UNIVERSIDAD VILLA RICA

ESTUDIOS INCORPORADOS A LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

"LAS CONDUCTAS DE RELEVANCIA PARA EL DERECHO PENAL EN MATERIA DE INTERNET"

TESIS

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

PRESENTA:

LEO MISAEL JÁCOME GAMBOA

Directora de Tesis:	**Revisor de Tesis**
LIC. ADELA REBOLLEDO LIBREROS	MTRO. MIGUEL ÁNGEL RODRÍGUEZ GONZÁLEZ

BOCA DEL RÍO, VER. **2012**

A Dios,
por haberme dado a mi familia y por haber puesto en mi camino a todos los seres que amo.

A mis Padres Joaquín y Ofelia,
quienes me apoyaron incondicionalmente no solo económicamente, sino además moralmente.

A mis abues Paz, América y Leocadio,
quienes decidieron creer en mí cuando ni yo mismo lo hacía.

A mi hermano Luis,
por todo ese apoyo incondicional que solo él sabe dar.

A Teresa,
quien me ha apoyado y confiado en mí en cada decisión que he tomado.

A mis amigos Camely, Eduardo, Elisa, Maricarmen y Orlando,
quienes ocuparán por siempre un lugar en mi corazón y que me demostraron que la amistad es un verdadero valor humano.

A mis grandes maestros especialmente a los licenciados, Adela Rebolledo, Adriana Rodríguez, Miguel Ángel Rodríguez, Teresa Muñoz y Rodolfo García,
quienes mas que catedráticos fueron excelentes amigos.

Por el sueño de alguien más que decidí hacer mío…
Sueño que decidí defender como si siempre lo hubiese sido.

ÍNDICE

CAPÍTULO II
EVOLUCIÓN HISTÓRICA DEL INTERNET.

CAPÍTULO III
LEGISLACIÓN MEXICANA E INTERNACIONAL EN MATERIA DE INTERNET.

CAPÍTULO IV
CONDUCTAS DE RELEVANCIA PARA EL DERECHO PENAL EN MATERIA DE INTERNET.

INTRODUCCIÓN

A lo largo de la historia el ser humano ha necesitado transmitir y tratar la información de una forma continua. Desde que el hombre descubre el lenguaje comenzando por medio de señas y sonidos, las señales de humo, la escritura hasta medios tan complejos como los códigos, como el caso del famoso código Morse, la humanidad no se ha detenido en la creación de métodos para procesar información.

Hoy en día es indiscutible que la computadora más que ser un lujo, se ha convertido en una verdadera herramienta indispensable para el desarrollo humano y más sorprendente aún el hecho de que Internet, haya logrado cautivar a millones de personas con los múltiples servicios que ofrece al público en general, servicios que van desde el e-mail hasta las compras por medio de la *Web* que por medio de portales que sirven de catálogo de productos ofrecidos por empresas o usuarios particulares mismos que se encuentran previamente registrados en dichos portales, citando como ejemplos Mercado libre y EBay que son conocidos por ofrecer este tipo de servicios entre usuarios de todo el mundo.

Gracias a toda esta tecnología informática, hoy en día podemos hacer uso de muchos de esos servicios desde la comodidad de nuestro hogar con solo conectarnos a la red, por medio del servicio proporcionado por alguna compañía telefónica, de una compañía de televisión que además proporciona internet o de

compañías especializadas en brindar servicios de Internet. Lamentablemente, la tecnología no se ha empleado solo para el beneficio del hombre, sino que algunas personas sin escrúpulos, han traspasado, los límites de la seguridad y han realizado actos ilícitos, lo que ha generado una gran preocupación evidentemente fundada por parte de las personas que utilizan la red, dedicándose muchos a la tarea de buscar una forma de solucionar este problema que personas como Julio Téllez llaman *Delincuencia Informática* o *Delitos Cibernéticos*.

En esta investigación se podrá apreciar la evolución de internet desde sus precedentes hasta la actualidad, obtener información de los diferentes conceptos que se han dado por algunos expertos en la materia de los Delitos Cibernéticos y el Derecho Informático, la clasificación que les han dado a dichos delitos, así como la visión general que se le ha dado a esta problemática en nuestro país y una breve reseña de las medidas que han optado los demás países frente a este problema y sobre todo valorar las condiciones jurídicas referentes a esta materia, en las que vivimos actualmente.

Los sistemas informáticos ofrecen nuevas oportunidades para infringir la ley, esto porque los cibernautas han creado la posibilidad de encuadrar en los tipos penales tradicionales en formas no tradicionales.

Una de las metas que tiene este trabajo es analizar las conductas ilícitas que pueden aparecer debido al gran avance tecnológico, sobre todo en el mundo de la informática.

En la actualidad la gran mayoría de la población que posee una computadora personal y tiene conexión a Internet, corre el gran riesgo de ser atacado por alguno de los grandes problemas informáticos entre los que encontramos a los famosos virus.

Si analizamos las legislaciones que se han promulgado en diversos países veremos que esa información arroja que las normas jurídicas que están en vigor van dirigidas a proteger y resguardar la utilización abusiva de la información en las computadoras, y que inclusive en algunas de ellas han creado órganos especializados para proteger a las personas amenazadas por los múltiples problemas existentes.

Casi todos los países europeos han hecho todo lo posible para que sus leyes contemplen las conductas punibles penalmente, como son el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

De igual forma en los países occidentales hay ordenamientos legales que se asemejan a los de los países de Europa. Todos enfocados e inspirados en conseguir la mayor confiabilidad y seguridad en los medios de comunicación electrónicos, las transacciones bancarias, los intercambios y compras entre muchas cosas más realizadas en Internet.

En el primer capítulo hablaremos acerca de la metodología que tiene esta tesis abarcando el planteamiento, la justificación, los objetivos que se plantean, hipótesis, el tipo de estudio, diseño y entre otras cosas las variables y su definición.

En el segundo capítulo abarcaremos lo que es Internet, como surge, porque, como funciona, como está organizada, las medidas de seguridad y los riesgos en Internet entre los que destacan los virus informáticos y además resaltamos cuales son los beneficios que ofrece Internet.

En el tercer capítulo observamos el plano legal a nivel nacional e internacional en regulación a Internet en el que mencionaremos que es la

Informática Jurídica y El Derecho Informático, y sobre todo el análisis exhaustivo en que son los delitos cibernéticos y su regulación en los distintos países del mundo en el que señalamos las diferentes formas en que las naciones han optado para regular ya sea desde sus constituciones hasta en una ley específica de la materia, a su vez señalaremos lo poco que tenemos en el país en los distintos códigos penales de las entidades federativas y en el código penal federal.

En el capítulo cuatro se señalaran que delitos informáticos son los existentes, las distintas clasificaciones aportadas por los juristas maestros en la materia y por los órganos reguladores y los que deben tipificarse al considerarlos como conductas más que contrarias a la buena convivencia, al sano uso, privacidad, libertad y demás bienes jurídicos de las personas en Internet.

Por último se agregan las conclusiones en las que se hace un breve recuento de lo más relevante expuesto a lo largo de todo el trabajo de investigación y en el apartado de las recomendaciones y sugerencias presentamos las medidas que se deben de tomar al respecto para poder solucionar el problema de las conductas que se cometen en Internet que quedan impunes.

CAPÍTULO I
METODOLOGÍA DE LA INVESTIGACIÓN.

1.1. PLANTEAMIENTO DEL PROBLEMA.

¿Deben de crearse tipos penales cibernéticos cuya conducta lesione bienes jurídicos fundamentales en la vida en sociedad?

1.2. JUSTIFICACIÓN DEL PROBLEMA.

Esta investigación se fundamenta en que desde el surgimiento de las computadoras, seguido por Internet y los celulares, ha ocurrido un gran avance tecnológico, uno que hace posible distinguir fácilmente el siglo pasado del presente, al que algunos autores incluso han llamado de la revolución digital la cual es según De Sola Quintero “caracterizada por el desarrollo de tecnología en todas sus formas y, por ello nos encontramos ante un complejo y laberíntico entramado de cables, satélites, redes, computadoras, fibra óptica, televisores e

impulsos eléctricos que constituyen la infraestructura del ciberespacio"[1], así pues ha traído esto consigo un sinnúmero de ventajas como hacer más sencilla la comunicación entre las personas, ya que sobre todo cuando se trataba de poder comunicar a personas que se encontraban a grandes distancias era muy costoso y tardado además de que podía incluso llegar a perderse el mensaje, dichos avances tecnológicos propician la compraventa entre las personas de distintos países y hasta continentes cuando en la mayoría de los casos ni se ven físicamente nunca, algo que prácticamente era imposible antes.

El acceso a la información más sencilla, sin tener que ir forzadamente a las bibliotecas tradicionales, facilita conocer los grandes avances en la medicina, biología, física y todas las demás ciencias existentes así como noticias internacionales y de otras comunidades del mundo, la economía en gastos de comunicación y mucho más.

Pero el problema surge cuando las personas usan estos medios y facilidades como una forma de causar perjuicios y daños a las demás personas; así, desde el punto de vista de las grandes desventajas que ha traído, encontramos que con la misma facilidad que se encuentra información útil, también hay información nociva como lo es la pornografía, la violencia explícita, el terrorismo, etcétera, que en muchos de los casos van encaminadas hacia los más vulnerables que son los menores; también la Internet genera una gran dependencia o vicio sobre todo a las redes sociales, así también ha facilitado la expansión de la piratería y la aparición del spam, malware, la proliferación de los virus y el phising solo por mencionar algunos.

Así, hoy en día han aparecido conductas que para mala suerte de la sociedad, no se han podido regular en el Derecho Penal, y en consecuencia dichos comportamientos no pueden ser sancionados dentro del campo del derecho penal,

[1] www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf

mismo que ha dejado en un estado de indefensión a todas las personas que sean víctimas de los autores de esas conductas y es que hasta que no haya algo en qué sustentarse legalmente, estos quedarán impunes, pues de no hacer algo al respecto se estarían violando sus garantías, mismas que enuncia nuestra Constitución. Es ahí cuando nos damos cuenta de que para evitar esto, hace falta darle un sentido, buscar soluciones al problema y prever otras situaciones que puedan aparecer y evitar que queden sin el castigo de la justicia.

Sin embargo, este problema se ha propiciado y descontrolado por muchos factores como la falta de educación respecto al tema, la facilidad del acceso a estos medios electrónicos, etcétera, aunque quizás de todos ellos el más relevante haya sido la omisión de nuestros legisladores respecto de crear un código o por lo menos incluir un capítulo en el existente, que realmente regule las conductas lascivas de esta índole que es el Derecho Informático.

Con esta investigación se busca beneficiar al Estado en cuanto a poder controlar la situación consistente en los conflictos presentados en la red, como la usurpación de identidades, el robo de información privada, las amenazas por medio de la Internet, los fotomontajes, el acoso por medio de las redes sociales, etcétera, que sufre la población y poder castigar a las personas que atenten contra la integridad y la seguridad de los datos de estas, así como la identidad de estos o su patrimonio o recursos en cuentas bancarias dependiendo del objetivo de la conducta realizada; y también se busca apoyar a los ciudadanos, en cuanto a protegerlos ante estas agresiones en su contra y que se castigue al que viole sus derechos en el uso de la red con el pleno uso de las normas, cumpliendo con el requisito de legalidad en la actuación de las autoridades, porque de no crear los tipos penales necesarios y al no existir esa regulación, se estaría facilitando la evasión de responsabilidad y quedando sin justo castigo todas aquellas personas que actúan con plena intención de causar algún perjuicio.

1.3. OBJETIVOS.

1.3.1. Objetivo general.

Explicar la necesidad de tipificar las conductas que lesionen los bienes jurídicos fundamentales mediante el uso de Internet y sus redes sociales.

1.3.2. Objetivos específicos.

Destacar la evolución histórica de la Internet.

Investigar la regulación jurídica existente en los diversos ordenamientos nacionales e internacionales acerca de la Internet y su empleo negativo.

Explicar en qué consisten los tipos penales que se planteen en relación a los ilícitos en materia de Internet.

Fomentar la tipificación de las conductas de relevancia para el Derecho Penal en materia de la Internet.

1.4. HIPÓTESIS.

Porque la falta de regulación en el código penal motiva la proliferación de dichas conductas lesivas a los bienes jurídicos fundamentales.

.

1.5. VARIABLES.

1.5.1. Variable independiente.

La ausencia de la responsabilidad penal por conductas desplegadas a través de la Internet.

1.5.2. Variable dependiente.

Apoyar la tipificación de los delitos cibernéticos en el código penal.

1.6. DEFINICIÓN DE VARIABLES.

Ausencia de responsabilidad penal.- es cuando existe una de las "circunstancias que excluyen la responsabilidad penal por la realización de la conducta punible."[2]

Delitos cibernéticos.- "Los Delitos Informáticos son todos los actos que permiten la comisión de agravios, daños o perjuicios en contra de las personas, grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio del uso de computadoras y a través del mundo virtual de Internet."[3]

1.7. TIPO DE ESTUDIO.

El presente escrito se ubica dentro del esquema de los estudios analítico-propositivos, pues consiste en buscar explicar a un fenómeno desde sus

[2] html.rincondelvago.com/derecho-penal-en-colombia.html Página consultada el veinticinco de febrero del 2012

[3] www.buenastareas.com/ensayos/Delitos-Ciberneticos/113654.html Página consultada el veinticinco de febrero del 2012

diferentes elementos, para comprenderlo como un todo y a su vez busca proponer posibles soluciones al problema planteado.

1.8. DISEÑO.

1.8.1. Investigación Documental.

Debido a la naturaleza critico-propositiva del presente trabajo de investigación, se acudió a diferentes centros de acopio de información para recopilar los datos en los que soportamos esta investigación, así como también el estudio de las diferentes legislaciones relacionadas con el tema, así como consultas hechas en Internet.

1.8.1.1. Centros de Acopio de Información.

1.8.1.1.1. Bibliotecas Públicas.

Biblioteca Pública Unidad de Servicios Bibliotecarios y de Información de la Universidad Veracruzana, en sus campus:

Veracruz Juan Pablo II esquina Ruiz Cortines, Fraccionamiento Costa Verde, Boca del Río, Veracruz.

Xalapa Avenida de las Culturas Veracruzanas No. 1. Zona Universitaria Col. Zapata 91040 Xalapa, Veracruz.

Biblioteca Pública Coronel Manuel Gutiérrez Zamora, Zaragoza 397 esquina Esteban Morales, C.P. 91900, Colonia Centro, Veracruz, Veracruz.

1.8.1.1.2. Biblioteca Privada.

De la Universidad Autónoma Villa Rica, Progreso esquina Urano, Fraccionamiento Jardines de Mocambo, Boca del Río, Veracruz.

1.8.1.1.3. Biblioteca Particular.

Libros particulares del sustentante ubicados en Guadalupe Victoria esquina callejón Fortín número 210 Colonia El Fuerte, Soledad de Doblado, Ver.

1.8.1.2. Técnicas empleadas para la recopilación de información.

Para la realización de la presente investigación se utilizaron principalmente fichas bibliográficas y de trabajo como a continuación se describe.

1.8.1.2.1. Fichas bibliográficas.

En ellas se anotan los datos específicos de determinado libro o artículo de ley, se registran las fuentes de información de trabajo.

Las fichas bibliográficas son aquellas que contienen nombre del autor, título de la obra, número de edición, editorial, lugar, año y total de páginas.

1.8.1.2.2 Fichas de trabajo.

Se realizaron para el presente estudio las fichas de trabajo en modalidad de transcripción en la que se realiza la transcripción del párrafo que contenga una idea importante para el trabajo de investigación que se está realizando.

Estas fichas contienen nombre del autor, título de la obra, número de edición, editorial, lugar, año, páginas consultadas y transcripción del material de interés.

CAPÍTULO II
EVOLUCIÓN HISTÓRICA DEL INTERNET.

2.1. ¿QUÉ ES INTERNET?

La internet podría definirse como el conjunto de redes de cómputo interconectadas entre sí que permiten el tráfico de todo tipo de archivos en todo el mundo, para Víctor Manuel Rojas internet es el "…conjunto de servidores de archivos distribuidos en todo el mundo e interconectados mediante un sistema maestro de redes de computo"[4], así entonces queda claro que internet no es más que un medio de comunicación y transporte de todo tipo de archivos por medio del uso de computadoras; además hoy en día también no solo por el uso de computadoras sino de un sinfín de diversos aparatos portátiles de comunicación como lo son los iPod, las Palms, las laptops o computadoras portátiles y los teléfonos celulares.

[4] ROJAS AMANDI, Víctor Manuel. *El uso de internet en el derecho.* Segunda edición, México, Distrito Federal, Porrúa, 2001, p.1.

Cabe mencionar que cualquier persona puede ingresar fácilmente a esta e ingresar de cierta forma todo tipo de información desde un programa de cómputo y documentos de texto hasta imágenes y videos, y de igual forma que una persona ingresa información a esta, cualquier otra puede tener el acceso a esa información debido a su característica de que la información que entra a esta se vuelve de cierta forma pública.

Así a Internet se le puede considerar como un enorme portal que permite el tráfico de información, esto creando una enorme biblioteca en la que existe todo tipo de información, infinidad de archivos digitales, videos, imágenes, música videos, libros electrónicos, etcétera al acceso del público en general; "Sin embargo, en una biblioteca real solo las autoridades tienen la facultad de introducir nuevos libros o documentos; en cambio, internet permite que los usuarios introduzcan libremente información, lo que propicia un crecimiento enorme e ininterrumpido del acervo disponible."[5]

Básicamente "Internet surgió de un proyecto desarrollado en Estados Unidos para apoyar a sus fuerzas militares. Luego de su creación fue utilizado por el gobierno, universidades y otros centros académicos."[6]

Así desde su nacimiento "Internet ha supuesto una revolución sin precedentes en el mundo de la informática y de las comunicaciones. Los inventos del telégrafo, teléfono, radio y ordenador sentaron las bases para esta integración de capacidades nunca antes vivida. Internet es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores independientemente de su localización geográfica."[7]

---

[5] ROJAS AMANDI, Víctor Manuel. Op. Cit.
[6] www.maestrosdelweb.com/editorial/internethis Página de Internet consultada el diez de marzo del 2012
[7] Op. Cit.

2.1.2. La historia de Internet.

“Internet no se concibió como una red de sistemas de cómputo; más bien, debía satisfacer ciertas necesidades del Ministerio de Defensa de Estados Unidos de América. Para lograrlo, se necesitaba una red que no fuera dependiente de una sola computadora central. Esto es importante, pues el concepto original de red de computadoras exige una computadora central (servidor) que administre la información y esté al servicio de los usuarios enlazados con la red. Este es el sistema de red de computadoras que los juristas veían habitualmente en los centros de trabajo antes de la aparición de Internet.

Un sistema tradicional de red con una computadora central les pareció muy vulnerable a los expertos del Ministerio Público de Defensa de Estados Unidos de América. Un ataque a la computadora central hubiese significado la caída de toda la red. Por eso, a partir de la década de 1960 empezó a desarrollarse un sistema de red que no dependiera de un servidor, sino que se organizara de modo que cada computadora funcionara de manera independiente de las otras. Así, debido a que era posible obtener la información en cualquiera de las computadoras enlazadas al sistema, se evitaría el riesgo de que el daño que llegara a sufrir una computadora específica se extendiera a todo el sistema.

Los científicos del Ministerio de Defensa de Estados Unidos de América desarrollaron una red con las características mencionadas, la cual se puso en funcionamiento con el nombre de ARPANET.

Para el funcionamiento del sistema ARPANET fue necesario construir procesadores especiales, a los que se denominó *procesadores de mensaje de interfaz* (IMP, Interface Message Processors), que debían funcionar como nodos en la red. El primer procesador de este tipo fue puesto en funcionamiento el 1 de agosto de 1969 en la Universidad de California en Los Ángeles (UCLA), con una

microcomputadora Honeywell 516 que tenía 12KB de memoria. Pocas semanas después se instalaron IMP en el Stanford Research Institute en Menlo Park, California, en la universidad de California en Santa Bárbara y en la universidad de Utah en Salt Lake City. Cuando estos procesadores comenzaron a intercambiar paquetes de datos a larga distancia, ya había nacido ARPANET. En 1972 se habían instalado 37 IMP. El primero de junio de 1990 se desinstalo ARPANET, lo que pasó inadvertido porque ya había en las grandes ciudades un número suficiente de proveedores de servicios de Internet.

ARPANET funcionó con un programa de computación especial denominado *Network Control Protocol* (NPC), que hizo posible el uso descentralizado de la red. Una gran ventaja que ofreció el NPC fue que trabajaba con diferentes tipos de computadoras y programas, lo que condujo a una expansión considerable de ARPANET. En la década de 1970, esta red creció más allá de sus objetivos originales de sistemas de información del Ministerio de Defensa, debido a que varias redes científicas se enlazaron al sistema. Científicos y profesores de los Estados Unidos de América comenzaron a considerar la posibilidad de transmitir mensajes electrónicos mediante la red para participar en el desarrollo de proyectos científicos.

En la década de 1980 el NPC fue sustituido por un programa nuevo llamado TCP/IP, que funciona de manera más eficaz. El TCP/IP convierte los datos en pequeños paquetes, los envía a su lugar de destino con base en sus direcciones a través de diferentes puntos de enlace de Internet y la computadora de destino los recompone.

A principios de la década de 1980 Internet se separó de ARPANET, de tal forma que se desligo de los objetivos militares y se expandió de una manera más rápida. Esto permitió que instituciones científicas tanto estadounidenses como extranjeras se enlazaran a Internet.

En 1986 se fundó la NSFNET. Financiada por el gobierno federal estadounidense, la NSFNET creo diferentes líneas de enlace para Internet, a las que se denominó *Backbones* (espina dorsal), con las que se facilitaban la transferencia de datos. A partir de entonces, Internet inicio su expansión hacia el exterior de Estados Unidos de América, sobre todo hacia Europa. Hasta 1995, la NSFNET intento imponer una política de uso aceptable (acceptable use policy), con el fin de que Internet se utilizara solo con propósitos científicos, no comerciales. Sin embargo, dicha política fue puesta fuera de vigor a principios de 1995, cuando el gobierno estadounidense decidió privatizar y no otorgar más subsidios a Internet. Desde ese año es posible utilizar este sistema para objetivos de índole muy diversa, incluidos los de carácter comercial.

A menudo se formula la pregunta sobre el financiamiento de Internet: ¿existe una instancia central a la que se encuentre subordinada? La respuesta nos dice que los datos suministrados de Internet se envían de una computadora a otra sin saber desde un principio la ruta que seguirá la información hasta llegar a la computadora final. Debido a ello será imposible imponer una cuota sobre la base de la información consultada, porque el camino que siguen los datos solo se conoce cuando se reciben."[8]

ARPANET fue entonces la primera red que apareció en Estados Unidos con fines militares, siendo después aprovechada en las Universidades Americanas puesto que sirvió para dar paso a lo que hoy conocemos como Internet, con esto apreciamos que la creación de Internet fue con motivación de crear una red de computadoras para comunicarse sin que pudieran ser interceptados por los enemigos.

[8] ROJAS AMANDI, Víctor Manuel, Op. Cit. Nota 4, p. 2

2.2. ORGANIZACIÓN Y FUNCIONAMIENTO DEL SISTEMA INTERNET.

La estructura de Internet se caracteriza por su organización no jerárquica. Esto se debe a que todas las computadoras y los sistemas de redes enlazadas a Internet poseen exactamente la misma capacidad de acceso a la información y demás servicios que se ofrecen. Aunado a lo anterior, y debido a que la información que se introduce en el sistema no se deposita en una computadora o una red determinada, sino que se transmite por una computadora a otra, tampoco es posible es poner al sistema fuera de servicio. En caso de que una parte se caiga siempre resulta imposible obtener la información perdida por otro camino.

Otra característica propia de Internet es el sistema de autorregulación. Internet no cuenta con un órgano de control que regule su funcionamiento. En cambio, el sistema se regula desde el interior, por medio de los protocolos TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet por sus siglas en inglés), con los que trabaja cada computadora enlazada al sistema. Mientras el otro sistema de comunicación, como el teléfono, tiene lugar a una comunicación directa entre quien emite la señal y quien la recibe; en Internet la información emitida se divide en pequeños paquetes, que se envían por diferentes rutas del sistema y al final, en la computadora receptora vuelven a ensamblarse. El emisor de la información cuenta con la necesidad de volver a enviar los paquetes de datos que se reciban o que lleguen dañados a la computadora receptora. Por lo mismo, no existe en Internet, como la comunicación telefónica, una comunicación directa entre el emisor y el receptor de la señal, controlada por una instancia central.

Un aspecto de especial importancia para los juristas en materia de Internet es el sistema de nombres de dominio en la red, este concepto se utiliza en dos sentidos, por una parte, en relación con las direcciones de servicios de

información que pertenecen a Internet; y por la otra se emplea para direcciones de correo electrónico.

Todos y cada uno de los servicios de información a los que es posible acceder mediante Internet tienen su propia dirección, con la que se invoca el servicio de que se trata, a estas secciones especiales que tiene cada dirección se les denomina *dominios*, que sirven para señalar a que empresa u organización de Internet pertenecen.

En la Informática podemos apreciar que la mayor parte de los servicios informativos de interés se encuentran en el servicio de Internet que se ha denominado World Wide Web (WWW). A la dirección de un servicio de Internet se le llama URL siglas que en español significan Localizador Uniforme de Recursos; a la dirección de un servicio de Internet.

Ahora bien, en el uso de Internet en ocasiones vemos al principio de una dirección HTTP, la cual significa Hypertext Transport Protocol o en español Protocolo de Transferencia de Hipertexto, mismo que es un programa que los clientes y servidores utilizan para intercambiar archivos en WWW.

En una URL existen secciones, las cuales son normalmente la www seguida por el nombre de la empresa, compañía o servicio del que se trata y a su vez termina con una referente al dominio. Sin embargo, una dirección de Internet puede tener más secciones de las comunes. Ejemplo: www.nombredelaempresa.dominio.

La sección más importante dentro de una URL es la que hace referencia al dominio, que es la que define el tipo de organización a la que pertenece esta. A continuación las más usuales:

- .com
    - Estas hacen referencia a que se tratan de organizaciones comerciales.

- .edu
    - Relacionadas a universidades, colegios, bibliotecas y otras instituciones de enseñanza.

- .gob o .gov
    - Usadas para señalar que la página de Internet es una dependencia de gobierno o cualquier otra organización estatal.

- .net
    - Son de sistema de la red y sistemas de la administración de Internet.

- .org
    - Esta es para otras organizaciones no incluidas en las anteriores o para algunas que optaron por usar este tipo de dominio.

2.2.1. Códigos por países.

Como Internet surge en los Estados Unidos de América, los demás países para hacer alusión a que las páginas no son estadounidenses decidieron incluir códigos en las URL’s, a continuación se señalan los existentes:

AD Andorra
AE Emiratos Árabes Unidos
AF Afganistán
AG Antigua y Barbuda
AI Anguila (Caribe)
AL Albania
AM Armenia
AN Antillas Holandesas
AO Angola
AQ Antártida
AR Argentina
AS Samoa Americana
AT Austria
AU Australia
AW Aruba
AZ Azerbaijan
BA Bosnia-Herzegovina
BB Barbados
BD Bangladesh
BE Bélgica
BF Burkina Faso
BG Bulgaria
BH Bahrain (Bahréin)
BI Burundi
BJ Benín
BM Bermudas, Islas
BN Brunei Darussalam (Brunei)
BO Bolivia
BR Brasil
BS Bahamas
BT Bután
BV Bouvet, Isla
BW Botswana
BY Bielorrusia
BZ Belice
CA Canadá
CC Cocos, Islas
CF República Centroafricana
CG Congo
CI Costa de Marfil (Côte D'Ivoire)
CK Cook, Islas
CL Chile
CM Camerún
CN China
CO Colombia
CR Costa Rica
CS Antigua Checoslovaquia (Czechoslovakia (former))
CU Cuba
CV Cabo Verde
CX Navidad, Isla (Kiribati)
CY Chipre (Cyprus)
CZ República Checa (Czech Republic)
CH Suiza
DE Alemania
DJ Djibouti
DK Dinamarca (Denmark)
DM Dominica
DO República Dominicana
DZ Argelia
EC Ecuador
EE Estonia
EG Egipto
EH Sahara Occidental
ER Eritrea
ES España
ET Etiopía
FI Finlandia
FJ Fiji
FK Malvinas, Islas
FM Micronesia
FO Feroe, Islas
FR Francia
FX Francia-Área Metropolitana

GA Gabón
GB Gran Bretaña (Reino Unido) (Great Britain) (UK)
GD Granada (Grenada) (Caribe)
GE Georgia (ex-URSS)
GF Guayana Francesa
GH Ghana
GI Gibraltar
GL Groenlandia
GM Gambia
GN Guinea
GP Guadalupe, Isla
GQ Guinea Ecuatorial
GR Grecia
GS Georgias y Sandwich del Sur, Islas
GT Guatemala
GU Guam
GW Guinea-Bissau
GY Guyana
HK Hong Kong
HM Heard y McDonald, Islas de (Antártida)
HN Honduras
HR Croacia (Hrvatska)
HT Haití
HU Hungría
ID Indonesia
IE Irlanda
IL Israel
IN India
IO Territorios Británicos en el Océano Índico
IQ Irak (Iraq)
IR Irán
IS Islandia
IT Italia
JM Jamaica
JO Jordania
JP Japón
KE Kenia
KG Kirguistán
KH Camboya
KI Kiribati
KM Comores, Islas
KN Saint Kitts y Nevis, Islas de (Caribe)
KP Corea del Norte (Korea (North))
KR Corea del Sur (Korea (South))
KW Kuwait
KY Caimán, Islas
KZ Kazajstán
LA Laos
LB Líbano
LC Santa Lucía, Isla de (Caribe)
LI Liechtenstein
LK Sri Lanka (ex Ceylán)
LR Liberia
LS Lesotho
LT Lituania
LU Luxemburgo
LV Latvia
LY Libia
MA Marruecos
MC Mónaco
MD Moldavia
MG Madagascar
MH Marshall, Islas
MK Macedonia
ML Malí
MM Myanmar (ex-Birmania)
MN Mongolia
MO Macao, Isla
MP Mariana del Norte, Islas (Micronesia)
MQ Martinica (Martinique)

MR Mauritania
MS Montserrat
MT Malta
MU Mauricio, Islas
MV Maldivas, Islas
MW Malawi
MX México
MY Malasia (Malaysia)
MZ Mozambique
NA Namibia
NC Nueva Caledonia
NE Níger
NF Norfolk, Isla (Oceanía; territorio australiano)
NG Nigeria
NI Nicaragua
NL Holanda (Netherlands)
NO Noruega
NP Nepal
NR Nauru, Isla de (Micronesia) (Nauru)
NT Zona Neutral (en este momento se encuentra en Oceanía)
NU Niue, Isla de (Oceanía)
NZ Nueva Zelanda
OM Omán
PA Panamá
PE Perú
PF Polinesia Francesa
PG Papúa Nueva Guinea
PH Filipinas (Philippines)
PK Pakistán
PL Polonia
PM San Pedro y Miquelón, Islas de (Caribe)
PN Pitcairn, Islas (Oceanía, Polinesia)
PR Puerto Rico
PT Portugal
PW Palau, Islas (Polinesia)
PY Paraguay
QA Qatar
RE Reunión, Isla (África)
RO Rumania (Romania)
RU Federación Rusa
RW Ruanda (Rwanda)
SA Arabia Saudita (Saudi Arabia)
Sb Salomón, Islas
SC Seychelles, Islas
SD Sudán
SE Suecia
SG Singapur
SH Santa Helena, Isla de
SI Eslovenia
SJ Svalbard y Jan Mayen, Islas de (Noruega)
SK República Eslovaca (Slovak Republic)
SL Sierra Leona
SM San Marino
SN Senegal
SO Somalía
SR Surinam (Guayanas)
ST Santo Tomé y Príncipe, Islas de
SU Ex-Unión Soviética (USSR (former))
SV El Salvador
SY Siria (Syria)

SZ Suazilandia (África)
TC Turks y Caicos, Islas de (Bahamas)
TD Chad
TF Territorios Franceses del Sur (África)
TG Togo
TH Tailandia
TJ Tadjikistan
TK Tokelau, Islas (Oceanía)
TM Turkmenistán
TN Túnez
TO Tonga
TP Timor Oriental
TR Turquía
TT Trinidad y Tobago
TV Tuvalu, Islas
TW Taiwán
TZ Tanzania
UA Ucrania
UG Uganda
UK Reino Unido (United Kingdom)
UM Islas Menores-Territorios de ultramar de Estados Unidos
US Estados Unidos de América (United States of America)
UY Uruguay
UZ Uzbekistán
VA Vaticano, Ciudad del
VC San Vicente y Granadinas, Islas (Caribe)
VE Venezuela
VG Vírgenes Británicas, Islas
VI Vírgenes Estadounidenses, Islas
VN Vietnam
VU Vanuatu, Islas (Oceanía)
WF Wallis y Futuna, Islas (Oceanía)
WS Samoa
YE Yemen
YT Mayotte
YU Yugoslavia
ZA Sudáfrica
ZM Zambia
ZR Zaire
ZW Zimbabwe

2.2.2. Elementos o secciones de una dirección de correo electrónico.

En cuanto a las direcciones de correo electrónico constan de las siguientes secciones:

Usuario@servidor.nivel más elevado. Código país

Usuario: hace referencia al nombre del usuario que pudo haber sido designado por la empresa prestadora del servicio seleccionado por el mismo usuario.

@: Símbolo arroba que en ingles significa at y en español en.

Servidor: nombre de la empresa que presta el servicio.

Nivel más elevado: hace referencia a esto mismo al nivel que tiene y al dominio.

Código país: solo para hacer referencia al país en el que se encuentra el usuario.

2.3. ACCESO A INTERNET.

Para acceder a Internet hoy en día es muy sencillo, pero técnicamente se requiere:

1. Una computadora o laptop.
2. Modem o una conexión ISDN; esta consiste en que es una red digital de larga distancia capaz de transportar datos de manera directa.
3. El software correspondiente que permita la conexión a Internet.
4. Contar con acceso directo a Internet o acceso a un prestador de servicios de Internet.

2.3.1. Los requisitos mínimos para conectarse a Internet.

Contar con un "procesador 486, con 16 o 32 megabytes (MB) de memoria en RAM y un disco duro de al menos 1GB (un gigabyte) de capacidad. Sin embargo, en la medida en que el usuario vaya apreciando los servicios que le ofrece internet, querrá disponer de más espacio de disco; por lo tanto, es aconsejable que adquiera, desde un principio, uno de 3.0 a 4.0GB de capacidad."[9]

En cuanto al módem, hoy en día tienen incluido un módem interno; "…si no es así, se puede adquirir en el comercio local que mediante un cable se conecta a uno de los puertos de su computadora. Su velocidad se mide por la cantidad de bits de información que puede transferir cada segundo (bps). Hoy en día se ofrecen módems 36.600 o 56.000 bps a un precio que es directamente proporcional a la velocidad que alcanzan. Esto significa que, entre más rápida sea la transmisión de los datos, mejor será su conexión a internet. Sin embargo, la velocidad a la que su computadora puede enviar y recibir datos, no solamente depende del modem, sino también de la calidad de la línea telefónica y de la cantidad de gente que esté conectada a la red de su proveedor más el trafico (flujo de datos o información) en internet al mismo tiempo."[10]

Requieren además contar con línea telefónica, la que sirve "…para establecer una conexión tipo DUN (Dial Up Network) del Inglés: Red de Marcado o más conocida como red de acceso telefónico, esta debe de estar en buen estado y sin ruido para un flujo óptimo."[11]

Es necesario contar con un proveedor de acceso, gracias a que el mercado actual de proveedores es amplio ya no es tan costoso como al principio ya que "… los primeros proveedores que tuvo el mercado cobraban tarifas de inscripción y

[9] www.gatelink.net/gatelink/tips/internet/req.htm Página de Internet consultada el doce de marzo del 2012
[10] Op. Cit.
[11] Ibídem.

mensualidades que estaban lejos del alcance del bolsillo promedio"[12] y solo las personas de clase alta podían acceder a estas desde sus hogares las demás para poder usar Internet tenían que acudir a los ya no tan necesarios café-Internet.

2.3.2. Ingresar a Internet: costo.

Actualmente acceder a Internet es muy económico, y ya casi cualquier persona cuenta con servicio de Internet en su casa, aunque la verdad para llegar a este punto tuvieron que aparecer nuevos servidores y compañías que hicieran competencia obligando a los pocos servidores a bajar sus precios o desaparecer del mercado de no hacerlo, las tarifas eran realmente muy excesivas y personas de clase alta eran las que contaban con Internet en sus hogares lo que provoco que la existencia de los café-Internet fuera tan popular y un gran negocio para los dueños, hoy en día ya es menos usual y en su mayoría solo acuden a estos gente de clase media-baja.

2.4. MEDIDAS DE SEGURIDAD Y RIESGOS EN INTERNET.

2.4.1. Uso de la red y sus riesgos potenciales.

Internet surgió como un medio de comunicación rápido y efectivo, como la forma en que las personas sin salir de sus casas pudiera comunicarse entre sí de una forma rápida, sencilla y económica. Para que se lograra este objetivo se dejaron en segundo término el tema de la seguridad, pues en su inicio lo que se planteaba era que las personas podrían usar esta para algo positivo y sin fines negativos.

En el espacio de los juristas deben tenerse presentes los riesgos que se pueden presentar con el uso de la red. De cualquier forma hay que señalar que todo medio de comunicación lleva consigo riesgos de seguridad. Desde los

[12] Ídem.

medios impresos ya sean revistas periódicos hasta las llamadas telefónicas. Así para reducir estos riesgos aparece la necesidad de incluir un enfoque legal al uso de Internet a través sobre todo de medidas de seguridad.

Los problemas en materia de seguridad por el uso de Internet aparecen en la esencia del sistema. Internet apareció para funcionar bajo el sistema operativo UNIX que es un sistema operativo portable, multitarea y multiusuario que brinda el fácil acceso a la información, sin embargo descuida el plano de la seguridad a sus usuarios, de ahí que Internet cuente con la misma estructura de seguridad.

2.4.2. Problemas de seguridad propios de Internet.

El hecho de que el sistema ofrezca con gran facilidad el acceso a la información disponible en Internet. De aquí que una persona pueda copiarla, leerla y en su defecto hasta pueda alterarla. Y más grave aun cuando se trata de personas expertas en el uso de computadoras llegan a incluso copiar y robar información privada que puede que no se encuentre ni en Internet, por el uso de ciertos programas que se conocen como virus creados por personas que se les ha denominado hackers, los virus son programas de cómputo que se introducen de manera clandestina en otros programas y archivos, estos llevan finalidades distintas mismas que más adelante se detallaran.

Para el caso de los abogados la existencia de hackers es un problema realmente grave, a modo de ejemplo, cuando se trata de litigantes el tener datos que son sobre sus clientes en los que el principio de secreto de confesión dice que se deben mantener en secreto, ¿qué ocurriría si un hacker invade una computadora que sabe que contiene estos datos como medio para saber lo que dijo el cliente del abogado? De ahí que la importancia sea algo que nos ocupe, para lo cual lo más viable es contar con medios de protección para tratar de evitar esto, como el uso de antivirus.

Aunque los riesgos solo son para computadoras que se encuentran conectadas de una manera permanente en Internet o para archivos que se almacenan en una computadora conectada con dicho sistema.

2.4.2.1. Virus informáticos.

Los virus informáticos son programas maliciosos o en inglés llamados malwares, que infectan a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en adherirse a un archivo de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección.

"Su nombre lo adoptan de la similitud que tienen con los virus biológicos que afectan a los humanos, donde los antibióticos en este caso serían los programas Antivirus."[13]

Los virus informáticos tienen la función de propagarse a través de un software, son muy nocivos y algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

2.4.2.1.1. Tipos de virus informáticos.

2.4.2.1.1.1. Virus de Boot.

Uno de los primeros tipos de virus que aparece es conocido como el virus de Boot, este infecta el sector de arranque del sistema operativo. Es muy dañino ya que el virus se activa cuando la computadora es encendida y el sistema operativo se carga.

[13] www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos Página de Internet consultada el quince de marzo del 2012

2.4.2.1.1.2. Time Bomb o Bomba de Tiempo.

Este tipo de virus del tipo llamados bomba de tiempo, reciben ese nombre porque son programados para que se activen en determinados momentos, definido por su creador. Una vez que el virus ha infectado un sistema, este se activará y causará algún tipo de daño en el día o el instante que previamente fue definido. Algunos virus de este tipo que se hicieron famosos, son el Viernes 13 y el Michel Ángelo.

2.4.2.1.1.3. Gusanos, lombrices o worms.

Estos virus nacieron con la idea de hacer un virus pudiera esparcirse de la forma más amplia posible, de hecho sus creadores a veces se enfocan más en esta cualidad de que se multipliquen que dejaron de lado el hecho de dañar el sistema de los usuarios infectados quedando estos sin el objetivo de causar graves daños al sistema. De esta forma, sus autores tratan de hacer sus creaciones más conocidas en internet. Este tipo de virus pasó a ser llamado gusano o worm debido a esa característica de esos tipos de insectos que comen y dejan sus larvas a su paso. Estos son cada vez más perfectos, de hecho hay una versión que al atacar la computadora, no sólo se replica, sino que también se propaga por internet enviándose a los e-mail que están registrados en el cliente de e-mail, infectando las computadoras que abran aquel e-mail, reiniciando el ciclo.

2.4.2.1.1.4. Troyanos o caballos de Troya.

Quizás los más conocidos, mencionados y hasta temidos en Internet son los Troyanos, estos son virus que traen en su interior un código aparte, código que le permite a una persona acceder a la computadora infectada o recolectar datos y enviarlos por Internet a un desconocido, sin que el usuario se dé cuenta de esto.

Inicialmente, los Troyanos permitían que la computadora infectada pudiera recibir comandos externos, sin que el usuario se percatara de esto. De esta forma el creador del virus podría leer, copiar, borrar y alterar datos del sistema. Actualmente los caballos de Troya tienen la intención de robar datos confidenciales del usuario, como contraseñas bancarias, lo cual es realmente peligroso y dañino principalmente al patrimonio del usuario.

Los demás virus eran en el pasado, los mayores responsables por la instalación de los caballos de Troya, como parte de su acción, pues estos no tienen la capacidad de replicarse. Actualmente, los caballos de Troya se han vuelto más peligrosos ya que no llegan exclusivamente transportados por virus, ahora son instalados cuando el usuario baja un archivo de Internet y lo ejecuta. Esto es una práctica eficaz debido a la enorme cantidad de e-mails falsos que llegan a los buzones de los usuarios, e-mails que contienen una dirección en la web para que la víctima descargue, sin saberlo, el caballo de Troya, en vez del archivo que el mensaje dice que es, a esta práctica se le ha denominado como phishing, la cual es una expresión derivada del verbo en inglés to fish, que en español significa pescar. Hoy en día la mayoría de los caballos de Troya simulan ser webs bancarias, como forma de obtener la contraseña que es introducida por los usuarios de las computadoras infectadas.

2.4.2.1.1.5. Hijackers.

En el mundo de la informática los hijackers son aquellos programas o scripts que de cierta forma son muy molestos ya que cuando atrapan a navegadores de Internet no los dejan salir ya que cuando eso pasa, el hijacker altera la página inicial del navegador e impide al usuario cambiarla, entonces invade con publicidad a través de pop-ups o ventanas nuevas, además instala barras de herramientas en el navegador que en su mayoría solo hacen más lento al sistema operativo y pueden impedir el acceso a determinadas webs.

2.4.2.1.1.6. Keylogger.

Keylogger se define como una de las especies de virus existentes, el significado de este en inglés que más se adapta al contexto sería: Secuestrador de teclas. Ya que luego que son ejecutados, usualmente los keyloggers quedan escondidos en el sistema operativo, de manera que el usuario no sabe que se encuentra vigilado y que su computadora hasta de cierta forma controlada. Hoy en día los keyloggers son desarrollados para medios ilícitos, entre los que destaca el robo de contraseñas bancarias. Estos virus son utilizados en potencia por usuarios con un poco más de conocimiento para poder obtener contraseñas personales, como cuentas de email, MSN, Facebook, twitter y demás redes sociales, por mencionar algunos. En la actualidad existen tipos de keyloggers que capturan la pantalla de la víctima, como una manera de saber lo que la persona está haciendo en la computadora. Estos virus tienen la cualidad de que lejos de ser dañinos al equipo, son una especie de espías.

2.4.2.1.1.7. Zombie.

Este tipo de virus recibe ese nombre inspirado en las películas de ciencia ficción y terror, puesto que el estado zombie en una computadora ocurre cuando es infectada y está siendo controlada por terceros. Pueden usarlo para diseminar virus, keyloggers, y procedimientos invasivos en general. Usualmente esta situación ocurre porque la computadora tiene su Firewall y/o sistema operativo desactualizado. Según estudios, una computadora que está en internet en esas condiciones tiene casi un 50% de chances de convertirse en una máquina zombie, pasando a depender de quien la está controlando, esto ocurre casi siempre con fines criminales.

2.4.2.1.1.8. Virus de Macro.

Los virus de macro o macro virus, son aquellos que vinculan sus acciones a modelos de documentos y a otros archivos de modo que, cuando una aplicación carga el archivo y ejecuta las instrucciones contenidas en el archivo, las primeras instrucciones ejecutadas serán las del virus.

Los virus de macro son muy similares a otros virus en varios aspectos, es decir son códigos escritos que bajo ciertas condiciones, este código se multiplica, haciendo una copia de él mismo. Y como otros virus, pueden ser desarrollados para causar daños, presentar un mensaje como podría ser una broma o hasta hacer cualquier cosa que un programa pueda hacer.

2.4.3. Medidas de seguridad aplicadas en Internet.

En este sentido lo más importante es que los estudiosos del derecho tengan el conocimiento de los riesgos que se presentan con el uso de Internet, sin que influya esto para que dejen a un lado las ventajas del uso de este. Porque si bien son reales a veces son ya en un caso muy especial como el que se mencionaba que un hacker desee robar una información en específico, realmente lo más común que se presenta es la presencia de virus, sin embargo para prevenir un ataque es mejor tomar medidas como las que se señalan a continuación.

Para comenzar hay que mencionar el problema que se presenta entre las personas en Internet, citando por ejemplo el de los abogados con sus clientes, si un abogado se comunica con su cliente por Internet lo más adecuado sería que le advirtiera que el uso de este conlleva riesgos de que sean interferidos y leídos por otras personas. Así lo mejor sería evitar él envió de documentos importantes por la red a menos que se desee correr el riesgo de esto.

Otra opción para los abogados es elegir entre conectarse desde la computadora de la oficina o despacho o si desea que sea desde la propia a modo de no exponer la que contenga la información confidencial, aunque lo mejor sería que se tuviera una computadora especial para el trabajo en Internet y otra para lo que no deseamos que llegue a exponerse por esta, aunque el problema que acarrea es el precio de comprar varias computadoras.

Una medida muy recomendada es realizar respaldos de información o copias de seguridad también llamados backups, de los archivos de las computadoras enlazadas a Internet.

El uso de antivirus también es una medida que resulta muy útil, ya que aunque no existe un antivirus que proteja al cien por ciento de la invasión de estos, el contar con uno o unos es mejor ya que una computadora conectada todo el tiempo a la red sin una protección hará que esta se infeste de virus y que incluso llegue a quedar inservible.

Existen antivirus capaces de detectar la posibilidad de virus en Internet y advierten al usuario cuando descubren algo sospechoso, además, ahora ya examinan archivos comprimidos (forma en la que están muchos documentos y archivos disponibles en la red) antes de abrirlos.

Una medida que resulta muy efectiva pero en consecuencia muy cara es el uso de una computadora firewall, que consiste en que se conecta con la computadora que tiene acceso a Internet y se encarga del examen antivirus previo y en su caso, de la limpieza de los archivos que consultaran por medio de Internet.

Otra medida útil es la codificación de los correos electrónicos y demás información que se envié a través de Internet, de tal manera que no sea posible que terceros sin autorización puedan leerlos.

"Los riesgos de la seguridad en Internet provocan que la codificación de datos sea un procedimiento al que los juristas que utilizan el sistema recurren con mucha frecuencia. En la actualidad se examina en Estados Unidos de América la necesidad de que un abogado se halle obligado a codificar información que envía a su cliente por Internet. Debido a que en ese país el abogado solo se ve obligado a mantener en secreto la información que él o su cliente no deben poner a disposición del público, se plantea también la cuestión de si el abogado debe guardar el secreto profesional de las informaciones no codificadas a disposición del público en Internet."[14]

2.5. SERVICIOS QUE OFRECE INTERNET.

Actualmente el servicio q ofrece Internet que ha tenido más auge y por lo tanto mayor importancia es la WORLD WIDE WEB (WWW). Este servicio es quien ha permitido la comunicación y enlace de cientos de miles de servidores con los usuarios.

La World Wide Web fue creada y aparece a finales del siglo pasado. Conceptualizada en 1989 y comenzando a proporcionar sus servicios al público en 1993. Actualmente existen billones de páginas web y han aparecido millones de servidores desde su creación. A mediados del año 1996, ya existía un promedio de dos mil servidores nuevos por día.

Con la WWW se ha vuelto prácticamente muy sencillo navegar a través de Internet, ya que esto ha hecho muy fácil el flujo de información y el acceso a la que encontramos en la red, que puede ser desde documentos, bases de datos hasta videos, imágenes, música, etc. Para esto la www utiliza una interfaz o lenguaje demarcado de hipertexto (HTML), este permite que se establezca una

[14] ROJAS AMANDI, Víctor Manuel. Op. Cit. Nota 4., p. 14

conexión con otra página y otro sitio de Internet, sin utilizar el menú, a estos se les llama hipervínculo o en ingles hyperlink.

2.5.1. Beneficios para los juristas en Internet.

En Internet para nosotros los abogados hay muchos servicios de interés, como el correo electrónico que permite la comunicación con usuarios de cualquier parte del mundo que cuenten con computadoras conectadas a Internet.

Otro servicio que brinda el Internet para apoyo de los abogados es el ftp que facilita el flujo de la información de una computadora a otra, esto se encuentra integrado a los navegadores actuales y ya no necesita el usuario manejar una habilidad especial más allá de la del uso normal de las computadoras, como lo era al principio ya que solo basta ingresar a un navegador y en este escribir la dirección ftp y seleccionar el archivo deseado.

Un servicio más es el Gopher que es un servicio de dirección de menú que en la actualidad ya no se utiliza tanto, aunque facilita la búsqueda de información, pero por su desventaja ante WWW de que no facilita una conexión de hipertexto.

Un servicio más que se menciona es Telnet, el cual es un programa que hace posible que los usuarios de Internet se pongan en contacto con otra computadora usando la propia como terminal, pero como Telnet es un programa de UNIX hace que sea más difícil su uso por lo que prevalece más el uso de WWW.

CAPÍTULO III
LEGISLACIÓN MEXICANA E INTERNACIONAL EN MATERIA DE INTERNET.

3.1 INTERÉS DEL DERECHO EN INTERNET.

Los juristas ingresamos a Internet desde el momento en que este fenómeno global ha influido en todas las ciencias existentes, y como era de esperarse, afecta directamente las relaciones interpersonales al permitir este medio la comunicaciones entre sujetos de todo el mundo, inclusive hace posible las compra-venta, permutas, transacciones bancarias, solo por mencionar algunas, entre personas que quizás nunca tengan contacto físico entre ellas.

El problema aparece cuando personas actúan con dolo y caen en conductas fraudulentas o cuando por el uso de mensajería instantánea o las redes sociales, llámese Facebook o Twitter, llegan a ofender, difamar, amenazar e incluso usurpar a otras personas o el abuso del copyright que cometen las empresas creadoras y responsables de estas, es cuando los estudiosos del derecho nos vemos en la necesidad de buscar una regulación y castigo para todas estas conductas que deben de ser respaldadas por nuestros códigos penales, en

nuestro caso México ha hecho muy poco en ámbito de regulación cibernética, tal es el caso que otros países ya cuentan con leyes o un capitulado dentro de sus códigos penales que regule los nuevos tipos penales a través de Internet mismos que se han denominado delitos cibernéticos o delitos informáticos.

3.2. INFORMÁTICA JURÍDICA Y DERECHO INFORMÁTICO.

3.2.1. Informática Jurídica.

Antes de proseguir consideramos conveniente definir lo que es la informática jurídica ya que está inmersa en el tema de la regulación de Internet, esta es una disciplina de las ciencias de la información que tiene por objeto la aplicación de la informática en el Derecho. Se diferencia del Derecho Informático, puesto que este es la regulación jurídica de las nuevas tecnologías.

3.2.2. Derecho Informático.

El derecho informático es llamado por algunos autores como la otra cara de la moneda, porque afirman que en esta moneda encontramos por un lado a la Informática Jurídica, y por otro, entre otras ciencias, al Derecho Informático. El Derecho Informático se diferencia de la Informática Jurídica en que ya no se dedica al estudio del uso de los aparatos informáticos como ayuda al derecho, sino que con él se integra el conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática, es decir, que desde este punto de vista la informática en general es regulada por el derecho.

El derecho informático constituye una ciencia, que estudia la regulación normativa de la informática y su aplicación en todos los campos. Pero, cuando se dice derecho informático, entonces se analiza si esta ciencia forma parte del

derecho como rama jurídica autónoma; así como el derecho es una ciencia general integrada por ciencias específicas que resultan de las ramas jurídicas autónomas, tal es el caso de la civil, penal y contencioso administrativa.

3.3. LOS DELITOS CIBERNÉTICOS Y SU REGULACIÓN INTERNACIONAL.

El fenómeno global de internet ha traído consigo problemas que ya hemos mencionado, los países europeos son los que han incursionado principalmente en este aspecto, haciendo legislaciones completas o capítulos que se han ingresado a sus códigos penales. “En función del innegable carácter económico inherente a este problema, es conveniente presentar la situación internacional de hecho y de derecho en torno al mismo, estructurada en tres grupos de países bien definidos de acuerdo al régimen jurídico prevaleciente, a saber: los que regulan el problema desde la constitución, los que lo hacen mediante leyes generales y quienes disponen de una ley particular al respecto.”[15]

3.3.1. Regulación Constitucional.

Existen países que debido a la gran trascendencia e impacto que ha tenido Internet entre la sociedad, han decidido regular a este fenómeno desde sus cartas magnas. Entre los países que optaron por esta medida, podemos señalar a Austria, España, Holanda, Portugal y Suiza entre otros, siendo Portugal en 1976, el primer país que considero esta situación a nivel internacional. España en 1978 dispuso sus limitaciones de que será objeto la informática en función del honor y la intimidad personal y familiar de los ciudadanos.

[15] TÉLLEZ VALDÉS, Julio. *Derecho informático*. Tercera edición. México. McGraw Hill. 2004. p. 63.

3.3.2. Regulación mediante una ley general.

Existe el caso de que países que han optado por incluir en sus cuerpos de leyes existentes o algunos que se crean, la regulación del uso de las computadoras, de ahí que se mencionen a ejemplo los siguientes.

3.3.2.1. Estados Unidos de América: *Privacy Act.*

En los Estados Unidos de América cuentan con la Privacy Act de diciembre de 1974, esta surgió como una solución a la protección de la vida, misma en la que se señala que el órgano jurisdiccional competente para imponer sanciones de tipo penal son los tribunales federales. Esta ley se complementa con otras leyes como la *Fair Credit Reporting Act, la Equal Credit Opportunity Act, la Fair Debt Collection Practices Act, la Right to Financial Privacy Act, la Fair Credit Billing Act, la Bank Secrecy, la Tax Reform y la Family Educationnal Right and Privacy Act, pero sobre todo la Freedom of Information Act o FOIA* por sus siglas en inglés es la más importante de todas estas.

3.3.2.2. Canadá: *Human Rights*.

En Canadá en julio de 1977 nace la *Human Rights* misma que se inspira de la ley de su país vecino Estados Unidos. La *Human Rights* señala en su capítulo IV los problemas derivados del uso de la computadora con respecto a los derechos humanos, en este capítulo se señala la creación de una autoridad que fungirá como el comisario para la protección de la vida privada de las personas quien se encargará de velar el cumplimiento de esta ley, mismo que es nombrado por el ministro de justicia.

3.3.3. Regulación mediante una ley específica.

En cambio existen países que para enfrentar este problema han creado una ley especial al respecto puesto que han llegado a la conclusión de que integrar en códigos, leyes generales o en la misma constitución no sería suficiente puesto que es necesario contemplar varias características que no se abordarían de otra forma que con la creación de una ley que se base totalmente en lo que es el Internet. A continuación señalaremos unos ejemplos de lo que han optado hacer otros países del mundo ante este problema.

3.3.3.1. Suecia: *Datalog*.

El primer país en tener una regulación a nivel nacional fue Suecia, mismo que con su Datalog o ley del 11 de mayo de 1973 se convierte en el pionero en tomar esta medida, cabe señalar que Suecia fue el primer país con regulación nacional porque la primera ley que existió a nivel mundial fue de corte local, en 1970 en el Bünder o estado Alemán de Hesse.

Suecia cuenta con un organismo supervisor que es la data Inspektion Board (DIB); la Datalog es complementada por la ley de información sobre Solvencia de 1973 y la ley de trabajo y cobro de créditos por cuenta ajena de 1974.

3.3.3.2. Alemania: *Datenschutzegesetz.*

Otro país es Alemania quien actualmente cuenta con la Bündes Datenschutzegesetz o ley Federal de protección de datos de 27 de enero de 1977, quien contempla la existencia de un comisario federal de datos quien debe velar su cumplimiento y misma que es complementada por diversos ordenamientos.

3.3.3.3. Francia: Ley de Informática Archivos y Libertades.

En Francia existe la ley de informática, Archivos y Libertades del 6 de enero de 1978, en esta se crea la Comisión Nacional de Informática y Libertades (CNIL), y se le concibe como un órgano especial y autónomo con funciones de control por medio de reglamentos, el cual cuenta con derecho a informarse y a su vez la obligación de informar

3.3.3.4. Otros países.

A su vez existen otros países que tienen disposiciones específicas como Dinamarca quien cuenta con sus leyes sobre Archivos Públicos y Privados del 8 de junio de 1978, en Noruega tienen la Ley sobre Datos de Carácter Personal del 9 de junio de 1978, después en Austria crean la ley de Protección de Datos del 18 de octubre de 1978, y en Luxemburgo hacen su Ley Reglamentaria de la utilización de datos nominativos en los tratamientos informativos del 11 de abril de 1979, así como a su vez la de Islandia del 1º de enero de 1982 y la de Gran Bretaña del 1º de julio de 1984.

Algunos otros países, preocupados por la trascendencia del problema, de manera más reciente han aprobado en su legislatura leyes particulares en materia de protección de datos, como es el caso de España, Bélgica, Portugal, Holanda, Japón, Italia, Finlandia, Australia, Nueva Zelanda y numerosos países más, algunos de los cuales lo regulan de manera concurrente, es decir, a través de una ley nacional y de leyes estatales, regionales o locales.

3.3.4. El Puerto Seguro o *Safe-Harbor*.

A principios del año 2000 las administraciones de los EUA y la Unión Europea (EU) se llegaron a un acuerdo en el cual las empresas estadounidenses

que se unieran al programa denominado safe-harbor, en materia de protección de datos no se verían sancionadas por la administración de la Unión Europea. Tras esto Safe Harbor entro en vigor el 1º de noviembre de 2000.

3.3.5. Panorama de los Organismos y Comités Internacionales.

Antes de adentrarnos a la regulación que ha optado cada país nos referiremos brevemente a lo que han realizado los principales organismos y comités internacionales en materia de regulación de datos en la red.

Comunidad Europea: La Comunidad Europea decretó la Directiva Europea 95/46/CE relativa a la protección de las personas físicas con respectos a los datos de carácter personal y a la libre circulación de estos datos de 24 de octubre de 1995. Esta comunidad creó una autoridad denominada la Comición Europeenne DG Marche Interieeur.

Página de Internet: http://europa.eu.int/comm/internal_market/fr/index.htm

Consejo de Europa: Cuenta con el Convenio 108 para la protección de las personas respecto al tratamiento automatizado de los datos de carácter personal de 28 de enero de 1981 (convenio de Estrasburgo). El consejo señaló en el convenio la creación de Consell de l´Europe Direction des Affaires juridiques Section Protection.des Donnees como autoridad de vigilancia y control de este.

Página de Internet: www.legal.coe.int/dataprotection

OCDE: La Organización para la Cooperación y el Desarrollo Económicos cuenta con las Líneas Directrices reguladoras de la protección de la vida y los flujos transfronterizos de datos de carácter personal de 23 de septiembre de 1980. Es regulada y vigilada por la misma OCDE.

Página de Internet: www.oecd.org/index-fr.htm

Organización de las Naciones Unidas: En el caso de la Organización Mundial más conocida y reconocida por casi todos los países del mundo, optaron por crear las Líneas Directivas para la reglamentación de los Archivos informatizados de datos de carácter personal de 1989.

Página de Internet: www.unhchr/french/htmlintlinst_fr.htm

3.3.6. Países con regulación en materia de Internet.

A continuación se enlistaran los países que cuentan con ordenamientos legales acerca de la materia, además de si crearon una autoridad para su vigilancia y cuál es su página en Internet.

Albania: Ley 8517 Sobre La Protección De Datos Personales de 1999

Alemania: Ley Federal Del 21 De Enero De 1977 Para La Protección Contra El Empleo Abusivo De Datos De Identificación Personal En El Cuadro De Tratamiento De Datos de 1977, modificada por la Ley Federal De Protección De Datos De 20 De Noviembre De 1990, reformada por ley del 14 de Septiembre de 1994. Adecuación a la Directiva Europea 95/46/CE con su Ley Federal De Protección De Datos de 2001. Legislación en cada uno de sus territorios federales o Lander.

Autoridad creada: Bundesbeauftragle für den Dalenschutz.

Página de Internet: www.Dalenschutz.de

África del Sur: Ley De Fomento Al Acceso De Información Del 2000.

Argentina: Ley 25.326 Sobre La Protección De Datos Personales de 2 de noviembre d 2000. Cabe mencionar que la comisión Europea, mediante la Decisión 2003/490/CE, de 30 de junio de 2003 (Diario Oficial de la Unión Europea L 168, de 5 de julio de 2003), ha reconocido que Argentina proporciona un nivel de

protección adecuado para los datos personales. Esta decisión permite el libre tránsito de datos personales desde la Unión Europea hacia Argentina sin requerir garantías adicionales. La decisión adoptada por la comisión se tomó después de contar tanto con el dictamen favorable de las autoridades de protección de datos europeas como con el voto favorable de los estados miembros y del parlamento Europeo.

Australia: Ley Federal Sobre La Vida Privada de 1988 para el Sector Público y para el sector privado de 6 de diciembre de 2000.

Autoridad creada: Federal Privacy Commission.

Página de Internet: www.privacy.gov.au

Austria: Ley Federal sobre la protección de datos de 18 de octubre de 1978, modificada en 1986 adecuación a la Directiva Europea 95/46/CE con su ley de protección de datos de 2000.

Autoridad creada: Director buro der Datenschutzicommission und des datenschutzrater.

Página de Internet: www.bka.gv.at/datenschutz

Bélgica: Ley Relativa A La Protección De La Vida Privada Con Respecto A Los Tratamientos De Datos De Carácter Personal de 8 de diciembre de 1992. Adecuación a la directiva Europea 95/46/CE con su ley de 11 de diciembre de 1998, con ejecución mediante decreto real de 13 de marzo de 2001.

Autoridad creada: Commission De La Pretection De La Vie Privée, Ministere De La Justice.

Página en Internet: www.privacy.fgov.be

Bulgaria: Proyecto de la Ley de Preparación.

Canadá: Ley Federal sobre la Protección de las informaciones personales de 1982 y de documentos electrónicos de 2000.

Autoridad creada: Federal Privacy Commission.

Página de Internet: www.orivcom.gc.ca

Chile: Ley Para La Protección De La Vida Privada De 1999.

Chipre: Ley de 2001.

Corea del sur: Ley Sobre La Protección De Datos Personales De 1994.

Dinamarca: Ley 293 Sobre Registro Privados Y Ley 294 Sobre Registros De Los Poderes Públicos, ambas de 8 de junio de 1078, reformadas en 1988 y 1991. Adecuación a la Directiva Europea 95/46/CE con su ley parcial de 1º de octubre de 1998 y ley 429 de 31 de mayo de 2000.

Autoridad creada: Datatilsynet

Página de Internet: www.datatilsynet.dk

España: LORTAD de 1992, abrogada por la Ley Orgánica de protección de datos de carácter personal de 13-12-1999 (transposición por la directiva europea 95/46/CE).

Autoridad creada: Agencia de Protección De Datos

Página de Internet: www.ag-protecciondatos.es

Estonia: Ley Sobre La Protección De Datos Personales de 1997.

Autoridad creada: Estonia data protection inspektorate.

Página de Internet: www.dp.gov.ee

Eslovaquia: Ley Sobre La Protección De Datos Personales De Los Sistemas Informativos De 1998.

Autoridad creada: Office for the protection of personal data.

Eslovenia: Ley 210-01/89-3 Sobre La Protección De Datos Personales De 1999.

Autoridad creada: Namestnik varuha clovekovih pravic.

Estados Unidos de América: Ley Sobre La Protección De Las Libertades Individuales De La Administración Federal De 1974 (Ley de Privacidad)

Autoridad creada: Federal tradecommission.

Finlandia: Ley De 30 De Abril De 1987sobre Los Archivos De Datos De Carácter Personal, modificada por Ley de 7 de abril de 1995. Adecuación a la directiva de europea 95/46/CE con su ley 523 de 10 de febrero de 1999.

Autoridad creada: Office of the data protection ombudsman.

Página de Internet: www.tietosuoja.fi

Francia: Ley 78-17 de 6 enero de 1978, relativa a La Informática, Archivos Y Libertades. Adecuación a la Directiva Europea 95/46/CE con su proyecto de ley. Aprobado en la 1ª lectura en el senado el 1º de abril de 2003.

Autoridad creada: Commission nationale de l´ informatique of tes libertes.

Página de Internet: www.dpa.gr

Grecia: Ley 2472 Sobre La Protección De Las Personas Respecto Al Tratamiento De Datos De Carácter Personal de 26 de marzo de 1997. Adecuación a la Directiva europea 95/46/CE con fecha de 26 de marzo de 1997.

Autoridad creada: Comisión para la protección de datos.

Página de Internet: www.dpa.gr

Holanda: Ley Sobre Protección De Datos de 28 de diciembre de 1988, completada por Ley De Archivos Policiacos de 21 de junio de 1990. Adecuación a la Directiva Europea 95/46/CE con su Ley de 6 de julio de 2000.

Autoridad creada: Data protection authority.

Página de Internet: www.cbbpweb.nl

Hong Kong: Ley Sobre Protección De Datos de 1990. Ordenamiento Sobre Protección De Datos De 1995.

Autoridad creada: Privacy Commission for personal data.

Página de Internet: www.pco.org.hk

Hungría: Ley Sobre Protección De Datos Personales Y La Comunicación De Datos Públicos de 1992.

Autoridad creada: Parliamentary commissioner for data protection and Freedom of Information.

Página de Internet: www.obh.hu

India: Ley De La Información Tecnológica de 2000.

Irlanda: Ley Sobre La Protección De Datos de 13 de julio de 1988 adecuación a la Directiva Europea 95/46/ CE con su Ley de 18 de febrero de 2002.

Autoridad creada: Data protection commissioner.

Página de Internet: www.dataprivacy.ie

Islandia: Ley 63 Relativa Al Registro De Datos Personales de 1981. Reformada en 1989. Incorporada en su legislación nacional la Directiva Europea 95/46/CE para crear la Ley número 77 de 23 de mayo de 2000.

Autoridad creada: Personuvernd raouararstig.

Página de Internet: www.personuvernd.is

Israel: Ley Número 5741 Sobre La Protección De La Vida Privada de 1981, reformada en 1985 y 1996 y Ley Numero 5746 Sobre La Protección De Datos En La Administración de 1986.

Autoridad creada: Registrar of data bases

Italia: Ley 675 Sobre La Protección De Datos Personales De 31 De Diciembre de 1996, modificada en 1997,1998 y 1999. Ley 325 Sobre Las Medidas De Seguridad En El Tratamiento De Datos Personales de 3 de noviembre de 2000.

Autoridad creada: Garante per la protezione der dati personali.

Página de Internet: www.garanteprivacy.it

Japón: Ley Sobre La Protección De Datos Personales Informatizados Del Sector Publico de 1988 y en el Sector Privado de mayo de 2001.

Autoridad creada: Personal data protection task forcé.

Letonia: Ley Sobre La Protección De Datos de abril de 2000.

Autoridad creada: Ministry of Justice Of The Republic Of Latvia.

Lituania: Ley Sobre Protección De Datos Personales de 1996. Reformada en 2000.

Autoridad creada: State data protection inspectorate.

Página de Internet: www.is.lt/dsinsp

Luxemburgo: Ley Sobre Uso De Datos Nominativos Y En Los Tratamientos Informáticos de 31 de marzo de 1979 reformada en 1992. Adecuación a la Directiva Europea 95/46/CE con su proyecto de ley.

Autoridad creada: Commission consultative a la protection des Donnees.

Mónaco: Ley 1,165 Relativa Al Tratamiento De Informaciones Normativas de 1993.

Autoridad creada: Commission de controle des informations nominatives.

Noruega: Ley Sobre El Registro De Datos Personales de 1978. Incorporación en su legislación nacional de la Directiva Europea 95/46/CE creando la ley de 14 de abril de 2000.

Autoridad creada: Datatilsynet.

Página de Internet: www.datatilsnet.no

Nueva Zelanda: Ley Sobre La Información De Sector Publica de 1982. Ley Sobre La Vida Privada De 1993.

Autoridad creada: Privacy Commission.

Página de Internet: www.privacy.org.nz

Paraguay: Ley Sobre Protección De Datos de 28 de diciembre de 2001.

Polonia: Ley Sobre La Protección De Datos Personales de 1997.

Autoridad creada: Biuro geneeralnego inspektora.

Página de Internet: www.cnpd.pt

Portugal: Ley 10 Para La Protección De Datos De Carácter Personal Frente A La Informática de 29 de abril de 1991. Modificada por ley de 1º de agosto de 1994. Adecuación a la Directiva Europea 95/46/CE con la Ley 67 de 26 de octubre de 1998.

Autoridad creada: Comíssáo nacional de proteccao de datos informatizades.

Página de Internet: www.cnpd.pt

Reino Unido: Ley Sobre Protección De Datos de 12 de julio de 1988 adecuación a la Directiva Europea 95/46/CCE con su Ley de 16 de julio de 1998 y Ley Sobre Acceso A La Información de 30 de noviembre de 2000.

Autoridad creada: The office of Information commissioner.

Página de Internet: www.dataprotection.gov.uk

República de San Marino: Ley Relativa A La Protección De Datos Personales de 1983, reformada en 1995.

República Checa: Ley Sobre La Protección De Datos Personales De Los Sistemas Informáticos de 1992. Ley 101 Sobre Protección De Datos Personales de 10 de junio de 2000.

Autoridad creada: Office for personal data protection.

Página de Internet: www.uoou.cz

República de Macedonia: Ley Sobre La Protección De Datos Personales de 1994

Rumania: Ley Sobre La Protección De Datos De Carácter Personal números 677 de 2001 y 790 de 12 de diciembre de 2001.

Autoridad creada: Le Mediateur.

Rusia: Ley Sobre La Información, La Informatización Y La De Informaciones de 1995.

Suecia: Ley Sobre La Protección De Datos de 11 de mayo de 1973. Adecuación a la Directiva Europea 95/46/CE con su ley 204 de 24 de octubre de 1998.

Autoridad creada: Datainspeltionen.

Página de Internet: www.Datainspeltionen.se

Suiza: Ley Federal Sobre La Protección De Datos de 1992.

Autoridad creada: Commissaire a la protection des donnóes.

Página de Internet: www.edsv.ch

Taiwán: Ley Sobre La Protección De Datos Des Sector Público de 1995.

Autoridad creada: Ministry of justice.

Tailandia: Ley Sobre La Protección De Datos Des Sector Público de 1998.

Autoridad creada: Authority for the Protection of Personal Data.

Turquía: Proyecto de Ley.

En estos casos como podemos observar hay países que cuentan con leyes y verdaderos cuerpos legales para la protección de datos, pero al respecto la Unión Europea tiene una directiva (de obligado cumplimiento), la 95/46/CE, que señala la prohibición de transferir datos personales a un tercer país que no tenga un adecuado sistema de protección de la privacidad.

Pero en los Estados Unidos de América, por el contrario, no cuentan con una legislación amplia sobre la materia, por lo que se basan principalmente en la autorregulación.

“Las empresas Estadounidenses no parecen tener las cosas muy en claro, por lo que se muestran indiferentes por dicho acuerdo. Primero por no estar acostumbrados a plantearse el problema de la privacidad de la misma manera que en Europa se hace, aun cuando el acuerdo es bastante permisivo con la manipulación de datos desde el punto de vista de las propias leyes Europeas; segundo porque a las empresas les puede costar bastante dinero adecuar su infraestructura a dicha legalidad; y tercero por que será difícil para Europa mantener un control sobre lo que se hace en realidad con los datos del otro lado del atlántico.

Para obtener la exención europea las empresas estadounidenses, deben suscribirse a programas como el TURSTE o el BBB on line, y comprometerse a seguir, al menos, siete principios cuando utilicen y manejen datos personales de ciudadanos europeos. Así, por ejemplo, se prevén los derechos de información, de rectificación o de ser eliminado de la base de datos, ser informado sobre las

posibles cesiones de datos a terceros y el derecho a que existan sistemas seguros de acceso a los datos."[16]

3.3.7. Legislaciones y Convenios de Protección del Ciberespacio en Latinoamérica.

Como ya se ha visto, diversos son los tratados y legislaciones que existen en todo el mundo con referencia a las formas en las que pueden ser regulados los delitos informáticos y el uso de las tecnologías de la información y comunicación, cada ordenamiento jurídico guarda diferentes formas de proteger la seguridad de los internautas, por el hecho de que cada país resguarda bienes jurídicos distintos en su afán de proteger el ciberespacio.

Es de vital importancia analizar las legislaciones de otros países en el mundo, examinar sus procedimientos y la aplicación de sanciones, los resultados que se han logrado, avances, retrocesos y debilidades.

Hacer un comparativo con lo establecido en los ordenamientos nacionales para comprobar y/o procurar dar una visión de lo que puede México como nación, establecer en sus normas para tener una mayor eficacia en cuanto hace a la protección de delitos informáticos.

Tras ya haber analizado brevemente a los países europeos e inclusive los de Norteamérica, pasaremos a aquellos países pertenecientes a Latinoamérica, entre los que se encuentran: Cuba, Argentina y Chile; así como también se nos hace interesante hacer una investigación más a fondo de un país europeo como el caso de España; otros a analizar serán los correspondientes a cumbres mundiales en las que se consideran medidas preventivas y protocolos de acción para disminuir la delincuencia en medios informáticos y a través de ellos.

[16] ROJAS AMANDI, Víctor Manuel. Op. Cit. p. 72.

Si bien es cierto, México se encuentra rezagado en sus mecanismos de defensa y protección, también es cierto que han surgido iniciativas de reformas actuales en los ordenamientos nacionales que pretenden, dadas las circunstancias de vacío, tutelar diversos bienes jurídicos que en la actualidad no gozan de la protección del derecho, ya que los beneficios que ofrecen los medios informáticos deben realizarse de forma segura y confiable y sobre todo libre de los peligros que representa la posibilidad de usar las herramientas informáticas para transgredir, violentar o dañar a los propios bienes informáticos o al emplear éstos para cometer diversas conductas delictivas en perjuicio de terceros, es así como lo expresa la Comisión de Justicia del Congreso de la Unión al ser presentada la iniciativa que reformó diversos artículos del Código Penal Federal con respecto a delitos informáticos.

3.3.7.1. Cuba y el Decreto 209-1996.

"Con el pretexto de defender la seguridad nacional o preservar la unidad o valores nacionales, muchos gobiernos han optado por impedir a sus ciudadanos un acceso libre a internet. La mayor parte de estos países se encuentran localizados en África y Asia. En especial en Oriente Medio y Asia Central, aunque también países de otros continentes, como Cuba o Ucrania, continúan ejerciendo algún tipo de control sobre los contenidos en la Red"[17].

En este primer ordenamiento a analizar, se tratará de establecer el marco normativo en materia de regulación de delitos informáticos, los bienes jurídicos tutelados y la forma en la que se llevan a cabo los procesos en Cuba, cuando se transgrede un precepto legal establecido.

Tomando en cuenta que para cada país la prioridad de protección es diversa, algunos protegen la libertad de expresión como bien jurídico tutelado y

[17] http://fundacionorange.es/areas/28_observatorio/pdfs/censura.pdf

algunos otros, como es el caso de Cuba, protegen la seguridad de su gobierno, tratando de mitigar el libre tránsito de información que circula en la red de redes llamada, Internet.

Expresarse en Cuba no es igual que hacerlo en México, ya que, según Decreto 209-1996, artículo 7° se limita esa libertad y se establece una autoridad y una serie de requisitos para poder emitir sus opiniones y difundir información en las redes de internet, a la letra dicho artículo dice lo siguiente:

"El ministerio de Ciencia, Tecnología y Medio ambiente tendrá la responsabilidad de establecer las normas relativas de acceso y uso de la información en las redes informáticas de alcance global, así como el establecimiento del Registro para otorgar licencias correspondientes a la difusión de información en redes informáticas de alcance global o nacional".

Con el texto anterior podemos hallar una cierta restricción en cuanto hace, a la difusión de la información que circula por las redes informáticas en Cuba, así como también una persona destinada a su resguardo y quien deberá otorgar permisos y emitir las reglas que considere pertinentes para llevar a cabo el manejo de la difusión de información de manera segura y responsable por parte de los ciudadanos cubanos.

Abordando el mismo ordenamiento, ahora analicemos el capítulo II del Acceso de la República de Cuba a redes informáticas de alcance global, en su numeral 12 segundo párrafo, que a la letra dice:

"Esta política debe asegurar que, la información que se difunda sea fidedigna, y la que se obtenga en correspondencia con nuestros principios éticos, y no afecte los intereses ni la seguridad del país".

Como podemos observar, el bien tutelado en la República de Cuba, es la seguridad de su país, y las leyes que se emitan deberán de pugnar por ésta, la información que se difunda deberá ser cierta y además acorde con los principios éticos del país, por tanto encontramos una segunda restricción en cuanto a la información que circula en la red pero, una de las ventajas que podemos encontrar es que, la información que circula y que difunde el país es certera y cuenta con estándares de calidad que logran cimentar la seriedad del país pero asociado a ello, encontramos poca libertad de expresión y difusión.

Pasemos ahora al respectivo análisis del Artículo 13: “Los servicios de redes informáticas de alcance global tendrán carácter selectivo”.

“Artículo 14: el acceso directo desde la República de Cuba a la información en redes informáticas de alcance global tendrá que estar autorizado por la Comisión Interministerial que se crea por el presente Decreto.”

Un claro ejemplo del carácter selectivo de las redes informáticas de alcance global en Cuba es el mencionado en un artículo publicado por la Asociación Jurídica Cubana, escrito en fecha 8 de diciembre de 2011 por el Licenciado en derecho Veizant Boloy González:

“La red social Facebook, a la que trabajadores del gobierno, podían acceder semanas atrás desde su centro laboral, ha sido bloqueada; así me lo corroboraron un amigo que labora en el MINREX (Ministerio de Relaciones Exteriores) y un vecino que presta servicios en el sector del turismo.

Lejos de ser dañinas, estas redes han cambiado el mundo en que vivimos, nos han acortado el tiempo y la distancia, nos han permitido disfrutar de una nueva vía informativa y comunicativa, nunca antes fantaseada. La razón que la vuelve “dañina” es que, por su extraordinario tráfico, al Gobierno se le dificulta

monitorear y manipular ese gran flujo de información que no puede controlar permanentemente. No es la Seguridad Nacional, ni la escasez de recursos materiales, ni problemas legales, ni de índole ético-moral. Es obvio, que redes sociales o no, el gobierno les teme.

El acceso a las redes en nuestro país tiene un carácter selectivo, algo difícil de creer para los que viven fuera de nuestras fronteras"[18]; el derecho a la libre información, brilla por su ausencia.

Otro ejemplo de la seguridad con tintes de restricción imperante en Cuba y que llega a convertirse en censura en sus redes informáticas, es un estudio realizado por la CPJ, Comité para la Protección de los Periodistas, por sus siglas en inglés, con motivo del día mundial de la libertad de prensa, indica que Cuba se encuentra entre los 10 países con mayor censura en el mundo señalando que el gobierno cubano controla y posee todos los medios y restringe el acceso a internet; refiere algunas características que definen a los países que conforman su lista entre las que destacan: el control arbitrario sobre la cobertura informática mediante combinación de propaganda, fuerza bruta, tecnología sofisticada; así como también nos muestra las pautas que surgen del análisis en mención, y entre las que se destacan:

- Control total: los medios escritos y electrónicos en los 10 países bajo fuerte control o influencia del estado.

- Gobiernos unipersonales: la mayoría de los países en la lista de la CPJ son gobernados por un hombre que ha permanecido en el poder manipulando los medios y haciendo fraude en cuanto elección se celebra. Los medios fomentan un culto a la personalidad.

[18] ajudicuba.wordpress.com/2011/12/08/redes-sociales-o-no/ Página de Internet consultada el seis de abril del 2012

- Uso de la gran mentira: la gran mayoría de las noticias son positivas a su gobierno, es decir, no hay hambre, no hay pobreza y los gobernados simpatizan con sus gobernantes y están conformes bajo su dirección.

- Tolerancia cero para la cobertura negativa: los periodistas son atacados o bloqueados cuando emiten reportajes mostrando la realidad de su país.

- Cínica indiferencia por el bienestar de la gente: los gobiernos suprimen las noticias de los peligros y de las dificultades de los ciudadanos.

Pero más que sólo enumerar algunas características, nos muestra la realidad de la censura en Cuba, destacando que, los medios nacionales son controlados por el Partido Comunista que reconoce la libertad de prensa “Sólo en acuerdo con los objetivos de la sociedad socialista.

Los proveedores de servicios se ven obligados a bloquear cualquier contenido objetable; todos los periodistas independientes y blogueros trabajan en páginas web hospedadas en el exterior y actualizadas por medio de las embajadas o costosas conexiones de hoteles.

Por otro lado, la organización de defensa de los Derechos Humanos, alerta que países como Siria, China o Cuba han extendido su censura de la internet a través del bloqueo de los motores de búsqueda, el encarecimiento del precio de internet, la tortura a activistas para conseguir sus contraseñas de “Facebook”, “Twitter”, o la aprobación de leyes para controlar lo que se publica en la red.

3.3.7.2. Normatividad Argentina

3.3.7.2.1. Código Penal Argentino (Ley 26.388)

En Argentina se protegen bienes jurídicos en materia informática, distintos a los establecidos en la República de Cuba, analizaremos algunos preceptos jurídicos que aluden a dicho tema y la forma en que lo sancionan las autoridades del referido país. En este sentido la ley a analizar será, el Código Penal Argentino y en específico la Ley 26.388 la cual hace referencia a la modificación emitida en junio de 2008 por las autoridades legislativas de dicho país y en la cual se sustituyen y/o modifican algunos numerales del ordenamiento en comento, entre los que sobresalen por ser parte del tema en análisis (delitos informáticos) siguientes:

"ARTÍCULO 4º — Sustituyese el artículo 153 del Código Penal, por el siguiente: Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

ARTICULO 6º — Sustituyese el artículo 155 del Código Penal, por el siguiente: Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

ARTICULO 9º — Incorporase como inciso 16 del artículo 173 del Código Penal, el siguiente: Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

En los artículos anteriores de la legislación argentina podemos observar y resumir que los bienes jurídicos tutelados serán:

1. Las comunicaciones y la divulgación de las mismas en cuanto hace a medios escritos y electrónicos;

2. El fraude realizado por cualquier técnica de manipulación informática.”

En cuanto al punto número 1 podemos percatarnos de que se resguarda la privacidad de las comunicaciones y sanciona de manera pecuniaria y con prisión dependiendo la gravedad del delito cometido, ya que cuando la información que se deba resguardar sea de carácter restringido y se haga pública la penalidad por

dicho acto será sancionada con una cantidad pecuniaria mayor; pero cuando hablamos de interceptar comunicación y posteriormente comunicarla a un tercero o hacerla pública, la sanción será de prisión y, aumentará al doble.

Aludiendo al punto 2, podemos mencionar que lo que se sanciona es la manipulación que se hace mediante o a través de sistemas informáticos para producir con ello un fraude a otra persona alterando el normal funcionamiento de su sistema o la transmisión de los datos en éste contenidos.

3.3.7.2.2. Proyecto de Ley Incorporando el art. 138 bis al Código Penal, por el cual se tipifica el delito de Suplantación de Identidad Digital.

En Argentina se encuentra un nuevo proyecto de Ley que llego al senado el día 15 de mayo del año en curso, fue realizado por 2 senadoras, una de ellas la ingeniera María de los Ángeles Higonet, quien destacó que:

"Hay un fenómeno donde se vivencia que la identidad física de las personas se traslada al mundo virtual. Entonces, es necesario entenderla como un bien jurídico a proteger, dado que cualquier daño realizado hacia este aspecto digital de la personalidad, tiene sus efectos sobre toda la persona. Por ello, se consideró el merecimiento de la tutela más atenta por parte del Estado".[19]

Rescatando algunas palabras de la ingeniera: la identidad física de las personas se traslada al mundo virtual, he ahí la importancia y la inquietud que debería de manejar cada país para poder dar una mayor cobertura en la protección de usuarios de internet, y tomando como referencia a la suplantación de identidad lo podríamos trasladar al contexto especifico, llamado redes sociales, abordadas anteriormente en el capítulo 2° del presente trabajo.

[19] www.comercioyjusticia.com.ar/2012/06/01/quienes-roben-identidad-en-internet-podrian-ir-a-prision/ Página de Internet consultada el doce de abril del 2012

No desviándonos del apartado en análisis, abordemos las características del tipo penal que se requiere adherir al ordenamiento penal argentino y su importancia, el cual a la letra dice lo siguiente:

"Proyecto de Ley para penalizar la Suplantación de Identidad Digital. El mismo ocurre cuando una parte adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la intención de cometer fraude u otros delitos relacionados, sea por Internet o por cualquier medio electrónico"[20].

La suplantación se dará entonces, cuando mis datos personales sean utilizados con fines delictivos y sea a través de cualquier medio electrónico o por internet. Dándonos como características las siguientes:

1. Utilización de mis datos/información personal
2. Sin autorización/ no exista voluntad para ello
3. Para cometer fraude u otro delito
4. Se lleve a cabo por internet u otros medios electrónicos

El bien jurídico tutela en este proyecto de ley será la integridad de la persona cuando es robada su identidad en medios informáticos, y tomando en cuenta que no sólo daña la moral de la persona si no que puede derivar en conductas delictivas sancionadas por la ley penal.

Manifestó la senadora María de los Ángeles Higonet Con respecto a la situación nacional, la normativa precisa que "actualmente, la suplantación de identidad digital se encuentra en amplio crecimiento en Argentina dada su falta de regulación legal. El marcado aumento de bases de datos ilegales con información privada sobre las personas permite a los delincuentes acceder con relativa

[20] www.segu-info.com.ar/cruzada-robo-identidad Página de Internet consultada el doce de abril del 2012

facilidad a esos detalles de información, que son materia prima para facilitar la usurpación de una identidad con la cual el autor encontrará allanado el camino para poder realizar sus conductas maliciosas"[21].

Es de suma importancia hacer hincapié en dicho proyecto de ley, debido a que en la actualidad todos estamos inmersos en la internet y nuestros datos personales que son aquellos que nos hacen únicos ante los demás, corran grandes riesgos de ser aprehendidos y utilizados por otros, y peor aún, con fines que lesionen a la sociedad y que por consiguiente repercutirán en una responsabilidad que se remitirá al o la titular de dichos datos, sin tener la certeza de que sea ésta la que incurrió o llevo a cabo dicha conducta.

3.3.7.2.3. Proyecto de Ley Incorporando al Código Penal el Delito de la Práctica del Grooming.

Las mismas senadoras que formularon la iniciativa acerca de la suplantación digital, elaboraron con anterioridad un proyecto de ley dirigido a la incorporación al código penal de un artículo que hiciera referencia al engaño realizado por parte de una persona adulta hacia un menor haciéndose pasar el primero por un menor para ganarse la confianza del otro y posteriormente inducirlo a realizar actos de contenido sexual, a través de una red social, o de la internet, medios electrónicos.

Así mismo en fecha 08 de septiembre de 2011 fue ingresada al senado dicha propuesta realizada por la senadora María de los Ángeles Higonet y el senador Carlos Alberto Verna, quienes ven en la irrupción de las nuevas tecnologías y el acceso masivo a la red internet una proliferación de la tendencia a ser utilizadas para cometer a través de ellas conductas delictivas, entre las

[21] Diariojudicial.com/noticias/No-sos-vos-soy-yo-20120529-0008.html Página de Internet consultada el trece de abril del 2012

cuales se encuentran el “Grooming” , siendo necesario que sea tipificada y penada en el código penal; la inquietud de la y el senador, nace debido a que su país de origen, Argentina, no se ve exento de que se cometa dicho delito con tintes sexuales que posteriormente deriva en otras conductas delictivas, siendo que además países como Reino Unido, Escocia, Australia, Estados Unidos, Singapur, Alemania y hasta hace poco, también España, lo contemplan en sus legislación debido a la gravedad que implica dicha conducta .

Por tal motivo es necesaria, dicen la y el senador, tipificar dicha conducta en el código penal, y proponen que:

“Artículo 1°: agréguese como artículo 128 bis del Código Penal el siguiente:

Artículo 128 bis: será reprimido con prisión de seis (6) meses a cuatro (4) años el que por intermedio de identidad falsa, mediante la utilización de cualquier medio electrónico, cometiere acciones destinadas a ejercer influencia sobre un menor para que este realice, a través del mismo medio, actividades sexuales explicitas o actos con connotación sexual.

La pena será de dos (2) años a seis (6) años cuando el material pornográfico obtenido a través de la conducta anterior sea utilizado para obligar al mejor a hacer o no hacer algo en contra de si voluntad.”

Entre los fundamentos expuestos ante el senado podemos hacer mención de algunos factores que, a consideración de la Ley y el senador, son los que contribuyen a que se lleve a cabo dicha conducta entre la población:

- ✓ Las cámaras fotográficas digitales;
- ✓ Celulares con cámara incorporada;
- ✓ Mensajes de texto;
- ✓ Salas de chat

- ✓ Sitios de redes sociales como Facebook, MySpace, Hi5, Messenger, Twitter, etc.

Lo anterior como medios de acceso a comunidades virtuales en donde no existe claridad respecto a la identidad de las personas con quienes conversan o se relacionan los menores; y es donde surge la más grave problemática, debido a que en la convivencia sin restricciones que se lleva a cabo a través de dichos medios/redes digitales, podemos encontrar, sin saber cómo identificarlos a primera vista, a posibles víctimas y victimarios y por si fuera poco, se genera un ambiente propicio para el anonimato y el encubrimiento de los abusadores.

Se desglosan, en la misma fundamentación, las etapas por las cuales se lleva a cabo la conducta delictiva, “Grooming”:

1. Etapa: generar un lazo de amistad con un menor fingiendo ser un niño o una niña.
2. Etapa: obtener información clave del menor víctima de grooming.
3. Etapa: mediante seducción, conseguir que el menor frente a la webcam del computador se desvista, se masturbe o realice otro tipo de expresiones de connotación sexual.
4. Etapa: inicio del ciber-acoso, dando inicio a la fase de extorsión de la víctima, con el objeto de obtener material pornográfico, o bien el contacto físico con el menor para concretar un abuso sexual.

Como podemos observar es un grave problema que desencadena más de una conducta ilícita que es ayudada por la falta de regulación y prevención debido a la falta de educación tecnológica que debería de llevarse a cabo sobre todo en el sector más vulnerable, siendo éste, los menores de edad, que al adentrarse a tempranas edades a las redes sociales y/o espacios virtuales, son presa fácil de

gente sin escrúpulos que aprovechándose de la ignorancia y falta de experiencia de sus víctimas logran su cometido.

Después de desglosar y analizar el proyecto de ley emitido por la y el senador, podemos concluir que la inquietud por regular la grave problemática existente derivada de las múltiples características que identifica a la internet, ya que una de ellas sería el anonimato mediante el cual personas mayores de edad se hacen pasar por niños o niñas y lograr fomentar un lazo entre su víctima para posteriormente inducirla a realizar conductas obscenas a través de los medios electrónicos iniciando así un ciber- acoso que dará como resultado próximo, obtener material pornográfico de la víctima y que en algún momento puede llegar a difundirse a través de diversos medios; no es un problema que ataña sólo a un país y es donde podemos aludir a una segunda característica de la internet, la universalidad y extraterritorialidad, por tanto es importante que cada país logre fomentar la cultura de la prevención y sanción de conductas como la mencionada.

Como podemos darnos cuenta hay una marca diferencia entre lo que se protege en un país, Cuba, y los tutelados en otro, Argentina, que perteneciendo a un mismo continente muestran marcadas diferencias jurídico-protectoras en cuanto hace a los delitos cometidos con o a través de medios informáticos.

3.3.7.3. Chile y su Marco Legal.

3.3.7.3.1. Ley Relativa a Delitos Informáticos (Ley No.:19223).

“Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.”

Como podemos observar, en los artículos mencionados en la referida ley chilena, lo que tutela son las irrupciones en medios o sistemas informáticos con el fin de dañarlos o alterarlos, así como también protege la información que de cierta manera puede ser interceptada por persona ajena a la titular de ésta, pero fuera de eso no tutela bienes jurídicos referentes a acciones que pueden llegarse a cometer a través de los medios informáticos que tengan repercusiones más graves en la personalidad de un usuario, como fue el caso expuesto en la ley argentina.

Básicamente esta ley se enfoca a sancionar aquellas conductas que se puedan hacer en medios informáticos, es decir un daño material involucrando las

conductas que pueden realizar las personas en un medio electrónico, pero no así, las que llegaran a cometerse a través de los mismos.

3.3.7.4. Convenios Internacionales con Referencia a la Protección en los Medios Electrónicos.

3.3.7.4.1. Decisión número 276/1999 del Parlamento Europeo y del Consejo de 25 de enero de 1999.

El Parlamento Europeo y El Consejo de la Unión Europea emiten la decisión número 276/1999 en la que se enfocan en la problemática existente por el mal uso de la internet y en la lucha contra los contenidos ilícitos y nocivos en las redes mundiales.

Así después de analizar las problemáticas existentes en Europa en lo concerniente a contenidos ilícitos en la red, se llegó a la conclusión de que era necesario aplicar un plan de acción que tendría como objetivo propiciar una mayor seguridad en la utilización de internet y fomentar a nivel europeo la creación de un entorno favorable para el desarrollo de la industria vinculada a internet, lo anterior se encuentra plasmado en el artículo 2 de dicho documento.

Dicho plan de acción se llevó a cabo en un periodo de 4 años, abarcando desde su creación 1999 hasta diciembre de 2002, para poder llegar a cumplir con el objetivo establecido en el numeral 2 del documento en mención, se llevaron a cabo una serie de acciones entre las que destacan las siguientes:

Artículo 3:

- “Fomentar la autorregulación del sector y los mecanismos de supervisión de los contenidos (por ejemplo, los relativos a contenidos tales como la pornografía infantil o aquellos que inciten al odio por motivos de raza, sexo, religión, nacionalidad u origen étnico).

- Alentar al sector a ofrecer medios de filtro y sistemas de clasificación que permitan a padres y profesores seleccionar los contenidos apropiados para la educación de los menores a su cargo, y a los adultos decidir a qué contenidos lícitos desean tener acceso, y que tengan en cuenta la diversidad cultural y lingüística.

- Mejorar entre los usuarios el conocimiento de los servicios ofrecidos por el sector, especialmente entre padres, educadores y menores, para que puedan entender y aprovechar mejor las oportunidades que ofrece Internet.

- llevar a cabo medidas de apoyo como la evaluación de las implicaciones jurídicas.

- Realizar actividades para fomentar la cooperación internacional de los campos mencionados."

Algunas de las líneas de actuación que se implementaron con esta decisión fueron las siguientes:

- En la línea de actuación 1: encontramos la creación de una red de líneas directas, es decir una red europea de centros que permita a los usuarios notificar contenido que hayan encontrado al utilizar Internet y que a su juicio sean ilícitos para de esta manera, restringir su circulación. En este sentido, se deberán de respetar las diferencias existentes entre los diversos ordenamientos jurídicos y culturas nacionales.

- Línea de actuación 2: elaboración de sistemas de filtro y clasificación, cuando se trate de temas como la violencia o la sexualidad, se deberá de llevar a cabo un filtro de lo que se podrá o no mostrar como contenido en la red.

- Línea de actuación 3: fomento de las actividades de sensibilización, las actividades de sensibilización contribuyen a aumentar la confianza de padres y profesores en la utilización más segura de Internet por los menores. Dicha línea de acción será necesaria para poder implementar la 1 y 2 mencionadas, ya que sólo se podrán llevar a cabo las políticas si los usuarios presentes y futuros tienen conocimiento de ello. Entre las actividades de sensibilización que se podrán llevar a cabo están, talleres, preparación de material específico impresos y multimedios y su difusión dirigido a profesores.

- Línea de actuación 4: medidas de apoyo, evaluación de las repercusiones jurídicas, en esta línea se toma en consideración el hecho de que internet funciona a escala mundial y que las leyes se aplican en un ámbito territorial nacional, y es donde surge una problemática marcada en cuanto hace al conflicto jurídico que se pueda llegar a propiciar cuando se tenga que aplicar una ley específica en la coalición de un acto delictivo.

Debido a la alarmante preocupación imperante en países europeos, éstos se dieron a la tarea de organizar un plan de acción que llevaron a cabo durante 4 años y que fue posteriormente evaluado para ver si cumplió o no con las metas establecidas.

Es interesante como un país se dio a la tarea de tomar medidas autor regulatorias con respecto a restringir, clasificar y filtrar contenidos que puedan ser dañinos a la sociedad, pero sobre todo antes de llevar a cabo dicha acción, se fomentó la cultura de la prevención y el conocimiento por medio de talleres, difusión de material, etc., para dar un mayor conocimiento de lo que implican las conductas delictivas llevadas a cabo a través de medios informáticos.

3.3.7.4.2. Protocolo adicional al Convenio sobre ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.

Dicho protocolo fue emitido por el mismo consejo europeo que, preocupado por el riesgo de la mala utilización o la utilización abusiva de los sistemas informáticos para difundir propaganda racista o xenófoba, y conscientes de la necesidad de garantizar un equilibrio idóneo entre la libertad de expresión y una lucha eficaz contra los actos de índole racista y xenófoba, han convenido en que:

Se emite el presente protocolo con la finalidad de tipificar los actos de índole racista y xenófoba cometidos mediante sistemas informáticos; según el artículo 2 de dicho protocolo nos define que se deberá entender por material racista o xenófobo:

"Todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de la raza, el color, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores"[22].

No estarán permitidas acciones como las siguientes, por entrar en el tipo penal que se menciona en dicho protocolo:

"Artículo 3: difusión de material racista y xenófobo mediante sistemas informáticos, es decir estará tipificado como delito el hecho de difundir o poner a disposición del público o de otro material racista y xenófobo por medio de un sistema informático.

[22] www.gdt.guardiacivil.es/webgdt/media/Legislacion/Protocolo_adicional_convencion_cibercrimen.pdf Página de Internet consultada el veinte de abril del 2012

Artículo 4: las amenazas con motivación racista y xenófoba, amenazar por medio de un sistema informático a personas por razón de su pertenencia a un grupo caracterizado por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores.

Artículo 5: insultos con motivación racista y xenófoba, insultar en público, por medio de un sistema informático a un grupo que se caracterice por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para ello.

Artículo 6: negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad, es decir, difundir o poner a disposición del público por medio de un sistema informático, material que niegue, minimice burdamente, apruebe o justifique actos constitutivos de genocidio o crímenes contra la humanidad.”

En este protocolo se trata de establecer como tipo penal el hecho de que se difunda, amenace, insulte o minimice a una persona por razón de sus características físicas, ideológicas o culturales, tratando de resguardar como bien jurídico tutelado la integridad de la persona, y también teniendo en cuenta esa balanza que entre la libertad de expresión y el respeto hacia las personas, tomando en cuenta que en la internet sea el escenario a través del cual se lleven a cabo dichas conductas.

3.3.7.4.3. Convenio sobre la ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

Los Estados miembros del Consejo de Europa y los demás Estados signatarios, preocupados por el riesgo de que las redes informáticas y la

información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes, han convenido adoptar medidas a nivel nacional en contra de la ciberdelincuencia.

Así, en el titulo 2 de dicho convenio, se establecen y desglosa los tipos penales que serán castigados como delitos informáticos, los cuales son los siguientes:

“Artículo 7: falsificación informática; es la deliberada e ilegítima, introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados para efectos legales como si se tratara de datos auténticos.

Artículo 8: fraude informático; son actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o supresión de datos informáticos; así como también cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Artículo 9: delitos relacionados con la pornografía infantil, la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático; la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático; la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona; la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos. Para efectos de lo anterior, se entenderá por pornografía infantil: todo material que contenga la representación visual de un menor comportándose de una forma sexualmente explicita, una persona que parezca un menor

comportándose de una forma sexualmente explicita. Será considerado como menor, toda persona menor de dieciocho años.”

Como podemos observar en este convenio se habla tanto de delitos cometidos en medios informáticos, como a través de ellos, y se toma en cuenta la difusión, la posesión y adquisición de material denominado pornografía infantil, siendo éste un delito que traspasa el contexto virtual afectando directamente la personalidad del menor, ya que no sólo implicaría una cuestión de honor, sino también una serie de conflictos emocionales.

Los Estados miembros del Consejo Europeo y que ratificaron el convenio son:

1. Albania
2. Alemania
3. Armenia
4. Azerbaiyán
5. Bosnia y Herzegovina
6. Bulgaria
7. Croacia
8. Chipre
9. Dinamarca
10. Eslovaquia
11. Eslovenia
12. España
13. Estados Unidos
14. Estonia
15. Finlandia
16. Francia
17. Hungría
18. Islandia
19. Italia
20. Letonia
21. Lituania
22. Macedonia, Antigua República
23. Montenegro
24. Países Bajos
25. Portugal
26. República de Moldavia
27. Rumania
28. Serbia
29. Ucrania

3.4. MÉXICO: SU PERSPECTIVA ANTE LOS DELITOS CIBERNÉTICOS.

En nuestro país es una lástima que a pesar de que en muchos países se haya regulado o hayan hecho el intento por hacerlo y que nuestros legisladores no han podido dar solución a este grave problema, se les reprocha directamente a ellos puesto que ellos deben de observar la gran efervescencia nacional por el escandaloso manejo de enormes bases de datos, como la electoral a nivel nacional, la de personas con licencia de conducir en la capital del país, la del registro vehicular, las novedosas redes sociales y sobre todo el auge de los blogs y videos en Youtube solo por mencionar algunas. De esta manera, ni en la Constitución Federal de 1917, en los artículos 6, 14 y 16 relativos al derecho a la información o a privilegios personales sobre la familia, papeles, posesiones, etc., o las disposiciones penales sobre violación de correspondencia, revelación de secretos o incluso las referidas al uso ilícito de las computadoras o el daño moral en materia civil ni la ley de información estadística y geográfica y su reglamento, ni el propio código federal de instituciones y procedimientos electorales o la aprobada Ley Federal De Trasparencia Y Acceso A La Información Pública Gubernamental u otros tantos ordenamientos jurídicos, son suficientes para regular de manera adecuada este delicado problema. México necesita una ley y una autoridad que ponga fin al alarmante desorden imperante en la materia de datos personales en la red. Nuestras autoridades deben voltear a ver lo que ocurre y que se preocupen de verdad, hagan la legislación que regule a Internet y así como se crean instituciones de vigilancia en otras materias, creen una que le dé mayor solidez, fuerza y vigilancia adecuada a esa ley.

3.4.1. Códigos de Estados que han regulado conductas ilícitas en Internet.

Para poder exponer la situación en la que se encuentra nuestro país de una manera más comprensible pasaremos a enlistar los Estados que contemplan

como tipos penales a las conductas realizadas en Internet y señalaremos brevemente lo que han regulado dentro de sus respectivos Códigos Penales.

3.4.1.1. Código Penal de Sinaloa.

A pesar de que en nuestro país no cuenta con una legislación a nivel federal que realmente proteja a sus ciudadanos, algunas Entidades Federativas han intentado hacer algo frente al problema del control de datos en Internet, y en este supuesto un claro ejemplo es el del Estado de Sinaloa, Entidad en la que en el año de 1992 su Congreso local legisló sobre los delitos informáticos incluyéndolos en el Código Penal para el Estado de Sinaloa, siendo el primer órgano legislativo del país; así hasta el día de hoy se establece en el artículo 217 que Comete delito informático, la persona que dolosamente y sin derecho:

I. “Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o
II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.”

3.4.1.2. Código Penal de Aguascalientes.

Tras haber regulado de una manera muy exitosa, efectiva y eficaz, en su momento, las demás Entidades Federativas siguieron el ejemplo de Sinaloa buscando el contemplar los delitos informáticos dentro de sus códigos penales.

En el caso de Aguascalientes se contempla actualmente diversas conductas, entre ellas vemos que en su Código cuando habla de delitos en Contra de la Confidencialidad, abordando la Revelación de Secretos, ya menciona los archivos informáticos personales, algo que en nuestra materia representa un avance en intento de regulación de Internet en este caso acerca de los documentos y demás datos privados; también en el artículo 220 de dicho Código referente a la Defraudación Fiscal habla acerca de los sistemas informáticos en el uso de las operaciones contables, fiscales o sociales, cabe señalar que actualmente ya no se pueden llevar facturas impresas como comprobantes fiscales ahora se deben de rendir cuentas por medio de facturación electrónica en Internet, así que este tipo penal de Aguascalientes resultó ser una muy adecuada medida legislativa. En este Código también se prevé un título de los Delitos Contra la Seguridad en los Medios Informáticos y Magnéticos, mismo en el que se contempla el delito de acceso sin autorización y el de daño informático, en los que puede apreciarse que fueron creados con la idea de poder castigar a los creadores de los virus en cuanto ataquen a los ciudadanos de Aguascalientes.

3.4.1.3. Código Penal del Estado de Baja California Norte.

En Baja California Norte actualmente en el título de los Delitos Contra la Inviolabilidad del Secreto y de los Sistemas y Equipos de Informática del Código Penal de esta Entidad se observan a los tipos penales, referentes, al de Revelación del Secreto, el Acceso Ilícito a Sistemas y Equipos de Informática, a su vez en el título de los Delitos Contra el Libre Desarrollo de la Personalidad, habla de la Pornografía y Turismo Sexual de Personas Menores de Dieciocho Años de Edad o de Quienes no tienen la Capacidad para Comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo en el que se señala como medios de realización las redes públicas o privadas de telecomunicaciones, los sistemas de cómputo y demás medios electrónicos, y en el caso del tipo penal de Encubrimiento por favorecimiento se prevé que dicha conducta sea realizada

por periodistas, reporteros o personal y que lo hagan inclusive a través de medios electrónicos de comunicación.

3.4.1.4. Código Penal del Estado de Baja California Sur.

En Baja California Sur solo se tienen legislados tres artículos dentro del Código Penal que hablan acerca de la Violación de Correspondencia y otras Comunicaciones Privadas en el que son demasiado breves.

3.4.1.5. Código Penal del Estado de Campeche.

En el Código Penal del Estado de Campeche se encuentran tipificados los delitos de Falsedad Falsificación de sellos, llaves, punzones y marcas y el de Daño en propiedad ajena, en el primero se protegen las contraseñas que se usan en la red y en el segundo busca la protección de los datos y archivos.

3.4.1.6. Código Penal del Estado de Chiapas.

En el Estado de Chiapas se han previsto como conductas ilícitas dentro del Código Penal en los Delitos Contra el Honor el publicarse la sentencia en medios electrónicos, en los Delitos en Contra de las Personas en su Patrimonio se ha tipificado el fraude a través de medios electrónicos, en los Delitos contra la Moral y la Dignidad de las Personas, cuando habla de Corrupción de Menores e Incapaces señala que pueda realizarse esta conducta de igual forma a través de medios electrónicos, en el título de Falsedad se regula y sanciona la alteración de los medios de identificación electrónicos y por último en el título de los Delitos de Revelación de Secretos y de Acceso Ilícito a Sistemas y Equipos de Informática también prevé el Acceso Ilícito a Sistemas de Informática.

3.4.1.7. Código Penal del Estado de Chihuahua.

En el Código Penal de Chihuahua se contempla en el delito de Pornografía con Personas Menores de Edad o que no tienen la capacidad para Comprender el Significado del Hecho el que pueda llevarse a cabo a través de medios electrónicos, el delito de Robo en el que se señala el robo de archivos electrónicos, en el de Daños también se observa detallado que la conducta pueda ser realizada a un sistema o equipo de cómputo, en el de Violación de correspondencia se enlista la correspondencia o comunicación registrada, guardada o archivada en equipos o sistemas de cómputo y en el delito de Falsificación o alteración y uso indebido de documentos se menciona que pueda ser realizado delito a través de cualquier medio técnico del que se desprende que los electrónicos también pueden.

3.4.1.8. Código Penal del Estado de Coahuila.

Dentro del Código Penal de Coahuila existe el Capítulo de Delitos Contra la Seguridad en los Medios Informáticos en el que cerca de 6 artículos tratan de contemplar las conductas que atentan en contra de la seguridad en Internet.

3.4.1.9. Código Penal del Estado de Colima.

En Colima tenemos que en su Código Penal desde el artículo 10 señala que el exhibicionismo puede ser también mediante medios y anuncios electrónicos y en delito de Corrupción de menores de igual forma lo menciona y en el tipo penal de Delitos ambientales en la descripción de este dice que se considera delito ambiental si alteran el equipo o programas de cómputo para la verificación de automotores.

3.4.1.10. Código Penal del Estado de Durango.

Durango ha contemplado varias acciones en su Código Penal entre las que se señalan la falsificación, detención, posesión y alteración de tarjetas y el uso de equipos electrónicos para realizar estos fines, de igual forma la falsificación u obtención ilícita de contraseñas y el alterar al Registro Estatal de Electores entre otros, que se puede realizar a través de cualquier medio entre los que se podrían señalar los electrónicos.

3.4.1.11. Código Penal del Estado de México.

El Estado de México cuenta con el título de Delitos Informáticos dentro de su Código Penal, el que tiene el subtítulo de Delitos Contra la Libertad y Seguridad, y también contempla el Delito contra el Proceso Electoral.

3.4.1.12. Código Penal del Estado de Guanajuato.

En Guanajuato se tiene en el Código Penal el tipo de Violación de Correspondencia en el que se señala que puede ser realizado a través de equipo de cómputo o incluso con objeto de la información contenida en estos.

3.4.1.13. Código Penal del Estado de Guerrero.

Guerrero tiene un código muy peculiar en cuanto a la materia que nos ocupa, y un ejemplo es el hecho de que en el tipo penal de robo contenido en el artículo 165 fracción dos señala a Internet y los programas computarizados tal y como lo vemos a continuación, quien aprovechando energía eléctrica, algún fluido, programas computarizados, señales televisivas o de Internet, sin consentimiento de la persona que legalmente pueda disponer y autorizar aquéllas. De igual

manera maneja el uso de computadoras en el delito de Lenocinio y Pornografía y por último el uso de estos medios electrónicos para realizar los Delitos Electorales.

3.4.1.14. Código Penal del Estado de Jalisco.

En el Código Penal de Jalisco encontramos que hay delitos como el de Pornografía Infantil y Secuestro que en el caso del primero señala que puede ser por medio de este y en el segundo que se requiera de cajeros electrónicos, además hay otros delitos como el de la Obtención Ilícita de Información Electrónica y el de Falsificación de Medios Electrónicos o Magnéticos ambos tipificados para proteger a los usuarios de la red de redes.

3.4.1.15. Código Penal del Estado de Michoacán.

En Michoacán de igual forma en el Código Penal se señala dentro los delitos de Pornografía y turismo sexual de personas menores de edad o de personas que no tiene capacidad para comprender el significado del hecho y el de Falsificación de Documentos y Uso de Documentos Falsos, que puedan realizarse a través de Internet y los medios electrónicos.

3.4.1.16. Código Penal del Estado de Nuevo León.

Una característica muy particular aparece en el Código Penal del Estado de Nuevo León puesto que en su artículo 352 bis señala que se aumentará hasta la mitad de la pena a imponer por los delitos que resultaren, cuando se efectúen mediante la utilización de la televisión, radio, prensa escrita o Internet.

A su vez en el delito de Corrupción de Menores cuando habla de la reproducción de imágenes señala textualmente la reproducción de imágenes en medios magnéticos y electrónicos, y en el caso del tipo penal de Robo de igual

forma a otras Entidades Federativas hace alusión al robo de datos de computadoras.

3.4.1.17. Código Penal del Estado de Oaxaca.

En el Código Penal de Oaxaca se señala en el delito de Abuso Sexual que se configura tal ilícito aun cuando las imágenes a las que se le obligue a una persona a ver se encuentren en los multicitados medios electrónicos.

En el tipo penal de Secuestro de igual forma que en otros Estados se señala la obtención de lucro a través de tarjetas de crédito, bancarias, medios electrónicos e informáticos entre otros.

3.4.1.18. Código de Defensa Social para el Estado Libre y Soberano de Puebla.

En Puebla los legisladores han reformado el artículo 219 del Código de Defensa Social para el Estado Libre y Soberano de Puebla que habla de la Corrupción y Pornografía de Menores e Incapaces o Personas que no pudieren resistir, introduciendo en la fracción primera de este que las imágenes o representaciones de exhibicionismo sexual sean por medios electrónicos o producidos por el avance tecnológico. De igual forma en el tipo penal de Falsificación de Acciones, Obligaciones y Otros Documentos de Crédito Público señala en sus fracciones la adquisición, copia o falsificación de los medios de identificación electrónica, cintas o dispositivos magnéticos de tarjetas y el acceso indebido a equipos y sistemas de cómputo o electromagnéticos.

3.4.1.19. Código Penal del Estado de Querétaro.

En el Código Penal de Querétaro el tipo penal de Pornografía con Menores o Incapaces señala la reproducción de las imágenes que se obtengan con ese ilícito a través de medios impresos o electrónicos.

3.4.1.20. Código Penal para el Estado Libre y Soberano de Quintana Roo.

En Quintana Roo el tipo penal de Falsificación de Documentos y Uso de Documentos Falsos que se encuentra en su Código Penal enuncia la reproducción, copia o alteración de los medios de identificación electrónica, cintas o dispositivos magnéticos de documentos y el acceso indebido a equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo, entre otras. En el mismo Código el delito de Pornografía Infantil señala la reproducción de imágenes y videos por medio de medios electrónicos.

3.4.1.21. Código Penal para el Estado de San Luis Potosí.

En este Código los Potosinos también han previsto que el tipo penal de Violación de Correspondencia pueda darse con el uso de las computadoras.

3.4.1.22. Código Penal para el Estado de Tabasco.

En Tabasco, el tipo penal de Violación de la Comunicación Privada está directamente dirigido a sancionar penalmente los ataques comunicación privada de terceras personas, a través de medios eléctricos o electrónicos. A su vez en el título de los Delitos Contra la Seguridad en los Medios Informáticos y Magnéticos, en el delito de Acceso Sin Autorización se prevé el que las personas accedan a

otras computadoras o sistemas con un fin dañino o de lucro sin la autorización necesaria o excediendo esta. De igual forma existe el tipo de Daño Informático en el que el nombre lleva inmerso a que se refiere, en el que la forma más común de esta sería a través de los virus informáticos.

En este Código Penal también se incluye la Falsificación Informática que es referente a lo que vendría siendo la piratería de software y la obtención de bases de datos y sistemas de computadoras sin licencias y/o autorizaciones.

3.4.1.23. Código Penal para el Estado de Tamaulipas.

En el Código Penal de Tamaulipas se señala de igual forma dentro del tipo penal de Robo, la obtención de datos de computadoras o el aprovechamiento o utilización de dichos datos sin autorización.

3.4.1.24. Código Penal para el Estado de Tlaxcala.

En Tlaxcala los legisladores han insertado en el Código Penal un artículo que contemple los Delitos Cometidos por Medios Electrónicos e Informáticos, el cual tiene la idea de regular la Corrupción de Menores a través de Medios Electrónicos y en este hacemos una breve crítica en cuanto a que el nombre no fue el más adecuado para dicho tipo penal pues solo se refiere a la corrupción de un menor como tal y no abarca las demás actuaciones ilícitas que se presentan hoy en día.

3.4.1.25. Código Penal de Veracruz.

En el caso de Veracruz como en la mayoría de las Entidades Federativas, realmente es muy pobre lo que encontramos acerca de los delitos informáticos en el aspecto de que en su Código Penal solo contempla un artículo el cual es aparte

de pequeño, muy inespecífico, y para mayor ilustración plasmaremos el numeral 181 del Código Penal para el Estado Libre y Soberano de Veracruz de Ignacio de la Llave referente al Delito Informático:

"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."

Si bien como se ha señalado Sinaloa fue pionero y muy acertado en su momento, pero desgraciadamente esto ya quedo obsoleto y requiere más que una reforma, una creación de varios tipos que regulen las nuevas conductas que ha traído la gran evolución de Internet.

3.4.1.26. Código Penal de Yucatán.

En Yucatán ha pasado lo mismo, en su Código Penal se contempla dentro del tipo penal de Corrupción de Menores e Incapaces, Trata de Menores y Pornografía Infantil el que se realicen estas conductas a través o en apoyo de los medios electrónicos.

3.4.1.27. Código Penal de Zacatecas.

En esta Entidad del País se han señalado conductas como el que a través de Internet se induzca o facilite el acceso de un menor o incapaz a drogas, alcohol y demás estupefacientes, o que se le permita el acceso o se induzca al acceso de

páginas para mayores de edad, también en el delito de Corrupción de Menores señala lo mismo que otros Estados en cuanto al uso medios electrónicos en este tipo penal, este Código Penal también se contemplan las amenazas a través de los medios electrónicos, así como el daño a sistemas informáticos y robo de información y por último el atacar el sistema electrónico electoral.

3.4.1.28. Código Penal del Distrito Federal.

En la capital del país también los legisladores decidieron incluir en tipos penales existentes el uso de Internet y medios electrónicos para la comisión del delito de Pornografía, el Fraude en cuanto a creación de sistemas electrónicos o programas de informática con la finalidad de realizar operaciones en el sistema financiero y de igual forma en los Delitos Contra la Fe Pública en el que se prevé el uso de los sistemas informáticos para la comisión de este delito.

3.4.1.29. Código Penal Federal.

Tras haber hecho un breve recorrido por los Códigos de los Estados que contemplan o han intentado contemplar la comisión de delitos con el uso de la computadora, solo nos falta analizar lo que tenemos en el Código Penal Federal, es decir el que tendrá aplicación en toda la República en materia federal.

Este Código al igual que el de algunos Estados, señala la realización del delito de 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, a través del uso de sistemas de cómputo, medios electrónicos y redes de comunicaciones, además ha incluido un título que llama de la Revelación de secretos y acceso ilícito a sistemas y equipos de informática, en el que se contempla el Acceso ilícito a sistemas y equipos de informática que a grandes rasgos habla de la o las personas que sin

autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática, ya sea de datos de particulares, del Estado o de Instituciones Financieras entre otras. En este Código también se contempla dentro de los Delitos en Materia de Derechos de Autor la fabricación de dispositivos o sistemas con el fin de desactivar los dispositivos electrónicos de protección de un programa de computación.

En la reforma al código Penal Federal del 2012 se han incluido algunos tipos penales que son referentes a los delitos cibernéticos, entre los que destacan "La tipificación de delitos a la pornografía infantil, trata de personas, turismo sexual y corrupción de menores, duplicando la pena cuando para cometer tales perpetraciones se usan recursos informáticos.

Sanciones más severas a quienes empleen sistemas y medios informáticos en delitos como amenazas e ilícitos patrimoniales como extorsión y fraude, donde cabe el phishing, práctica de alta incidencia en México.

Penalizaciones en el caso de acceso e intervención ilícitas a medios y sistemas informáticos, robo de identidad y el uso indebido de dispositivos para tales fines, en caso de que tales actividades atenten contra sistemas informáticos del Estado, el sistema financiero nacional o cualquier institución o persona.

Y finalmente, penas específicas a quienes hagan mal uso de medios electrónicos del sistema financiero en delitos vinculados con el lavado de dinero y el encubrimiento de operaciones con recursos de procedencia ilícita." [23]

[23] www.informationweek.com.mx/analysis/reforman-codigo-penal-federal-para-castigar-mas-duramente-los-delitos-informaticos Página de Internet consultada el veintiocho de abril del 2012

Esta reforma si representa un gran avance en materia de delitos informáticos pero sigue siendo insuficiente al dejar muchísimas conductas sin sancionar como el sabotaje informático y el terrorismo en Internet a través de las redes sociales sobretodo.

CAPÍTULO IV
CONDUCTAS DE RELEVANCIA PARA EL DERECHO PENAL EN MATERIA DE INTERNET.

4.1 ¿QUÉ ES EL DELITO INFORMÁTICO?

Mucho se ha mencionado con anterioridad acerca de los Delitos Informáticos, pero no hemos entrado a fondo en dar una definición exacta de los también llamados cibernéticos. Ahora bien estos delitos son aquellas conductas criminales que los países han intentado incluir dentro de sus leyes penales para darles un carácter de tradicionales y comunes, tales como el fraude, falsificaciones, perjuicios, robo, estafa, sabotaje, terrorismo, etcétera, "…Sin embargo, debe destacarse que el uso de las computadoras ha propiciado, a su vez, la necesidad de regulación por parte del Derecho, para sancionar conductas como las señaladas." [24]

[24] NAVA GARCÉS, Alberto Enrique. *Análisis de los delitos informáticos*. Primera Edición. México. Porrúa. 2005. P. 18.

Julio Téllez al respecto define a los delitos informáticos como aquellas "…actitudes ilícitas que tiene a las computadoras como instrumento o fin," [25] desde un concepto atípico y como concepto típico como las "…conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin"[26].

4.1.1. Principales características de los Delitos Informáticos.

Los delitos cibernéticos o informáticos, tienen características peculiares, las cuales pasaremos a detallar a continuación.

1. "Son conductas criminales de cuello blanco, *white collar crimes*. En tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas"[27], es decir para llevar a cabo la comisión de un delito de esta índole se requiere de conocimientos técnicos o profesionales por parte del sujeto activo, además de la intención de realizarlos, ya que sin esta preparación no se podría realizar y por consecuente no existiría tal delito.

2. Otra característica es que "Son acciones ocupacionales en cuanto a que muchas veces se realizan cuando el sujeto está trabajando"[28], en este sentido las oficinas ya sea de empresas públicas o privadas son los principales contextos en los que se realizan dichas acciones.

3. "Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y

[25] TELLEZ VALDÉS, Julio. *Derecho Informático*. Cuarta Edición. México. McGraw Hill. 2009. p. 188.
[26] TELLEZ VALDÉS, Julio. Op. Cit.
[27] Ibídem.
[28] Ídem.

organizaciones del sistema tecnológico y económico”[29], esto porque obviamente en lugares que se requiere directamente el uso de computadoras, por ejemplos los bancos, es donde se presta para la realización de estas.

4. Muchas veces “Provocan serias pérdidas económicas, ya que casi siempre producen “beneficios” de más de cinco cifras a aquellos que las realizan”[30], puesto que las conductas más comunes son con tendencia a obtener lucro, dejando en segundo término las que se realicen con el simple fin de causar daños o afectar la imagen de alguien.

5. “Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física”[31], esta característica es la que ha hecho que hoy en día se hayan vuelto muy populares estas conductas, en cuanto a que para alguien que sabe de computadoras, le es muy fácil y rápida su comisión.

6. “Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional”[32], efectivamente la falta de regulación ha contribuido a que delitos de esta índole queden impunes puesto que aun cuando la voluntad del sujeto que sufre estas acciones sea la de presentar una denuncia, no se cuenta con leyes ni nacionales ni internacionales suficientes para castigar al o a los culpables.

[29] Ídem.
[30] Ídem.
[31] Ídem.
[32] Ídem.

7. “Son muy sofisticados y relativamente frecuentes en el ámbito militar”[33], puesto que la creación de Internet fue con fines militares, también la aparición de los delitos a través de la red de computadoras está estrechamente ligado, además de por otras razones, con ataques desde los de Naciones por poder hasta inclusive entre los civiles y sus gobernantes, como el recién llamado *Fenómeno Anonymous* que es “un movimiento internacional de ciberactivistas, formado por un número indeterminado de personas que reciben ese nombre porque no revelan su identidad”[34] que cuando no están conformes con alguna decisión del Gobierno, atacan las redes y páginas de las instituciones públicas con el fin de hacerse escuchar.

8. “Presentan grandes dificultades para su comprobación, por su carácter técnico”[35], esto es comprensible puesto que Internet es tan grande y existen millones de usuarios, páginas y blogs como se puedan ocurrir y para dar con la persona que se encuentra detrás del monitor, computadora o incluso cualquier otro aparato electrónico requiere de realizar un laborioso trabajo con el uso de rastreo de las IP y demás claves usadas para identificar una computadora.

9. “En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales.”[36] La verdad es que es mucho más alto el índice de conductas que se realizan con toda la intención de hacer el daño que las que ocurren de forma imprudencial puesto que como se ha mencionado estas no son

[33] Ídem.
[34] www.rtve.es/noticias/20120228/anonymous-quienes-son-como-actuan/438765.shtml
[35] TELLEZ VALDÉS, Julio. Op. Cit. Nota 26.
[36] Ibídem.

realizadas por cualquier persona y requieren de ciertas condiciones que no tienen todas las personas, sin embargo existe la probabilidad de algunas conductas si se efectúen culposamente.

10. "Ofrecen a los menores de edad facilidades para su comisión."[37] De acuerdo a estadísticas de la INEGI en el 2010 existían 32.8 millones de usuarios de Internet en México, de los cuales el 26.5% siendo la mayoría de personas en Internet son los jóvenes de 12 a 17 años y le siguen con el 23% los de 18 a 24 años, tomando también en consideración que solo el 12.3% de los usuarios de Internet tienen entre 35 y 44 años.

11. "Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional." INEGI también informó en Mayo del 2011 que la tasa de crecimiento "de usuarios de Internet mostrada en el periodo 2001-2010 es de 18.5 por ciento"[38]

Las personas que cometen este tipo de delitos vemos que entonces son en su mayoría jóvenes y que han dedicado tiempo para aprender a usar las computadoras o por cuestiones y facilidades en su trabajo caen en la tentación de cometer dichos ilícitos.

4.2. CLASIFICACIÓN DE LOS DELITOS CIBERNÉTICOS.

Ya que se ha establecido lo que son los delitos informáticos de una forma más a fondo pasaremos a hacer mención de cómo diversos autores los han

[37] Ídem.
[38] pueblaonline.com.mx/index.php?option=com_k2&view=item&id=12872:usuarios-de-internet-crecen-185-anualmente-inegi&Itemid=126 Página de Internet consultada el veintidós de abril del 2012.

clasificado, entre ellos como los ha catalogado la Organización de las Naciones Unidas.

4.2.1. Clasificación de Pablo A. Palazzi.

Este Profesor Jurista Argentino se ha especializado en Derecho Informático y ha realizado una clasificación de acuerdo con el bien jurídico tutelado:

Contenidos Ilegales en Internet;

Delitos contra la Intimidad;

Delitos contra la Seguridad Pública y las comunicaciones;

Delitos contra el Patrimonio; y

Falsificaciones Informáticas.

4.2.2. Clasificación de Correa.

Jurista Colombiano que retoma los trabajos de Uhlrich Sieber al clasificar a los delitos informáticos en categorías:

Acceso no Autorizado a sistemas de procesamiento de datos;

Espionaje informático;

Fraude por manipulaciones de un computador contra un sistema de procesamiento de datos;

Ofensas tradicionales en los negocios asistidos por computador;

Robo de servicios; y

Sabotaje informático.

"Esta clasificación no es genérica, más bien, determina las características de delitos en particular, ya que se refiere a conductas perfectamente definidas."[39]

[39] TELLEZ VALDÉS, Julio. Op. Cit. Nota 25. P. 27.

4.2.3. Clasificación de María de la Luz Lima.

Abogada mexicana, ella hace una clasificación de lo que denomina como delitos electrónicos, poniéndolos en tres categorías:

"1.- Los que utilizan la tecnología electrónica como método,

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

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

Como método.- Conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como medio.- Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo.

Como fin.- Conductas criminógenas dirigidas contra la entidad física del objeto o maquina electrónica o su material con objeto de dañarla."[40]

En esta el principal problema que se encuentra es que se crea un problema para diferenciar a método y medio, por lo que sería mejor si solo quedara en dos categorías que serían las de medios y fines.

4.2.4. Clasificación de Julio Téllez Valdés.

Este estudioso del Derecho Informático, hace su clasificación en base a dos criterios uno viendo a las computadoras como instrumento o medio y el otro como fin u objetivo.

[40] LIMA, María de la Luz citada por NAVA GARCÉS, Alberto Enrique. *Análisis de los delitos informáticos*. Primera Edición. México. Porrúa. 2005.

4.2.4.1. Como instrumento o medio.

Aquí podemos apreciar las conductas que tienen a las computadoras como medio, método o símbolo en la realización del delito. Por citar algunos ejemplos:

a) "Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
b) Variación de los activos y pasivos en la situación contable de las empresas.
c) Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).
d) “Robo” de tiempo de computadora.
e) Lectura, sustracción o copiado de información confidencial.
f) Modificación de datos tanto en la entrada como en la salida.
g) Aprovechamiento indebido o violación de un código para penetrar a un sistema con instrucciones inapropiadas (esto se conoce en el medio como *método del caballo de Troya*).
h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como *técnica de salami*.
i) Uso no autorizado de programas de cómputo.
j) Inclusión de instrucciones que provocan “interrupciones” en la lógica interna de los programas, a fin de obtener beneficios.
k) Alteración en el funcionamiento de los sistemas.
l) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.
m) Acceso a áreas informatizadas en forma no autorizada.
n) Intervención en las líneas de comunicación de datos o teleproceso.”[41]

[41] TELLEZ VALDÉS, Julio. Op. Cit. Nota 26. P. 190.

Tras haber visto algunas conductas que el mismo Téllez señala nos queda claro que tipo de acciones son las que él dice que se incluyen en esta clasificación.

4.2.4.2. Como objetivo o fin.

Dice Téllez que aquí veríamos aquellas conductas q se realizan en contra de la computadora, sus accesorios o programas de esta. Conductas que el señala a modo de ejemplo las siguientes:

a) “Programación de instrucciones que producen un bloqueo total al sistema.
b) Destrucción de programas por cualquier método.
c) Daño a la memoria.
d) Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).
e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etcétera).[42]

En este es donde el fenómeno, ya mencionado con anterioridad, Anonymous en cuanto a que no buscan otro fin más que afectar la red gubernamental o causar un daño en los sistemas de cómputo de empresas.

[42] Ibídem. P. 190, 191.

4.2.4. Clasificación de los Delitos Informáticos reconocidos por la ONU.

La Organización de las Naciones Unidas quien ya cuenta con su *Manual de las Naciones Unidas para la prevención y control de delitos informáticos* los ha clasificado en cuatro grandes grupos que son:

Fraudes cometidos mediante manipulación de computadoras;
Falsificaciones informáticas;
Daños o modificaciones de programas o datos computarizados; y
Falsificaciones informáticas.

4.3. DELITOS CIBERNÉTICOS Y SU TIPIFICACIÓN.

Después de haber señalado las distintas clasificaciones aportadas por reconocidos juristas que se han enfocado en el estudio del tema así como la que aporta la Organización de las Naciones Unidas, pasaremos a enlistar y señalar cuales son estas conductas en qué consisten y porque deben ser contempladas por el Código Penal de nuestra Entidad Federativa (Veracruz) así como en el Código Penal Federal. Sin más, esas conductas ilícitas son las siguientes:

Acceso ilícito a sistemas informáticos;
Fraude Electrónico;
Falsificaciones informáticas;
Piratería electrónica;
Interceptación y extorción por e-mail;
Revelación y uso ilícito de claves secretas o contraseñas;
Estafas electrónicas;
Terrorismo Cibernético;
Delitos informáticos contra la Privacidad;
Robo de identidad;

Pornografía Infantil en Internet;
Hostigamiento / Acoso en Internet;
Sabotaje Informático.

4.3.1. Acceso ilícito a Sistemas Informáticos.

También denominada esta acción como el *Hacking*, que es accesar sin autorización a sistemas informáticos de otras personas o empresas, valiéndose del uso de Internet. A través de esto se evaden las medidas de seguridad, como contraseñas o claves de acceso.

Existen muchas opciones por las que se realiza esta conducta entre las que pueden encontrarse descubrir secretos o datos reservados de terceros, apoderarse de secretos de empresa (espionaje informático industrial), datos políticos, de terrorismo. La comisión de estas suelen ser con el fin de obtener un lucro.

4.3.2. Fraude Electrónico.

El fraude según el artículo 386 del Código Penal Federal lo comete “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”, sin embargo por razones del gran avance tecnológico se han presentado diversas acciones con el uso de los medios electrónicos y es cuando ha aparecido una variante del delito de fraude que se le ha denominado como fraude electrónico o fraude informático que no es otra cosa que inducir a otra persona a hacer o el restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio que puede ser por alterar el ingreso de datos de manera ilegal. Este delito requiere que el delincuente tenga grandes conocimientos en la materia y por lo mismo es normal en empleados de una empresa que conocen bien las redes de información de la misma y pueden

ingresar a ella para alterar datos como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o inclusive dañar los sistemas, también puede darse al alterar, destruir, suprimir o robar datos, esto en la vida real puede ser difícil de detectar; el alterar o borrar archivos; alterar o dar un mal uso a sistemas o software, alterar o reescribir códigos con propósitos fraudulentos, para realizar estas acciones requieren de un alto nivel de conocimiento en materia de sistemas computacionales. Y otras formas de fraude informático son los que incluyen la utilización de sistemas de computadoras para robar bancos, realizar extorsiones o robar información clasificada o privada.

El bien jurídico que se tutela con la creación de este tipo penal es la Seguridad y la Privacidad en el uso de los sistemas informáticos o en Internet, y sobre todo el patrimonio de las personas físicas o morales que usan las redes.

Al ser un delito que se asemeja al fraude convencional, se cree conveniente que las sanciones sean muy similares a las de este.

4.3.3. Falsificaciones Informáticas.

La Falsificación Informática es cuando con el uso de la computadora se realizan modificaciones ilícitas a documentos impresos o electrónicos para hacerlos pasar por los originales. Obviamente esto es realmente un problema porque hoy en día con los programas existentes se pueden crear documentos y títulos de crédito, así como credenciales o inclusive otro documentos públicos que a simple vista parecen originales y la existencia de esto nos dan lugar a que no se sabe cuándo algo es verídico o falso atentando en estos casos en contra de la fe pública.

El bien jurídico que se tutela con la creación de este tipo penal sería el de la legalidad en los documentos y la fe pública.

4.3.4. Piratería Electrónica.

Por piratería electrónica se entiende el realizar una copia ilegal de un programa o cualquier otro tipo de obra digital con derechos de autor para la obtención de un lucro a través de su venta. También consideramos que una variante de piratería electrónica sería el que una persona obtenga lucro indebido de una obra que no es suya y que la está haciendo pasar por suya.

Con este tipo de delitos se busca proteger el bien jurídico consistente en los derechos de autor y la propiedad intelectual en los medios electrónicos.

4.3.5. Interceptación y extorción por e-mail.

El e-mail es la aplicación más sencilla y más usada de Internet. La palabra e-mail en español lo dice todo; es un servicio de correo electrónico en Internet. Cualquier usuario puede enviar y recibir mensajes a través de la red.

Ahora bien existen personas que con ayuda de sus conocimientos en informática han encontrado la forma de interceptar los mensajes privados que se envían usuarios del e-mail invadiendo la privacidad de estos. Y en cambio hay otras que se dedican a mandar mensajes a otros usuarios intimidándolos y diciéndoles datos personales con la finalidad de que les den información o dinero a cambio de su seguridad personal.

Los bienes jurídicos que se tutelan al tipificar estas conductas son en el caso de la intercepción de e-mail, es la privacidad en las comunicaciones y en el caso de la extorción por e-mail se protege la seguridad de las personas.

4.3.6. Revelación y uso ilícito de claves secretas o contraseñas.

Para que los usuarios de Internet se puedan identificar y diferenciar de los demás usuarios se emplea el uso de los famosos *Nicknames* o nombres de usuarios y sus respectivas contraseñas. Esta medida de seguridad ha sido usada por la mayoría de páginas y sitios web debido a que acceder y crear cuentas es muy fácil y rápido.

El principal problema con el sistema de usuario y contraseñas es que para acceder a las páginas de Internet solo se necesita contar con estos dos requisitos y obviamente recordarlos para no estar creando contraseñas a cada rato pero el problema consiste en que cualquier persona puede ingresar con solo saber estos dos datos sin importar como los obtuvo o si tiene autorización para su uso.

"Para empeorar las cosas, existen varios mecanismos para obtener contraseñas sin la necesidad de adivinarlas, el más popular se basa en usar palabras de diccionario o generar caracteres en secuencia hasta que se obtiene la contraseña de acceso deseada. La mejor forma de asegurarnos en contra de estos ataques es usando contraseñas complejas, al azar y tan largas como sea posible."[43]

En Internet existen personas que suelen engañar a los usuarios nuevos y a los que tienen pocos conocimientos de Internet para que les revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio. Estos delincuentes usan programas para identificar claves de usuarios, que más tarde se pueden utilizar para esconder su verdadera identidad y cometer otras fechorías, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

[43] www.isocron.net/blog/2011/08/02/la-importancia-de-usar-contrasenas-seguras Página consultada de Internet el veintiocho de abril del 2012.

El bien jurídico que se tutela con este tipo es la seguridad y privacidad en Internet al notarse que es obvio que se violan estos con este delito.

4.3.7. Estafas Electrónicas.

Gracias a su gran evolución y avance tecnológico, hoy en día a través de Internet se pueden realizar compras con usuarios de casi cualquier parte del mundo, y es algo muy bueno ya que eso ayuda a los pequeños productores a expandir en el mercado mundial sus productos. El problema radica en que esto permite que aumenten también los casos de estafa. En este caso se trataría de un delito que cumple con todos los requisitos del ilícito de estafa, ya que existe el engaño y animo de defraudar a la persona que realiza la compra de buena fe.

Al no haber mayor explicación para la creación del tipo penal, se pretende con esto proteger el bien jurídico consistente en la Seguridad en las Transacciones realizadas a través de Internet.

4.3.8. Terrorismo Cibernético.

Por Terrorismo, según el Diccionario en línea de la Real Academia Española, es la "… Dominación por el terror. 2. m. Sucesión de actos de violencia ejecutados para infundir terror."[44] Y efectivamente el terrorismo son aquellos actos violentos usados para crear terror en las personas de un país determinado. La finalidad de los terroristas es conseguir objetivos políticos usando la fuerza en lugar de la razón; actos repudiables que provocan daño a menudo a gran cantidad de inocentes.

[44] buscon.rae.es/draeI/SrvltObtenerHtml?origen=RAE&IDLEMA=68265&NEDIC=Si Página consultada de Internet el veintiocho de abril del 2012.

Ahora bien, en el mundo de la informática han aparecido conductas que se asemejan al terrorismo y que los estudiosos de la materia han llamado Terrorismo Cibernético, puesto que a través de engaños o exagerando noticias se crea pánico entre las personas de determinada comunidad, ciudad, región, Estado o hasta de un país entero, mediante el uso de los medios electrónicos, hoy en día ha sido muy común debido a la gran influencia en la sociedad que ha obtenido Internet y sobre todo sus redes sociales.

Con un tipo de esta índole se busca proteger el bien jurídico del orden público, puesto que un pánico colectivo generaría aparte de inseguridad en las personas, un serio problema de descontrol por parte de los ciudadanos con el temor provocado por estas conductas.

4.3.9. Delitos Informáticos contra la Privacidad.

Existen personas que simplemente realizan conductas que pueden afectar la esfera de privacidad del ciudadano por medio de la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos

Este delito se refiere a que una persona no autorizada utilice, modifique o se apodere, en perjuicio de otra, de los datos reservados de carácter personal o familiar que se hallen registrados en ficheros, páginas de Internet o soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado.

El bien jurídico que se busca proteger no es otro que la privacidad de las personas en Internet.

4.3.10. Robo de Identidad en Internet.

El gran avance tecnológico brinda grandes comodidades sobre todo a los jóvenes interesados en información académica o inclusive laboral. En este ámbito la publicación del currículum vitae en Internet, con datos personales como nombre, teléfono, nivel académico, intereses profesionales, experiencia laboral y demás datos hacen que sean un blanco fácil para delincuentes informáticos.

La figura de robo de identidad se da cuando una persona adquiere información de otra y la utiliza para hacerse pasar por ella, provocándole por obvias razones un perjuicio. Este delito se presenta con personas que aprovechan las grandes ventajas que ofrece Internet al poderse escudar de que en tiempo real no son vistos físicamente y facilita el hacerse pasar por otro, sin embargo la prevención de estas conductas es de muy deficiente calidad.

Hoy en día las principales víctimas son los jóvenes de entre 15 y 30 años al ser los más vulnerables ya sea por sus pocos conocimientos o hasta inocencia, pero cabe señalar que nadie está exento de padecer un ataque de esta magnitud. Y esto lo vemos muy a menudo que en las grandes redes sociales observamos que en su mayoría los jóvenes más jóvenes, publican sus datos personales y, la latente posibilidad de que estos sean utilizados en forma ilícita, es grandísima, en la medida en que es mucha la información que se puede obtener de alguien a través de su perfil publicado, en el que solo por mencionar algunas de las más famosas redes sociales que es Facebook, lo podemos apreciar.

Es entonces que podemos ver que con la tipificación de esta conducta se busca proteger la identidad de las personas así como su honorabilidad e imagen ante la sociedad.

4.3.11. Pornografía Infantil en Internet.

En nuestro país como en muchos otros existe lo que se denomina pornografía infantil, que no es otra cosa que toda aquella representación de menores de edad de cualquier sexo en conductas sexualmente explícitas. Esta puede darse a través de representaciones visuales como lo serían las fotografías y demás imágenes, historias o inclusive en videoclips y archivos de audio. De hecho en el 2007 México era considerado el segundo país en pornografía infantil, ante esto diversos Estados de la República han decidido incluir en sus tipos penales el delito de pornografía infantil en Internet

El bien jurídico que se tutela es el sano desarrollo, desenvolvimiento físico, psíquico, intelectual y sexual de un menor de edad.

4.3.12. Hostigamiento / Acoso en Internet.

En Internet ocurre que hay personas que rastrean o buscan a otras con las que tienen problemas directamente o simplemente tienen la intención de causar un daño moral o psicológico a otras en ocasiones sin buscar obtener otro fin que el que se señala, es por eso que se pretende que se cree un tipo penal que abarque estas conductas que pueden ser injurias y ofensas, amenazas o la discriminación que constituyen lo que sería el Hostigamiento a través de los medios electrónicos, conductas que hoy en día vemos tan comunes sobre todo en las redes sociales.

Otras conductas que son muy comunes en Internet y por cierto muy parecidas a las anteriores es el Acoso en Internet, conductas que también son realizadas mayormente con las redes sociales, consistentes en mandar mensajes a una persona con información privada de esta para conseguir la realización de actos sexuales.

4.3.13. Sabotaje Informático.

Este tipo de delito consiste en que una persona destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones, materias primas o equipos informáticos con el fin suspender o paralizar el trabajo de una empresa o institución, y en este se busca la protección del bien jurídico consistente en la libertad de trabajo y asociación.

CONCLUSIONES

PRIMERA.- Internet surgió como una medida estratégica militar, después pasó a ser un apoyo en las grandes universidades y después a conectar al mundo entero. La red de redes creció y se desarrolló hasta ser lo que hoy en día conocemos; sin embargo al haberse abierto al público en general, personas malintencionadas comenzaron a utilizar la red para cometer actos ilícitos y dañinos contra otras personas físicas o morales y es cuando surge el interés de los juristas por contemplar conductas que se realizan a través de este medio, calificando a estas conductas como los delitos informáticos.

SEGUNDA.- Diversos países han regulado Internet y castigado penalmente a estas conductas para mantener el orden y poder ofrecer seguridad y protección a sus ciudadanos que usan a la gran red de redes, países que han optado regular estas conductas desde sus Cartas Magnas otros creándoles leyes específicas y otros tantos con ingresar estas en sus códigos penales.

TERCERA.- En México existe un evidente retraso en materia de regulación de Internet y esto es debido a que nuestros legisladores han regulado ante los

pocos problemas que se han presentado y no han tenido una visión preventiva en sí para enfrentar conductas que se puedan presentar.

CUARTA.- Sin embargo en nuestro país los diferentes códigos penales existentes han hecho el intento de tipificar esas conductas, a nivel estatal vemos que han regulado en cada uno de ellos distintas actividades y entidades como Sinaloa han sido de los que se han esforzado por cubrir la mayoría de las conductas incluyéndolas en varios tipos penales, en cambio otros como el de Veracruz solo tiene un artículo que por ser muy poco específico no cubre nada y es lo que conocemos en el campo jurídico como letra muerta.

QUINTA.- A principios de este año (2012) surgió una reforma en el código penal federal en la que se tipifica a nivel federal diversos delitos informáticos en los cuales, le dan un poco de refuerzo a las legislaciones al incluir delitos como el fraude cibernético y el acceso ilícito a sistemas informáticos, aunque consideramos que esta reforma no es suficiente pero es un gran avance el que estén tomándose medidas al respecto.

RECOMENDACIONES Y SUGERENCIAS

PRIMERA.- Hay necesidad de hacer una unificación de la legislación existente en materia informática con el objetivo de agrupar todas las disposiciones legales que se encuentran dispersas y agruparlas en un solo Código, y así tener una mejor y más fácil, localización de los mismos, ya que la regulación en materia informática es de nueva creación y existe aún un desconocimiento de los ordenamientos que la contempla, es por ello que recopilar estas disposiciones en un solo ordenamiento facilitaría el conocimiento de la materia, consolidando la cultura jurídica.

SEGUNDA.- Es menester una reestructuración de los tipos penales existentes relacionados con la informática, que los órganos legislativos sean apoyados por cuerpos técnicos especializados, para dar elementos de apoyo en materia de Internet, para la mejor elaboración de futuros proyectos de ley.

TERCERA.- Es necesario contar con cuerpos técnico multidisciplinarios especializados, que actúen conjuntamente con las personas encargadas de la impartición de justicia; esto para que se llegue a la sanción de la responsabilidad penal en condiciones más objetivas y justas.

CUARTA.- Se deben revisar las penas en materia de Delitos Informáticos, sobre todo atendiendo a las características de los sujetos activos, ya que es imposible que una persona común y sin la intención de realizar un mal a alguien, pueda llegar a cometer un Delito Informático en perjuicio de la sociedad, esto sería por la falta de conocimientos técnicos mínimos para realizar este tipo de delitos no típicos.

QUINTA.- Se deben de implementar programas para crear una cultura o políticas de prevención en materia de delitos informáticos, ya que en nuestro país, por tener pocos años y ser una rama realmente nueva, se piensa que jamás podríamos llegar a ser víctimas o vernos afectados por la delincuencia informática.

SEXTA.- Tener en cuenta los mínimos de seguridad al momento de hacer transacciones vía Internet, ya sea en cuestiones de compra-venta de un bien o servicio o, cuando proporcionamos datos importantes, personales y confidenciales, a personas las cuales no tenemos ninguna referencia de ellas.

SÉPTIMA.- Es realmente importante que las leyes expedidas en materia de Internet no sean redactadas como resultado de un problema que se haya planteado, sino por un estudio objetivo, en el que se diseñen para afrontar conductas que se presenten a medida que la tecnología avanza, prever situaciones que pueden ocurrir y esto se puede a través del apoyo de personas que se especializan en materia de informática e Internet.

BIBLIOGRAFÍA

ÁLVAREZ LEDESMA, Mario I., *Introducción al Derecho*, Editorial McGraw Hill, México, 1999.

C. MEJÁN, Luis Manuel, *El Derecho a la Intimidad y la Informática*, Editorial Porrúa, México, 2000.

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

Derecho Penal Informático En México. Instituto Nacional de Ciencias Penales. México. 2004.

G. ARECHIGA, R., *Introducción a la informática*, Editorial Limusa, México, 1986.

JARRA, Andrea Viviana. *Comercio Electrónico y Derecho. Aspectos jurídicos de los negocios en Internet.*

LEVINE GUTIERREZ, G. *Introducción a la Computación y a la Programación Estructurada*, Editorial McGraw Hill, México, 1984.

LÓPEZ BETANCOURT, Eduardo. *Derecho Procesal Penal,* Primera Edición, México, Editorial IURE Editores, 2006.

MOLINA SALGADO, Jesús Antonio. *Delitos y otros ilícitos Informáticos en el Derecho de la Propiedad Industrial*, México, Editorial Porrúa, 2003.

NAVA GARCÉS, Alberto Enrique. *Análisis de los Delitos Informáticos*, Primera Edición, México, Editorial Porrúa. 2005.

ROJAS AMANDI, Víctor Manuel. *El uso de internet en el derecho.* Segunda edición, México, Editorial Porrúa, 2001.

TÉLLEZ VALDÉS, Julio. *Derecho informático*, Tercera edición, México, Editorial McGraw Hill. 2004.

Derecho informático, Cuarta edición, México, Editorial McGraw Hill, 2009.

ZAMORA JIMÉNEZ, Arturo. *Cuerpo del Delito y tipo Penal.* Primera Edición, México, Editorial Ángel Editor, 2000.

LEGISGRAFÍA

Código de Defensa Social para el Estado Libre y Soberano de Puebla.

Código Penal Argentino (Ley 26.388).

Código Penal del Estado de Campeche.

Código Penal del Estado de Guerrero.

Código Penal del Estado de México.

Código Penal del Estado de Michoacán.

Código Penal del Estado Libre y Soberano de Durango.

Código Penal del Estado de Yucatán.

Código Penal Federal.

Código Penal para el Estado de Baja California Sur.

Código Penal para el Estado de Baja California.

Código Penal para el Estado de Chiapas.

Código Penal para el Estado de Chihuahua.

Código Penal para el Estado de Coahuila de Zaragoza.

Código Penal para el Estado de Colima.

Código Penal para el Estado de Guanajuato.

Código Penal para el Estado de Nuevo León.

Código Penal para el Estado Libre y Soberano de Jalisco.

Código Penal para el Estado Libre y Soberano de Oaxaca.

Código Penal para el Distrito Federal.

Código Penal para el Estado de Aguascalientes.

Código Penal para el Estado de Querétaro.

Código Penal para el Estado de San Luis Potosí.

Código Penal para el Estado de Sinaloa.

Código Penal para el Estado de Tabasco.

Código Penal para el Estado de Tamaulipas.

Código Penal para el Estado de Tlaxcala.

Código Penal para el Estado de Zacatecas.

Código Penal para el Estado Libre y Soberano de Quintana Roo.

Código Penal para el Estado Libre y Soberano de Veracruz de Ignacio de la Llave.

Convenio sobre la ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (Europa).

Datalog (Suecia).

Datenschutzegesetz o Ley Federal de Protección de Datos (Alemania).

Decisión número 276/1999 del Parlamento Europeo y del Consejo de 25 de enero de 1999 (Europa).

Decreto 209 – 1996 (Cuba).

Human Rights (Canadá).

Ley de Informática, Archivos y Libertades (Francia).

Ley Relativa a Delitos Informáticos (Ley No.19223) (Chile).

Privacy Act (Estados Unidos).

Protocolo adicional al Convenio sobre ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (Europa).

Proyecto de Ley Incorporando al Código Penal el Delito de la Práctica del Grooming (Argentina).

Proyecto de Ley Incorporando el artículo 138 bis al Código Penal, por el cual se tipifica el delito de Suplantación de Identidad Digital (Argentina).

LINKOGRAFÍA

www.ajudicuba.wordpress.com/2011/12/08/redes-sociales-o-no/

www.buenastareas.com/ensayos/Delitos-Ciberneticos/113654.html

www.comercioyjusticia.com.ar/2012/06/01/quienes-roben-identidad-en-internet-podrian-ir-a-prision/

www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf

www.Diariojudicial.com/noticias/No-sos-vos-soy-yo-20120529-0008.html

www.fundacionorange.es/areas/28_observatorio/pdfs/censura.pdf

www.gdt.guardiacivil.es/webgdt/media/Legislacion/Protocolo_adicional_convencion_cibercrimen.pdf

www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf

www.inegi.org.mx/inegi/contenidos/espanol/prensa/comunicados/modutih10.asp

www.informationweek.com.mx/analysis/reforman-codigo-penal-federal-para-castigar-mas-duramente-los-delitos-informaticos

www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos

www.maestrosdelweb.com/editorial/internethis

www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=123

www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

www.porticolegal.com/guias/delitosInformaticos.php

www.pueblaonline.com.mx/index.php?option=com_k2&view=item&id=12872:usuarios-de-internet-crecen-185-anualmente-inegi&Itemid=126

www.revista.seguridad.unam.mx/numero-02/seguridad-tv

www.rincondelvago.com/derecho-penal-en-colombia.html

www.rtve.es/noticias/20120228/anonymous-quienes-son-como-actuan/438765.shtml

www.segu-info.com.ar/cruzada-robo-identidad