encuadrarse a tipos penales existentes, pues específicamente el bien jurídico tutelado para cada una de estas es diferente a cada uno de estos.

PROPUESTAS

I. Por lo que respecta al gobierno federal se debe fortalecer la prevención y combate en este tipo de delitos desarrollando diferentes medios de información que lleguen a toda la sociedad.

II. Tomar las medidas pertinentes y la preparación o capacitación de parte de las autoridades encargadas de la procuración de justicia para la investigación, persecución y sanción de este tipo de delitos.

III. El Estado mexicano debe ser signatario de los instrumentos internacionales en materia de ciberdelincuencia los cuales pueden servir de patrón para la creación de una ley general, así como ser parte en convenios de colaboración internacional, lo cual ayudaría a poder hacer frente de manera conjunta al combate y prevención de los delitos informáticos.

IV. Creación de una Ley Federal de Conductas Ilícitas a través de Medios Informáticos y tecnologías de información cuya legislación secundaria sea el Código Penal Federal, haciendo énfasis en el capítulo de Acceso ilícito a sistemas y equipos de informática.

V. Creación de tipos penales que vayan enfocados de manera general a los códigos maliciosos y que prevengan las nuevas maneras o formas delictivas, ya que con los alcances que tengan o puedan tener las nuevas tecnologías de información resultaría difícil especificar.

VI. Sancionar con penas más severas y claras para quien utilice sus conocimientos para obtener acceso a mecanismos informáticos de manera ilícita, cuyo fin sea el menoscabo en el patrimonio de una persona física o moral y la utilización de sus datos personales.

VII. Las punibilidades deben de ser mayores o agregar un agravante en base al sujeto activo que las comete y la condición del sujeto pasivo. En relación al sujeto activo si se tratare de algún organismo gubernamental dentro de los tres niveles y en el sujeto activo cuando el sujeto este tenga alguna relación ya sea de trabajo, afinidad o amistad.

VIII. La ley deberá contener un capítulo de términos informáticos que defina los conceptos informáticos de mayor relevancia y sobre todo usados en esta para su mejor alcance y puesta en práctica.

IX. La Ley debe establecer el procedimiento o procedimientos para la investigación de los delitos informáticos tomando en cuenta la criminalística y computo forense de tal manera que cuando la investigación llegue a manos de la autoridad judicial correspondiente no se tenga duda alguna sobre esta y arroje los datos necesarios para su consignación o sentencia en su caso.

X. Se debe contemplar un apartado sobre la prueba electrónica o digital, de manera que indique los aspectos generales y procesos de la evidencia a manera de saber aportarla, descubrirla, generarla, y también lograr coadyuvar y lograr su desahogo. Así mismo se deben de cuidar los aspectos en cuanto a criminalística se refiere con la cadena de custodia.

XI. Establecer medidas de seguridad de índole técnica y organizativa que deben implementar las instituciones públicas y privadas sobre todo las financieras, así como su respectiva pena en caso de que estas no las contemplen.

XII. En base a la creación de una Ley General las legislaturas locales de cada uno de los estados deben tipificar dentro de sus Códigos Penales los delitos de nueva creación y su clasificación, como modelo base.

XIII. Se deben de crear normas procesales enfocadas a la acreditación de los delitos informáticos y electrónicos, y así lograr fundamentar y motivar la labor de los cuerpos especializados como el que existe actualmente en México denominado Unidad de Policía Cibernética, la cual depende de la Secretaría de Seguridad Pública Federal

GLOSARIO DE TÉRMINOS

802.11 o IEEE 802.11x. Serie de estándares convencionales para las comunicaciones de red inalámbrica. Existen diferentes versiones o modulaciones de 802.11. Los más conocidos son 802.11b y 802.11g. Las normas 802.11 también definen los protocolos de seguridad que incluyen WEP, WPA y WPA2

a. Ataque a sistemas de archivos

A. Instrucciones no autorizadas dentro de un programa legítimo. Estas instrucciones ejecutan funciones desconocidas al usuario no deseadas por el mismo.

Adware. Es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.

Amenaza. Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Amenazas Combinadas. Ataque que combina varios métodos de ataque tradicionales, como un gusano, un troyano y un registrador de pulsaciones de teclado. Para defenderse contra la mayoría de ellos, se requiere una combinación de herramientas de seguridad y capas de protección.

Amenazas polimorfas. Las amenazas polimorfas son aquellas que tienen la capacidad de mutar y en las cuales cada instancia del malware es ligeramente diferente al anterior a este. Los cambios automatizados en el código realizados a cada instancia no alteran la funcionalidad del malware, sino que prácticamente inutilizan las tecnologías tradicionales de detección antivirus contra estos ataques.

Antispam. Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus. Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El

antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones engañosas. Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

Armores. También conocido como virus blindado, es una forma muy peculiar de programación, donde el autor programa una serie de rutinas que usa como cubiertas o escudos (shells), en el archivo que contiene el virus, para que éste no pueda ser fácilmente rastreado y mucho menos desensamblado. Asimismo, para darle mayor protección, los autores de virus pueden utilizar utilitarios compresores de archivos, con parámetros cuya descompresión sea mucho más difícil para los desarrolladores de antivirus.

Ataque de negación de servicio **DoS**. Ataque a un ordenador o red que provoca una saturación en el ancho de banda o una sobrecarga en los recursos hasta que los servicios del ordenador o la red dejan de estar disponibles para los clientes. La negación de servicio también puede producirse cuando un código malicioso desconecta los recursos.

Ataques Web. Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Autoridad de certificación. En criptografía de clave pública, otro fabricante de confianza que autentica entidades y sus claves públicas. Para hacerlo, las autoridades de certificación emiten certificados digitales que confirman que una clave pública pertenece a la persona cuya firma digital se indica en el certificado.

b. Ataque a sistemas operativos

B. Cualquier programa que contenga otro subprograma con instrucciones no deseadas o virus.

Backup. Copia adicional de los archivos del ordenador que generalmente se guarda en un lugar físicamente separado de los originales. Resulta fundamental para la recuperación cuando se dañan o se pierden los archivos originales.

Blog. Proviene de "Web log" (registro web). Un sitio web donde un individuo publica entradas de diario o comentarios con cierta regularidad. Algunos propietarios de blogs permiten que otros escriban comentarios en su sitio.

Bluetooth o IEEE 802.15.1. Denominado de esa manera en referencia al rey danés del siglo X, Harald Blatan (Bluetooth), que fue conocido por unificar territorios. Se trata de una serie de estándares inalámbricos convencionales para las comunicaciones de corto alcance entre auriculares, teléfonos, PDAs (asistentes digitales personales), teclados y otros dispositivos inalámbricos diferentes. Bluetooth admite diversas medidas de seguridad, pero presenta fallos que pueden exponer los dispositivos que utilizan Bluetooth a ataques.

Bombas de Tiempo. Son programas que ejecutan órdenes destructivas al producirse alguna condición en el sistema: una determinada fecha, un determinado valor en un registro, una petición de interrupción, etc. Las bombas lógicas tienen la ventaja de poner tiempo entre el momento en que son instaladas y su activación, lo que permite a sus autores evitar ser relacionados con sus acciones.

Bot. Un bot es una computadora individual infectada con malware , la cual forma parte de una red de bots (bot net).

Botnet. Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección.

Bugware. Existen programas informáticos legales diseñados para realizar unas determinadas funciones, pero debido a una mala programación, a una deficiente organización de los recursos, o una inadecuada comprobación de

funcionamiento, pueden causar daño a los datos o al sistema, o pueden facilitar intrusiones o la fuga de información.

c. Ataque a sistemas de procesamiento

C. Cualquier programa que permita operaciones de monitoreo y/o control remoto del computador sin conocimiento del usuario. Este tipo de programas son llamados también Backdoor lo que se traduce a Puerta Trasera.

Caballo de Troya. Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

Canal web. Archivo, generalmente en formato XML, que contiene títulos y resúmenes de contenido web en constante cambio, como artículos de noticias, podcasts y blogs. Los canales web ofrecen vínculos a las versiones completas del contenido, mediante suscripción o para descarga única. También se pueden compartir y volver a publicar en otros sitios web y, de esa manera, se crea una especie de sindicación online. Consulte también *RSS*.

Carga destructiva. Una carga destructiva es la actividad maliciosa que realiza el malware. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el malware.

Certificado digital. También llamado *certificado de clave pública* o *certificado de identidad*. En criptografía de clave pública, certifica que una clave pública pertenece a la entidad que envía los datos cifrados o firmados digitalmente con esa clave. Los certificados digitales son emitidos por una autoridad de certificación y contienen la clave pública del emisor, más una firma digital que verifica que el certificado es auténtico y que la clave pertenece al emisor.

Ciberbullyng. Se entiende cualquiera de las posibilidades de uso de las nuevas tecnologías de la información y de la comunicación para hostigar con ensañamiento a su víctima. Belsey define el Ciberbullying como el uso de algunas Tecnologías de la Información y la Comunicación como el correo electrónico, los mensajes del teléfono móvil, la mensajería instantánea, los sitios personales vejatorios y el comportamiento personal en línea difamatorio, de un individuo o un grupo, que deliberadamente, y de forma repetitiva y hostil, pretende dañar otro[149].

Ciberdelito. El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Cibertalking. Cuando una persona es seguido y perseguido en línea. Su privacidad es invadida, todos sus movimientos vigilados. Es una forma de acoso que pueden alterar la vida de la víctima y se dejan sentir mucho miedo y amenaza. El también llamado acoso cibernético por lo general ocurre con las mujeres, que son acosadas por los hombres, o niños que son acosados por los depredadores adultos y pedófilos. Por lo general, la víctima del cibertalking es nuevo en la web, y sin experiencia con las reglas de la seguridad en Internet.[150]

Cifrado. Método de seguridad que vuelve la información ilegible a quien no tenga la clave para descifrarla. Se utiliza generalmente para proteger las compras y otras transacciones de Internet. Cuando un sitio web indica que es “seguro”, generalmente se refiere a que los datos que se envían y se reciben están cifrados. Consulte también *criptografía de clave pública*.

Clave privada. En el cifrado asimétrico, clave no publicada usada para descifrar mensajes cifrados con una clave pública correspondiente.

Clave pública. En el cifrado asimétrico, clave que se pone a disposición de cualquier usuario que desee enviar un mensaje cifrado al propietario de la clave.

---

[149] Belsey Bill, creador del sitio web *www.bullying.org*

[150] Parte del documento presentado en la 29 ª Conferencia de Criminología India, durante el 16-18 de 2006 en la Universidad Madurai Kamaraj, Madurai,India.

El propietario de la clave pública usa su clave privada para descifrar los mensajes.

Códigos Maliciosos[151]Programas de cómputo diseñados para hacer que los equipos de cómputo (móviles y fijos) realicen procesos o acciones distintas a las que fueron programados originalmente sin el consentimiento del usuario.

Companion. Modalidad por la cual el virus en lugar de modificar un archivo existente, al infectarlo crea un nuevo archivo del mismo nombre, el cual es inadvertido por el usuario. Cuando un programa es ejecutado, por ejemplo IEXPLORE.EXE, éste invoca al popular navegador de Internet, pero el virus ya ha creado un falso IEXPLORE.COM, de tal modo que éste es ejecutado en primer lugar, por ser un archivo COM de una sola imagen (máximo 64k) y puede arrastrar el código viral sin que el usuario se percate. Y así continuará haciéndolo. Mas aún, los verificadores de integridad (integrity checkers) fallarán en la acción de detectar este tipo de virus ya que éstos utilitarios solo buscan los archivos existentes.

Cookie. Pequeño archivo de texto que se ubica en el ordenador o al visitar una página web. Se utiliza para recordar el usuario o sus preferencias cuando vuelva a visitar esa página o para realizar un seguimiento de sus actividades de navegación. Las cookies facilitan el uso de carritos de la compra virtuales, la personalización de páginas y la emisión de publicidad seleccionada. No son programas y no pueden leer el disco duro ni causar daños en el ordenador.

Crimeware. Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software.

Cuando se accede a un canal de IRC, se recibe por DCC un archivo llamado "script.ini.

d. Ataque a sistemas de comunicación

[151] LIRA Arteaga, José Manuel, *Cibercriminalidad Fundamentos de Investigación en México,* México, Editorial INACIPE, 1ª. Edición, , 2010.

- Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.
- Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Definiciones de virus. Una definición de virus es un archivo que proporciona información al software antivirus, para identificar los riesgos de seguridad. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las definiciones de virus también se denominan firmas antivirus.

Dirección IP. Dirección de protocolo de Internet. Identificador exclusivo para cada ordenador u otro dispositivo en una red, incluso Internet. Las direcciones IP, similares a un número telefónico, son una serie de números que permiten a los ordenadores, los routers, las impresoras y otros dispositivos reconocerse (identificarse) entre sí y comunicarse.

Dirección URL. Localizador uniforme de recursos (Uniform Resource Locator) Dirección de un sitio web o una página web (por ejemplo, www.symantec.es o www.symantec.com/es/es/home_homeoffice/index.html). Los navegadores usan las direcciones URL para identificar y descargar páginas web de los servidores web en donde se encuentran.

e. Ataque a sistemas de almacenamiento

Ejércitos de botnets o zombies. Grupo de ordenadores que han sido atacados y puestos bajo el control de una persona. Algunas personas usan malware instalado en los ordenadores atacados para lanzar ataques de negación de servicio, enviar spam o perpetrar otros actos maliciosos.

Encriptación. La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

f. Ataque a extensiones de archivo específicas

Falsificación de dominio o Secuestro de dominio. Manipulación del sistema de nombres de dominio con el fin de asociar una dirección web legítima con un sitio web falso o malicioso. Se utiliza en actividades de phishing y para realizar otros tipos de ataque. Se dirige al usuario al sitio web falso con advertencia insuficiente o nula.

Falsificación de URL. Intento de enmascarar o imitar fielmente la dirección URL que aparece en la barra de direcciones del navegador web. Usado en ataques de phishing y otras estafas de Internet para que un sitio web falso parezca legítimo. El atacante oculta la dirección URL real al superponer una dirección que parece legítima o una dirección URL similar.

Filtración de datos. Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados

Firewall. Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Firma antivirus. Una firma antivirus es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las firmas antivirus también se denominan definiciones de virus.

Firma digital. Utilizada en la criptografía de clave pública para validar la integridad de los datos cifrados y confirmar tanto la identidad del titular del certificado digital como la autenticidad del certificado.

FTP. Protocolo de transferencia de archivos. Serie de pautas de comunicación convencionales para la transferencia de archivos entre ordenadores online. Si bien la mayoría de los navegadores web permite transferir archivos mediante FTP, también se puede usar un programa de FTP específico, que suele ofrecer mejores funciones de seguridad.

g. Ataque a aplicaciones específicas.

Gusanos. Un gusano se puede decir que es un set de programas, que tiene la capacidad de reproducir un segmento de él o su propio cuerpo a otras computadoras conectadas a una red.

Hacker. Por lo general, hace referencia a una persona que utiliza sus habilidades de programación y conocimientos técnicos para obtener acceso no autorizado a sistemas informáticos con fines maliciosos o delictivos. Sin embargo, entre los programadores, se prefiere utilizar el término "cracker" para tales personas, y reservar el término "hacker" para todo programador altamente capacitado y respetado.

Hay dos tipos de Gusanos:

Hipervínculo. Palabra, frase o imagen seleccionable que traslada al usuario de una página web a otra o a un recurso online. Los hipervínculos se crean utilizando marcas HTML y, cuando se muestran en un navegador, suelen mostrarse subrayados o resaltados con un color diferente.

Hoaxes. Los Hoaxes pueden ser mensajes de alerta o advertencia relacionada con código malicioso desconocidos de diversos tipos. Estos mensajes informan que ha aparecido una nueva especie viral, la misma que se está propagando a través de los canales de Internet para destruir la información o afectar a los sistemas de las computadoras". Estos mensajes deliberadamente falsos, son creados con la grave intención de provocar pánico provocando, a través de los propios usuarios, una reacción en cadena que ocasiona la saturación de los buzones de correo y la congestión de las conexiones en Internet.

HTML. Lenguaje de marcado de hipertexto. El lenguaje principal utilizado para crear y dar formato a las páginas web. Controla la distribución, el diseño y la presentación de textos, hipervínculos, imágenes y otros elementos en la mayoría de las páginas web.

HTTP. Protocolo de transferencia de hipertexto. Serie de pautas de comunicación convencionales utilizadas para controlar la transmisión de información en servidores y navegadores web por Internet.

HTTPS. Convenciones de HTTP para la transmisión de información a un servidor que se encuentra protegido con medidas de cifrado o autenticación. La dirección URL de los sitios web que ofrecen conexiones HTTP seguras comienza con https://.

I. Host Computer Worm: son contenidos totalmente en una computadora, se ejecutan y se copian a si mismo vía conexión de una red. Los Host Computer Worm, originalmente terminan cuando hicieron una copia de ellos mismos en otro host. Entonces, solo hay una copia del gusano corriendo en algún lugar de una red. También existen los Host Computer Worm, que hacen una copia de ellos mismos e infectan otras redes, es decir, que cada máquina guarda una copia de este Gusano.

II. Network Worms: consisten en un conjunto de partes (llamadas “segmentos”), cada una corre en una maquina distinta (y seguramente cada una realiza una tarea distinta) y usando la red para distintos propósitos de comunicación. Propagar un segmento de una maquina a otra es uno de los propósitos. Los Network Worm tienen un segmento principal que coordina el trabajo de los otros segmentos, llamados también “octopuses”.

Keystroke Logger o Programa de captura de teclado (Keylogger).

Los macro virus son pequeños programas escritos en el lenguaje propio (conocido como lenguaje script o macro lenguaje) propio de un programa. Así nos podemos encontrar con macro virus para editores de texto, hojas de cálculo y utilidades especializadas en la manipulación de imágenes.

Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar

códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web malicioso.

Macro Virus. Representan una amenaza tanto para las redes informáticas como para los ordenadores independientes. Su máximo peligro está en que son completamente independientes del sistema operativo o de la plataforma.

Malware. El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.

MIRC. Son una nueva generación de programas que infectan las PC's, aprovechando las ventajas proporcionadas por Internet. Consisten en un script para el cliente de IRC Mirc.

Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

Mutantes. Los virus polimórficos son quizás los más difíciles de detectar y en consecuencia de eliminar. Sus valores en la programación van cambiando en forma secuencial cada vez que se auto encriptan, de tal forma que sus cadenas

no son las mismas. El virus polimórfico produce varias, pero diferentes copias de sí mismo, manteniendo operativo su micro código viral.

Negación de servicio (DoS). La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o lugar en una red para los usuarios. Un ataque distribuido de negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque.

Objetivos de ataque:

Otras veces, infecta únicamente a los archivos de menor extensión y al usar esta técnica de programación bajo esta tecnología, al infectar archivos o sistemas en forma ocasional, se minimiza la posibilidad de descubrir fácilmente a las especies virales.

Página web. Archivo, generalmente en formato HTML, disponible para su visualización mediante un navegador en la Web. Las páginas web pueden incluir textos, imágenes y recursos multimedia. Generalmente incluyen hipervínculos a otros archivos o páginas web, y algunas pueden incluir formularios para enviar información a la página host.

Parse. Esta técnica consiste en instruir al virus bajo ciertos parámetros definidos, secuenciales o periódicos, como por ejemplo, que infecte cada 10 veces que se ejecute un programa.

- Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
- Permitir a un atacante hacerse pasar por otra entidad
- Permitir a un atacante realizar una negación de servicio
- Permitir que un atacante ejecute comandos como otro usuario

Pharming. Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System), o en el de los equipos de los propios usuarios, que permite a un atacante redireccionar un nombre de dominio (domain name) a otro equipo distinto. De esta forma un usuario que introduzca un determinado nombre de dominio, que haya sido redireccionado, en su explorador

de Internet, accederá a la página Web que el atacante haya especificado para ese nombre de dominio.

Phishing. Conducta fraudulenta que mediante la utilización de páginas de dominio falsas se apodera de los datos de los usuarios que accedan a ellas. En ocasiones se puede fraguar el engaño con una combinación de PHISIHING y de SPAM.

Por defecto, el subdirectorio donde se descargan los archivos es el mismo donde esta instalado el programa, esto causa que el "script.ini" original se sobrescriba con el "script.ini" maligno. Los autores de ese script acceden de ese modo a información privada de la PC, como el archivo de claves, y pueden remotamente desconectar al usuario del canal IRC.

Punto de acceso Wi-Fi. Área física donde se puede usar un dispositivo con Wi-Fi para conectarse a Internet mediante una red inalámbrica pública. Si bien algunos puntos de acceso no poseen medidas de seguridad instaladas, otros usan WEP o WPA para proteger las transmisiones.

Redes punto a punto (P2P). Red virtual distribuida de participantes que hacen que una parte de sus recursos informáticos estén a disposición de otros participantes de la red, todo sin necesidad de servidores centralizados. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware.

Retro Virus. Un retro virus intenta como método de defensa atacar directamente al programa antivirus incluido en la computadora. Con un poco de tiempo pueden descubrir cuáles son los puntos débiles del programa y buscar una buena forma de aprovecharse de ello.

Rootkits. Un rootkit es una herramienta, o un grupo de ellas usadas para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos. Hay rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows. Componente de malware que utiliza la clandestinidad para mantener una presencia persistente

e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final.

Router. Dispositivo de hardware que conecta dos redes y dirige el tráfico de una red al destino adecuado en la otra. Algunos routers, que a menudo se utilizan para conectar una red a Internet, tienen firewalls en red y otras funciones incorporadas.

Sexting. Consiste en la difusión o publicación de contenidos (principalmente fotografías o vídeos) de tipo sexual, producidos por el propio remitente, utilizando para ello el teléfono móvil (SEXTING) u otro dispositivo tecnológico (WEBCAM-SEX-CASTING), a través de e-mail, redes sociales o cualquier otro canal que permitan las nuevas tecnologías.[152]

Software de seguridad fraudulento (rogue). Un programa de software de seguridad rogue es un tipo de aplicación engañosa que finge ser software de seguridad legítimo, como un limpiador de registros o detector antivirus, aunque realmente proporciona al usuario poca o ninguna protección y, en algunos casos, puede de hecho facilitar la instalación de códigos maliciosos contra los que busca protegerse.

Spam. También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing

Spyware. Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial

[152] IX ENCUENTRO AMPAS, Dirección General de la Policía y de la Guardia civil, Gobierno de España, Miajadas 09 -10 de Abril de 2011.

incluye datos que la mayoría de personas no estaría dispuesta a compartir con nadie e incluye datos bancarios, números de cuentas de tarjeta de crédito y contraseñas. Los receptores de esta información pueden ser sistemas o partes remotas con acceso local.

Spyware. Programas, scripts, applets de Java, etc., que se instalan en una computadora y que registran las actividades de los usuarios y la envían a sus creadores. Colectan información de: tráfico, claves, cuentas, tarjetas de crédito. Algunos tienen módulos de keylogger que almacenan las teclas que son utilizadas por el usuario y la envían a Internet.

Stealth. Un virus stealth es aquel que cuando está activado esconde las modificaciones hechas a los archivos o al sector de arranque que están infectados. Esta técnica hace uso de todos los medios posibles para que la presencia del virus pase totalmente desapercibida, anulan efectos tales como el tamaño de los archivos, los cambios de la fecha, hora o atributo, hasta el decremento de la memoria RAM.

Técnicas de Ocultación de Códigos Maliciosos. Consiste en el empleo de técnicas y sofisticadas estrategias de ocultación, con el objeto de lograr especies más dañinas y menos detectables de códigos maliciosos y por consiguiente de difícil detección por parte de los distintos programas antivirus.

Toolkit. Paquete de software diseñado para ayudar a los hackers a crear y propagar códigos maliciosos. Los toolkits frecuentemente automatizan la creación y propagación de malware al punto que, incluso los principiante delincuentes cibernéticos son capaces de utilizar amenazas complejas. También pueden utilizarse toolkits para lanzar ataques web, enviar spam y crear sitios de phishing y mensajes de correo electrónico.

Troyano.

Un virus se valdrá de cualquier técnica conocida o poco conocida, para lograr su cometido. Así, encontraremos virus muy simples que sólo se dedican a presentar mensajes en pantalla y otros mucho más complejos que intentan ocultar su presencia y atacar en el momento justo.

Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema, incluyendo acceso remoto, intercepción de comunicaciones, así como procesos de ocultamiento, archivos, claves de registro y canales de comunicación.

Variantes. Las variantes son nuevas cepas de malware que piden prestado códigos, en diversos grados, directamente a otros virus conocidos. Normalmente se identifican con una letra o letras, seguido del apellido del malware; por ejemplo, W32.Downadup.A, W32.Downadup.B y así sucesivamente.

Virus. Los virus informáticos son uno de los principales riesgos de seguridad para los sistemas computacionales, ya sea se haga referencia a un usuario casero que utiliza su equipo para trabajar y conectarse a Internet o una empresa con un sistema informático importante que debe mantener bajo constante vigilancia para evitar pérdidas causadas por los virus.

Virus. Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

Vulnerabilidad. Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:br />

WEP. Privacidad equivalente alámbrica (Voice over Internet Protocol) WEP, que pertenece a la norma IEEE 802.11, es un protocolo de seguridad para el cifrado de información y la prevención del acceso no autorizado a las redes inalámbricas. La WEP fue diseñada para ofrecer seguridad similar a la de las redes conectadas por cables, pero presenta graves fallos, por lo que fue reemplazado por WPA y WPA2 como protocolos preferentes de seguridad inalámbrica.

Wi-Fi. Wireless Fidelity (fidelidad inalámbrica). Juego de palabras proveniente del inglés "hi-fidelity" que significa "alta fidelidad". Término descriptivo usado para hacer referencia a las redes inalámbricas 802.11, dispositivos o cualquier

dispositivo relacionado con la tecnología inalámbrica 802.11 (por ejemplo, punto de acceso Wi-Fi).

WPA. Acceso Wi-Fi protegido. WPA, que pertenece al estándar inalámbrico 802.11, es una extensión y una mejora del protocolo de seguridad WEP y ofrece mejores medidas de cifrado y autenticación de usuarios.

XML. Lenguaje de marcado extensible (Extensible Markup Language) De manera similar a HTML, XML es un lenguaje que usan los programadores web para dar formato y presentar información en la Web. A diferencia de HTML, XML no cuenta con un conjunto definido de marcas de formato. En cambio, es un meta-lenguaje que ofrece a los programadores flexibilidad para desarrollar sus propias marcas y, de esa manera, organizar y presentar información de formas innovadoras.

FUENTES DE INVESTIGACIÓN

DOCTRINA

AMUCHATEGUI REQUENA, Griselda, *Derecho Penal*, 3ª Edición, México, Oxford University Press, 2010.

ANDRÉS CÁMPOLI, Gabriel, *Derecho penal informático en México*, México, INACIPE, 2004.

CARRARA, Francisco, *Programa de Derecho Criminal, Parte General*, Colombia Bogotá, Editorial Temis, 2004, Volumen I.

CASTELLANOS Tena, Fernando, *Lineamientos Elementales de Derecho Penal*, Cuadragésima edición, México, Editorial Porrúa, 2003.

DÍAZ-ARANDA, Enrique, *Teoría del Delito*, Straf, México 2006.

DÍAZ-ARANDA, Enrique, *Derecho Penal Parte General*, 2ª Edición, México, Editorial Porrúa, 2004.

EBERT Udo, *Derecho Penal Parte General*, Traducción Escudero Said, México, Talleres Gráficos de la UAEH, 2005.

FIX FIERRO, Héctor, *Informática y Documentación Jurídica*, México, UNAM, 1990.

GOODMAN, Marc, *Cibercriminalidad,* México, INACIPE , 2003.

HUERTA MIRANDA, Marcelo y Líbano Manzur, Claudio, *Los Delitos Informáticos*, Santiago de Chile, Editorial Jurídica Cono Sur, 1998.

ISLAS DE GONZÁLEZ MARISCAL, Olga*, Análisis Lógico de los Delitos Contra la Vida*, 4ª Edición, México, Trillas, 2004.

JESCHECK HANS, Heinrich, Tratado de Derecho Penal Parte General, Barcelona, España. Bosch Casa Editorial, 1981.

LIRA ARTEAGA, José Manuel, *Cibercriminalidad Fundamentos de Investigación en México*, México. Editorial INACIPE, 2010.

MEZGER, Edmund, *Derecho Penal Parte General Libro de Estudio*, Argentina, Editorial Bibliográfica Argentina, 1958.

MURILLO DE LA CUEVA, Pablo Lucas y Piñar Mañas, José Luis, *El derecho a la autodeterminación informativa*. Madrid, Fundación Coloquio Jurídico Europeo, 2009.

MORENO HERNÁNDEZ, Moisés, *Modernas tendencias en la ciencia del derecho penal y la criminología*, Madrid, Universidad Nacional de Educación a Distancia, 2001.

MUÑOZ CONDE, Francisco, García Aran, Mercedes, *Derecho Penal Parte General*, 8ª. Edición, España, Editorial Tirant lo Blanch , 2010.

NILSSON en Sieber, Mocana, *Encuesta 2010 sobre Seguridad de Dispositivos,* "Crimen Tecnologías de La Información".

PALAZZI PABLO, Andrés, *Delito Informático*, Buenos Aires Argentina, Editorial Ad Hoc S.R.L. 2000.

PINA VARA, Rafael, *Diccionario de Derecho*, México, Editorial Porrúa, 2004.

PLASCENCIA VILLANUEVA, Raúl, *Teoría del Delito*, México, Instituto de Investigaciones Jurídicas UNAM, 2004.

REYES ECHANDÍA, Alfonso, *Derecho penal*, Bogotá, Editorial Temis, 2002

RODRÍGUEZ MOURULLO, Gonzalo, *Derecho Penal Parte General*, España, Editorial Civitas S.A., 1978.

SCHMELKES, Carolina, *Manual para la Presentación de Anteproyectos e Informes de Investigación*, México, Editorial Harla, 1998.

TÉLLEZ VALDÉS, Julio, *Derecho Informático*, 3ª. Edición, México, McGraw-Hill, 2004.

TANENBAUM A. S*. Redes de computadoras*, México, Pearson, 2003.

WELZEL, Hans, *El Nuevo Sistema del Derecho Penal (una introducción a la doctrina de la acción finalista)*, Trad. José Cerezo Mir, Barcelona, Ariel, 1961.

HEMEROGRAFÍA

Revista del Instituto de la Judicatura Federal, Poder judicial de la federación. México, 2009.

Centro de Estudios Constitucionales, *Protección de los datos personales automatizados*, Revista de Estudios Políticos (Nueva Época), Madrid, núm. 84, abril-junio de 1994.

LEGISLACIÓN

Acta Federal de Abuso Computacional de Estados Unidos de 1994.

Agenda Penal Federal 2012, México, Ediciones Fiscales ISEF, 2012.

Ley de reforma del Código Penal de 1987 en Austria.

Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y El Comité de las Regiones - Creación de una Sociedad de la Información más segura mediante la mejora de la seguridad de las infraestructuras de información 26.1.2001, COM (2000) 890.

Comunicado de la Conferencia Ministerial de los países del G-8 sobre la lucha contra la delincuencia organizada transnacional", Moscú, 19 a 20 octubre de 1999.

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, Informe sobre la Economía de 2005, UNCTAD/SDTE/ECB/2005/1

Decisión de 24 de febrero de 2005 sobre los ataques contra los sistemas de información. Marco del Consejo 2005/222/JAI

Delitos informáticos Legislación y capacidad de ejecución de proyectos de construcción 3 ª Conferencia de Expertos y el Seminario de Capacitación, APEC de Telecomunicaciones y el Grupo de Trabajo de Información, 32 ª reunión, 5-9 de septiembre de 2005, Seúl, Corea.

Descubrimiento de la fábrica de procesamiento de datos de virus en Italia," AFP Sciences, 2/17/94

G8 Gobierno-Industria Taller sobre Seguridad y seguridad en el ciberespacio, Tokio, mayo de 2001.

IX ENCUENTRO AMPAS, Dirección General de la Policía y de la Guardia civil, Gobierno de España, Miajadas 09 -10 de Abril de 2011.

Ley de los Delitos Informáticos de 1993 en Holanda.

Ley de reforma del Código Penal de 1987 en Austria.

Ley Especial sobre los Delitos Informáticos de Venezuela de 2001.

Ley número 88-19 de 1988 sobre el fraude informático en Francia.

Segunda Ley contra la Criminalidad Económica de 1986 en Alemania.

PÁGINAS ELECTRÓNICAS

Agenda Ciberseguridad Global / Grupo de Alto Nivel de Expertos, Informe Global Estratégico de 2008, página 17. *http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.*

Agenda de Túnez para la Sociedad de la Información, 2005, *http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0*

Asociación Mexicana de Internet, Las Redes sociales en México y Latinoamérica 2001, elaborado por VP Investigación de Mercados, Renato Juárez Research Director Elogia e Ivan Marchant Country Manager Comscore. Disponible en: *http://www.amipci.org.mx/*

Cámara de diputados h. Congreso de la Unión, Leyes Federales.
http://www.diputados.gob.mx/LeyesBiblio

Cámara de diputados h. Congreso de la Unión, Leyes Estatales.
http://www.diputados.gob.mx/LeyesBiblio/gobiernos.htm

China Fundación del campo de la frontera electrónica http://www.eff.org/pub/Global/China/

Código Penal de Canadá
http://insight.mcmaster.ca/org/efc/pages/law/cc/cc.html

CONACYT
DNS, El Servicio tras los nombres en Internet
http://www.conacyt.gob.mx/comunicacion/revista/193/Articulos/DNS/Ligas/Enlosorigenes01.html

Cooperación internacional en la prevención, investigación, enjuiciamiento y castigo del fraude, el uso indebido e ilícito y falsificación de identidad y otros delitos relacionados, Resolución del ECOSOC 2004/26 , *http://www.un.org/ecosoc/docs/2004/Resolution% 202004-26.pdf.*

Declaración de BangkokLas sinergias Declaración y respuestas: alianzas estratégicas en materia de Prevención del Delito y Justicia Penal", *http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.*

El Universal, viernes 17 de junio de 2011.
http://www.eluniversal.com/2011/06/17/japon-aprueba-ley-que-criminaliza-creacion-de-virus-informaticos.shtml

El Universal, Jueves 12 de Junio de 2003, *http://www2.eluniversal.com.mx/pls/impreso/noticia.html?id_nota=97982&tabla=nacion*

Fundación Manuel Buen Día, Apuntes académicos para una historia de internet en México.
http://www.mexicanadecomunicacion.com.mx/fmb/foromex/apuntes.htm

Gaceta Parlamentaria del Senado de la República
http://www.senado.gob.mx

Golg Steve, Hackers Take Scotland Yard's PABX For A Cool Million, 8/5/96, *www.apple.com.au/documents/newsbytes/1996/aug96/960807/2.html*

The Web Police
http://www.web-police.org

J. Katz PhD David L. Carter PhD and Adra, "Computer Crime : An Emerging Challenge for Law Enforcement," 12/96

http://www.fbi.gov/leb/dec961.txt

La Crónica de Hoy, Viernes 06 de Enero de 2012, disponible en: *http://www.cronica.com.mx/nota.php?id_nota=626209*

La venta por Internet de drogas lícitas a las personas a través de Internet, Resolución del ECOSOC 2004/42 disponible en: *http://www.un.org/ecosoc/docs/2004/Resolution% 202004-42.pdf*

Ley Especial sobre los Delitos Informáticos de Venezuela de 2001, texto *completo disponible en: http://www.tsj.gov.ve/legislacion/ledi.htm*

Ley Italiana del Crimen por Computadoras, *http://www.clarence.com/home/diritto/Comment2.htm*

Ley Modelo sobre la informática y los delitos informáticos the commonwealth, *http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/ 7BDA109CD2-5204-AA77-4FAB-86970A639B05 7D_Computer%% 20Crime.pdf.*

Manual de las Naciones Unidas para la Prevención y el Control de los delitos informáticos (publicación de las Naciones Unidas, N E.94.IV.5), disponible en *http://www.uncjin.org/Documents/EighthCongress.html.*

Linkses, La Historia de Internet, disponible en *www.mundosciberneticos.com*

Revista de Derecho Informático núm. 048, Campoli, Gabriel Andrés, Hacia una correcta hermenéutica penal delitos informáticos vs. delitos electrónicos AR:, *http://www.alfa-redi.org/rdi-artículo.shtml?x=1480*

Schjolberg / Hubbard, armonización de los enfoques Jurídico Nacional sobre el Delito cibernético, 2005, página 8, en: *http://www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf*

Suelete Dreyfus "Underground,", 1997, *http://www.underground-book.com/about.htm*

Tercer Informe de la Secretaría de Seguridad Pública, Prevención contra el delito cibernético, 31 de Agosto de 2009, pág. 61. Disponible en: *http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/550126//archivo*

http://www.cudi.mx

http://www.facebook.com

http://www.plus.google.com

http://www.twitter.com