El Saber de mis Hijos
hará mi Grandeza

Universidad de Sonora
División de Ciencias Sociales
Departamento de Derecho

"Ciber-criminalidad: Nuevos Retos Para la Seguridad Pública"

TESIS

Que presenta para obtener el título de Licenciado en Derecho:

Martina Livier Gómez

Martínez

Directora: Dra. Martha Frías Armenta

Hermosillo, Sonora. Febrero, 2014.

Universidad de Sonora

Repositorio Institucional UNISON

Agradecimientos

A MIS PADRES:

Mtra. Martha Martínez García

Lic. Martin Leobardo Gómez Tadeo

Por su dedicación en mi crianza, enseñanza y amor

que me hizo ser la persona que soy actualmente.

Gracias por ser mis padres, mis mentores y amigos.

A MI HERMANO Y ABUELA:

Ing. Jesús Antonio Gómez Martínez

Sra. María Dolores García Martínez

Por su apoyo y cariño constante

durante los años de mi vida.

A MIS MAESTRAS:

Dra. Martha Frías Armenta

Dra. Julia Romero Ochoa

Dra. Hortensia Arvizu Ibarra

Dra. Lucila Caballero Gutiérrez

Por haberme guiado dentro y fuera de las

aulas con su conocimiento científico.

A MIS AMIGOS:

A quienes me han ayudado durante

Los momentos felices, pero sobre todo en

los difíciles. Por su confianza y fraternidad.

ÍNDICE

1. Introducción

La tecnología de la comunicación avanza constantemente a pasos rápidos y agigantados. Es posible afirmar que existe una dependencia entre las máquinas de lenguaje ordenado y la población que se encuentra en los diversos sectores sociales quienes se ven beneficiados principalmente en cuestiones temporales y geográficas, sin embargo, el aspecto negativo del manejo de las TICs se refiere a los llamados delitos cibernéticos que se encuentran a la orden del día en su comicidad, ya que descritas como actitudes concebidas por el hombre y no propias de la máquina como se ha llegado a pensar. Este vínculo supone que a partir de la utilización reiterada de las mismas, se crean situaciones jurídicas de naturaleza tanto lícita como ilícita. Por ello, analizaré mediante la revisión de teoría, legislación y problemática socio-jurídica la pertinencia de la implementación de la figura de la Policía Cibernética en todos los Estados de la República Mexicana cuyas funciones deben ser competentes para la investigación en el ciberespacio así como para la recopilación de material digital que pueda ser utilizado como prueba en juicio. De tal manera, que intentaré resaltar los aspectos principales del uso de Internet en la actualidad, así como la forma en que es utilizado como armamento en guerras nacionales e internacionales y a favor de las organizaciones delictivas como territorio sin límite.

Por otra parte, la legislación mexicana, si bien se ha preocupado por regular la materia informática en México en aras de la protección personal y económica, la parte que le compete al derecho penal ha quedado vulnerable en la adición y actualización de ilícitos que pueden ser adecuados a los tipos penales, así como

aquellos que tienen su origen en las entrañas de Internet y requieren de la mira de los legisladores.

La cultura informática es un tema que se encuentra presente a lo largo de la utilización de los sistemas cibernéticos para cualquier uso o fin del usuario. Especialmente debe ser preponderante la supervisión por parte de los padres cuando los cibernautas son menores. Aunque la edad no es un factor determinante de quienes pueden ser víctimas de un ilícito en el ciber-espacio, es menester de todos concientizar a la sociedad de los peligros que acechan en la red.

El análisis histórico de las guerras cibernéticas permite determinar la escala de prohibición en salida de información y los regímenes autoritarios que permean por la corriente informática en los países del mundo.

La importancia de realizar un análisis de la figura de la policía cibernética mexicana permitirá identificar las fallas latentes en su sector y ampliará la perspectiva de la ciudadanía por adoptar una cultura de seguridad cibernética que les permita adquirir los conocimientos básicos ante las redes de delincuencia cibernéticas.

Además, contar con una policía cibernética eficiente en México es indispensable para la vigilancia y cumplimiento de las conductas criminales que han evolucionado junto con la tecnología pues es innegable que son supuestos generales que son aplicados a operaciones realizadas por medios electrónicos y se trata de reacciones que se producen en la sociedad, pues constituyen amenazas en diferentes niveles. En primer lugar, por la constante amenaza de inseguridad hacia el usuario que utiliza el ordenador con respecto al respeto de su integridad humana

y en segundo, la protección de la información confidencial generada por los Estados cuya filtración representa conflictos de seguridad nacional.

Analizar los riesgos que generan para los usuarios el uso de Internet y examinar el papel que ha desempeñado la policía cibernética en México desde su instauración para combatir la inseguridad que surge del uso de las nuevas tecnologías de la información. Además, revisaré las disposiciones legales existentes que rigen la utilización de la informática como medio por el cual se cometen delitos, así como aquellas que regulan la utilización de pruebas digitales para probar actos jurídicos en un juicio.

Con el presente trabajo se pretende evidenciar que los cuerpos policiacos informáticos son escasos y poco eficientes. La legislación por su parte debe actualizarse junto con la necesidad social de protección ante nuevas formas de delincuencia que surgen de las entrañas de las computadoras, es por lo anterior que presento la hipótesis de que si no se combate la delincuencia cibernética en México, esta representará una amenaza para el Estado y la seguridad de los ciudadanos.

2. *Derecho Informático*

A) ANTECEDENTES Y CONCEPTO

Debido al constante crecimiento y popularidad que ha ganado Internet, el campo de los delitos se ha extendido al área informática, lo que ha provocado el crecimiento de delitos cometidos mediantes las TICs, de forma que a los delincuentes se les ha suministrado de nuevas armas y medios para su comicidad. Las amenazas cibernéticas son diversas y no respetan rangos de edades por lo que cualquier usuario de Internet está expuesto a ser víctima de la delincuencia en el ciberespacio, así como cualquier usuario de cometer un delito informático.

Internet tuvo su origen en Estados Unidos como ARPANET mediante una propuesta que surgió de la idea de Lawrence G. Roberts en 1966[1] de tener la capacidad de compartir información académica mediante una red amplia en forma de paquetes. Es así, que en los años siguientes, específicamente en 1969, su proyecto se convirtió en realidad mediante la conexión de cuatro ordenadores en distintas universidades americanas para intentar realizar el primer envío de datos, lo que resultó en un bloqueo de redes. Sin embargo, en los próximos años hubo resultados satisfactorios, y los ordenadores de más campus universitarios en el país se adhirieron al enlace logrando compartir información académica.

Hacia el año de 1982, ARPANET había sido dividida en MILNET, red que fue creada específicamente para el tráfico de información del departamento de defensa de Estado Unidos, así que ARPANET siguió funcionando únicamente para cuestiones de carácter académico. El aumento de capacidad de conexión a la red

[1] G. ROBERTS, MIT, *"Hacia una red Cooperativa de Computadoras de Tiempo Compartido",* Estado Unidos, 1966 (Inglés)

aumentó drásticamente, pasando de tener al menos 200 ordenadores conectados en 1978, la cifra creció a más de 10,000 en 1989.

ARPANET fue desmantelada en 1990[2], debido a su rotundo éxito y dejó miles de enlaces que son los que hoy conocemos como Internet propiamente, aunque su tráfico comercial en ese año aún se encontraba prohibido, pues la idea principal del surgimiento de ARPANET había sido el de compartir información de carácter académico y al cual solo los estudiosos de grupos seleccionados tenían acceso. No obstante, dicha prohibición fue removida el año siguiente de 1991 y es en ese mismo año que Tim Berners-Lee hizo público el primer código de World Wide Web. Al mismo tiempo que unos programadores del Centro Nacional de Aplicaciones de la Supercomputación crearon el primer navegador gráfico para el *WWW* que se llamó *Mosaic*, y después se transformó en *Netscape*.

La primera vez que se habló del Derecho Informático data en el año de 1949, cuando Nortbert Wiener[3] menciona en su obra *Cibernética y sociedad,* que "*los problemas de la ley deben considerarse como comunicativos y cibernéticos, es decir, son problemas de regulación ordenada y reproducible de ciertas situaciones críticas",* en otras palabras, dado que la cibernética estudia la estructura de los sistemas reguladores basados en la retroalimentación y cuyo objeto es el de desarrollar un lenguaje y técnicas que permiten abordar el problema de control y comunicación, Weiner lo encontró aplicable al derecho desde el punto de vista sistémico.

[2] SUNDARAM, Ravi, "*Temas sobre informática teórica: problemas de la investigación del Internet",* publicado el 13-02-2002 y consultado el 10 de Octubre de 2013 http://mit.ocw.universia.net/18.996/s02/lecture-notes/lecture2_mit.pdf

[3] WIENER, Norbert, *"Cibernética y Sociedad",* INEGI, México, 1981, p.97.

Mientras que Téllez se refiere al derecho informático como la [4]. La secretaría de Programación y presupuesto considera que el Derecho informático constituye más bien un cuerpo jurídico y articulado en cuanto a su tema real: el uso de la informática y la tecnología. [5]

El derecho informático nace a partir de la utilización de los sistemas informáticos como medio o fin en la comisión de actos jurídicos que evolucionaron en un espacio virtual con finalidad material. La necesidad de proteger éstos actos jurídicos, así como el sancionar los delitos cometidos a través de las TIC se hizo ineludible desde el principio de la comercialización de las computadoras, especialmente en aras de la protección de la información personal. La privacidad es quienes somos, lo que pensamos, lo que hemos hecho, lo que sabemos y lo que queremos hacer[6], por tanto, la intrusión a lo que somos o el robo de la misma, constituye una amenaza a nuestra intimidad.

B) INFORMÁTICA JURÍDICA

La informática Jurídica es una parte de la Informática con aplicación en el Derecho[7], de modo que tiene su origen en la tecnología como herramienta que apoya a la ciencia jurídica y su utilización se ha convertido en soporte en el ámbito jurídico.

---

[4] TELLEZ Valdés, Julio, *"Derecho Informático",* Editorial UNAM, México, 1991, Pág. 7.
[5] Secretaría de Programación y Presupuesto, "*La Informática y el Derecho"*, INEGI, México, 1983, p. 23.
[6] FLINT, David, *"Ley modelando la tecnología: la tecnología modelando la ley",* Revista Internacional de Derecho, Computadoras y tecnología, Vol.23, Marzo-Julio de 2009.
[7] *Ídem.*

En este mismo tenor, no hay que confundir el término Derecho informático con el de Informática jurídica o Jurismática[8], pues el primero se basa en el estudio y regulación de conductas mediante un ordenador y el segundo alude a la utilización de las tecnologías como instrumento de apoyo en el campo jurídico. Aunque en un principio, la informática jurídica era solo de carácter documental como recuperación de información[9], no obstante, en la actualidad se ha ido configurando como una verdadera interdisciplina. Ejemplo de ello, la publicación de jurisprudencias en el sitio de la Suprema Corte de Justicia de la Nación; la actualización diaria de las demandas recibidas en los sitios del Poder Judicial de los Estados; los juicios en línea; las revistas jurídicas electrónicas; las bases de datos criminales de la policía, etc. cualquier actividad jurídica relacionada con el manejo de un ordenador por quienes actúan en el ámbito del derecho[10].

Su clasificación se divide en tres aspectos[11]:

i. Informática jurídica documental. Es una apreciable herramienta para obtener de modo mucho más ágil y certero al que permiten los métodos tradicionales, información referente a la legislación, jurisprudencia y doctrina.

ii. Informática jurídica de gestión y control. Aquellas que permiten desarrollar distintas actividades, mediante el uso de un computador, en las áreas registral, judicial y profesional, apto para producir la

[8] *Ibídem.*
[9] ROMEO CASABONA, Carlos Ma. , *"Poder informático y seguridad jurídica",* Fundesco, 1988.
[10] PEÑA, Carlos A. *"Informática Jurídica y Derecho Informático"* , Universidad de Palermo, *www.palermo.edu/ingenieria/downloads/pdfwebc&T8/8CyT05.pdf*
[11] PRADO, Pedro Antonio. *"La informática y el abogado"* Ed. Abelardo Perrot, Buenos Aires, 1988.

automatización de juzgados especialmente en las áreas de emisión de documentos, archivo de datos correspondientes a los expedientes, control y seguimiento del trámite de expedientes y manejo de agendas.

iii. Informática jurídica decisionaria o metadocumental. Los sistemas decisionales pueden resolver automáticamente los problemas que se les plantea o bien ayudar al usuario a adoptar una decisión, allanándole en ciertos aspectos, el camino hacia la solución apropiada. De allí que se afirme que estos sistemas se basan en lo que se denomina inteligencia artificial.

En México, los juristas nacionales se vieron amenazados por primera vez en su labor y eficiencia debido al desarrollo de las nuevas tecnologías, temerosos de ser superados por la época, fue entonces que los estudiosos de la Universidad Autónoma de México aprobaron en 1981 la creación de UNAM-JURE[12] mediante la cooperación con el *Institut de Recherche et d'Etudes pour le Traitement de l'Information Juridique* (IRETIJ) de Francia, un banco de datos en el que ambos pudieran intercambiar información específica de sus campos en la ciencia jurídica para su utilidad mutua. En 1986 este convenio fue renovado por su gran aceptación e importancia, mismo que actualmente se encuentra incluido en el programa de estudios científicos de CONACYT[13].

[12] CERVANTES CABALLERO, Eva Leticia. *"Problemática documental de la información jurisprudencial en México"* México, 1991. http://72.44.81.97:8080/jspui/bitstream/123456789/10017/2/mem21105-116.pdf
[13] FIX FIERRO, Héctor, MUÑOZ DE ALBA, Marcia, "*El sistema unam-jure hoy, Diálogo sobre informática jurídica",* Editorial UNAM, 1989. Págs, 31 y 32.

Su principal aportación como base de datos, es el contenido de fichas de análisis que elaboran los juristas a partir del estudio de documentos legislativos de relevancia general que son publicados en los periódicos Oficiales de la Federación y los Estados desde el año 1917 a la fecha.

Hacia el año 1988 se encontraban disponibles 19,000 fichas de análisis consultables en línea que constituye en México, un gran avance y herramienta que aporta la informática jurídica a nuestro sistema judicial.[14]

Además de la documentación digital, los juicios virtuales han provocado el asombro de la comunidad jurídica, ya que por su naturaleza no necesitan existir en un solo lugar físico, sino de manera electrónica, y pueden ser configurados sin requerir que las partes gasten fortunas en software o hardwares adicionales. Por una parte, su implementación representa una gran economía procesal y por otro lado, el temor de los abogados litigantes de saber si serán competentes para insertarse en esta nueva modalidad mediante capacitaciones. Ejemplo de ello es el éxito que ha significado para el sistema judicial de Singapur, la cual es una de las salas virtuales más completas en el mundo, con una conexión a Internet capaz de utilizar imágenes, multimedia y video conferencias en tiempo real.

En el campo del derecho, la informática se ha convertido en uno de los motores principales de apoyo para realizar las tareas que la abogacía requiere. Por lo tanto, los profesionales del derecho se encuentran aun subiéndose al barco de la actualización en el campo de las nuevas tecnologías.

[14] CÁCERES NIETO, Enrique. *"El sistema UNAM-JURE, un banco de información legislativa"*, México 1991.

Es por lo anterior, que se considera que *"el jurista que trabaje con internet debe considerar que el sistema se concibió y desarrolló con la idea de proporcionar un acceso fácil a la información y servir como un medio de comunicación rápido y efectivo (…). Esto no significa que el uso de internet no sea adecuado para el trabajo de los juristas, sino sólo hay que tener presentes los riesgos de seguridad cuando la utilizan.*

Puesto que aún no existen soluciones claras para muchos problemas en este campo, será tarea de todos nosotros, juristas interesados, proponer soluciones que contribuyan a brindar seguridad legal al uso de servicios de internet."[15]

C) INFORMATIZACIÓN DE LA SOCIEDAD

A partir de la fusión de las palabras "comunicación" (hacer común), e "información" (instruir hacia adentro)[16], es que encontramos la importancia que ha generado una cantidad de definiciones para explicar la informatización que ha surgido en la sociedad. Por ejemplo, *"telecomunicaciones" significa comunicar a distancia, "informática" que proviene de "información", auto y mática, supone el procesamiento automático de la información; "telemática" es la conjunción de "telecomunicaciones" e "informática", e implica la transmisión y el procesamiento automático de la información*[17].

[15] ROJAS AMANDI, Víctor M. *"El uso del Internet en el Derecho"* Ed. Oxford, México, 2000, P.11
[16] CARRANZA TORRES, Luis "Las nuevas tecnologías de la información y el contralor ciudadano de la administración" Revista Informática Jurídica http://www.informatica-juridica.com/trabajos/Las_nuevas_tecnollogias.asp
[17] CARRANZA TORRES, Luis." El derecho frente a la sociedad de la información" http://www.informatica-juridica.com/trabajos/El_derecho_frente_a_la_sociedad.asp

El avance de las tecnologías ha propiciado la facilitación de las tareas cotidianas a costa de convertirse en víctimas de los piratas informáticos. La informatización de la sociedad ha prevalecido y se ha desarrollado desde el inicio de la comercialización de los ordenadores a los ciudadanos normales. Su uso reiterado y capacidad de realizar enormes cantidades de tareas se ha convertido en una necesidad social, desde el niño al que los maestros le exigen presentar su trabajo de manera formal e impreso, hasta los magistrados que confirman o modifican sentencias en formato digital.

Lo anterior, aunado con el auge de Internet en el siglo XXI, deja en claro que su empleo ha borrado los límites nacionales y hemos sido forzados a entrar en la era digital.

Así mismo, nos ilustra Wegener[18] que *los beneficios de la era digital se acumulan solo si existe confianza en el funcionamiento, la fiabilidad, la integridad y la seguridad de las tecnologías subyacentes: es por ello que la seguridad digital se ha convertido en un desafío global.*

Se dice entonces que la globalización es un término relativamente viejo, que surge a partir de la revolución tecnológica como proceso histórico cuyo beneficio y detrimento es difícilmente reversible. Es un proceso adaptable a cierto periodo histórico según se haya presentado en su contexto pero con un enorme impacto social. Tal como señala Edgar Vieira P. "*Las transformaciones y cambios tecnológicos aportados por los periodos de globalización son de tal importancia y alcance que la humanidad ha ido ingresando en nuevos contextos de vida*

[18] HENNING Wegener, Los riesgos económicos de la ciberguerra dialnet.unirioja.es/descarga/articulo/4276097.pdf

prácticamente irreversibles, pero no imposibles de ajustar y de mejorar en aquellos resultados negativos de pobreza y distribución inequitativa del ingreso(…)"[19]

No podemos hablar de globalización sin recurrir a McLuhan[20], quien en 1962 acuñó su término "aldea global" y en su obra plasma pensamientos negativos acerca del deterioro de la imagen individual y colectiva tradicional la cual no se encontraba muy alejada de la realidad moderna. Y como éste, se han desplegado más términos que buscan adecuar su significado a estos cambios sociales como "era informática", "sociedad de la información", "sociedad del conocimiento" y otros cuya base en común reside en el contexto del desarrollo de las TIC que han sido clave en la aceleración de la globalización económica.

Se crea una homogeneización jurídica que se presenta desde el mercado económico, transmutando debido a los modelos jurídicos flexibles, que como dice Campuzano, "*la globalización se nos presenta como la era de la descentralización y de la dispersión normativa (…) la rehabilitación del derecho en el contexto transnacional precisa de la reformulación de la soberanía flexible, abierta, porosa y permeable, pero firmemente comprometida con el núcleo axiológico que representa el orden constitucional*"[21]

El surgimiento de la Corte Penal Internacional es un claro ejemplo de una homogeneización jurídica internacional, que surgió de la Conferencia de

[19] VIEIRA POSADA, Edgar. "Interpretaciones Y Transformaciones Tecnológicas En Los Procesos De Globalización."Papel Político 16.2 (2011): 667-699. consultado online el 8 de Octubre de 2013.
[20] Según McLuhan la televisión, la computadora y el satélite perturban y deterioran la imagen individual y colectiva, de tal forma que crean temor y ansiedad. Y por consiguiente la violencia se manifiesta de múltiples maneras como una búsqueda involuntaria de esa identidad perdida.
[21] CAMPUZANO, A.J, Racionalidad jurídica y globalización. Paradojas y perplejidad en torno al ordenamiento jurídico, Revista Cien. Jur. e Soc. da Unipar, Umaurama, v.11, n.1, p. 223-245, En/Jun, 2008.

Plenipotenciarios para el establecimiento de este organismo del 15 de Julio de 1998, y cuya fecha de entrada en vigencia fue el 1 de Julio de 2002 adoptando el carácter de permanente e independiente. Aunque esta Corte Penal Internacional (CPI), solo puede ejercer su competencia automática cuando el Estado en el que se ha cometido el delito ha ratificado el tratado, o bien si la persona que cometió el delito es ciudadano de un Estado que de igual manera a ratificado su tratado y específicamente cuando corresponda a la comisión de delitos considerados más graves por la comunidad internacional.[22]

El jurista Manuel Atienza[23] por su parte también hace un estudio del fenómeno de la globalización jurídica en la cual dice que "*hay que considerar al derecho como fenómeno esencialmente estatal, como un conjunto de normas establecidas por las autoridades de un Estado resulta cada vez más insatisfactorio (…) a excepción de la rama penal, en otros sectores del Derecho, la incidencia de reglamentaciones supraestatales o transnacionales es una exigencia simplemente, de la naturaleza de las cosas. El comercio internacional, el internet, los movimientos migratorios, la ecología o el terrorismo son fenómenos que no pueden regularse con eficacia en el ámbito nacional y escapan también al Derecho internacional entendido en sentido clásico (…). Se trata de entender que los elementos jurídicos, culturales, etc., integran una unidad compleja dentro de la cual tiene lugar una interacción constante. Así, el derecho ha contribuido a lo que llamamos globalización de nuestra sociedad pero, al mismo tiempo, la globalización está haciendo cambiar los sistemas jurídicos y la concepción del derecho*".

[22] PÉREZ CRUCI, Juan Ignacio, *"La globalización y sus consecuencias en el nuevo orden jurídico internacional".*
[23] ATIENZA, Manuel. *"Constitucionalismo, globalización y derecho. El Canon",* 2009.

El impacto tecnológico generado por la entrada de Internet que ha alcanzado a más de 500 millones de usuarios en el mundo actualmente, quienes se comunican, practican comercio o buscan una forma de entretenimiento que deja una idea clara de que el espacio cibernético es una parte primordial de la vida de las personas y que ha alcanzado su mayor auge a partir de los años noventa.

Solo para dejar un ejemplo más claro de esto, podemos observar en la vida cotidiana el uso reiterado y habitual que juegan Internet y los sistemas computacionales en ella. Los bancos utilizan sistemas de redes interbancarias para hacer diferentes tipos de transacciones, las compras en línea, las inscripciones a las escuelas ya se logran por este medio, reservar boletos del cinema, comprar un boleto de avión, la obtención de información para hacer una tarea, hablar con tus compañeros de trabajo, revisar el clima, leer tu novela favorita, entre miles de actividades que podría mencionar.

Por otra parte, el auge de las redes sociales ha sido un importante factor que vulnera la intimidad y seguridad de los usuarios quienes comparten información personal a la vista de millones. Redes sociales como Facebook y Twitter que han ganado tanta popularidad recientemente por ser espacios virtuales que permiten el intercambio no solo de información personal, sino de fotografías, videos y estados de ánimo resultan ser un atractivo para quienes quieren estar en contacto cercano con otros usuarios o simplemente por morbo social. Pero ¿Qué hacen estas empresas virtuales para asegurar nuestra información? El hecho de que cualquiera pueda hacer una cuenta en estos sitios mediante el registro de un correo electrónico permite la fácil creación de un alias falso. No hace mucho las extorsiones mediante *Facebook* se han convertido en realidad y no solo el usuario está en riesgo, sino

también los “amigos” de éste. De esta manera, los hábitos cibernéticos inseguros han aumentado los niveles de delincuencia mundial.

Es innegable que existe una responsabilidad reciproca del usuario y los proveedores de servicios en los sitios web. Los primeros tienen la responsabilidad de saber qué información comparten y en qué sitio, mientras los segundos tienen la responsabilidad de reforzar su seguridad cibernética para brindar confianza entre sus clientes o usuarios. Pero, ¿En realidad los sitios de Internet como las redes sociales –sin hablar de sitios de carácter institucional- tienen la obligación de protegernos?

Básicamente Internet no es más que una serie de ordenadores conectados entre sí que transmiten información[24] y su estrecho lazo con la *retroalimentación de usuarios* es el complemento que llena de riqueza el mundo del ciberespacio en el cual encontramos más de medio billón de sitios a los que podemos accesar diariamente de forma gratuita. La Web ofrece una infinita cantidad de información acerca de diversos temas que resultan atractivos a los usuarios de la red quienes accesan mediante la escritura de “WWW”[25] seguido del nombre del sitio al que pretenden visitar.

D) SISTÉMICA Y DERECHO

Un sistema es un conjunto que funciona completo, pues si dividimos sus partes dejaría de existir como tal y su connotación depende de que lo *consideremos* como un sistema para poder explicarlo.

[24] BADIA, Félix. *“Internet, situación actual y perspectivas”,* Ed. La Caixa, Barcelona, 2002, Pág. 22
[25] World Wide Web

Para Bertalanffy[26] la sistémica "*es un marco que estudia los sistemas integrados que derivan sus propiedades esenciales de sus interrelaciones en vez de las propiedades de sus partes"*[27]*.* Es decir, que la realidad se debe percibir como un conjunto, un todo y no como una discontinua colección de partes individuales, lo que se puede aplicar al derecho cuya visión es la de comprender al fenómeno jurídico como un todo y relacionar normas, hechos sociales y valores.

La sistémica intenta desarrollar su visión a partir del conjunto y no de las partes, pues hablar de cada parte significaría algo completamente distinto que al unificarlo y el resultado de ello sería el sistema. Por ejemplo, si pensamos en una Universidad, sus partes son maestros, alumnos, aulas, materias, etc., podemos describirlos por separado, pero el ente "Universidad" conlleva un significado distinto.

El Dr. Ulises Lugano señala que *"desde el punto de vista sistémico, puede definirse el derecho como un sistema de información obligatorio que tiende a obtener la adecuación de todas las conductas a cada nuevo estado del sistema, según la información que éste brinda"*[28]

Intzessiloglou[29] por su parte estipula que podemos considerar el sistema del derecho como un sistema cibernético pues trata de informaciones que conciernen a la vida social cotidiana porque tiene:

1. *"Un objetivo: la regulación social*

[26] VON BERTALANFFY, Ludwig "Teoría General de los Sistemas" Fondo de Cultura Económica, México, 1984.
[27] Op Cit.
[28] GRÜN, Ernesto, *"El derecho en el mundo globalizado del siglo XXI desde una perspectiva sistémico cibernética",* Revista Telemática de Filosofía del Derecho n°4 2000/2001, .43-124. http://www.rtfd.es/numero4/3-4.pdf
[29] INTZESSILOGLOU, Nikolaos G., *"L'approche systémique au système ouvercomme stratégie d' élaboration' d'un project d'étude interdisciplinaire de phénomène juridique* » Congreso jurídico de sistémica, Lausanne, 1989 p. 168

2. *Un programa de acción: que está grabado en un subsistema normativo*
3. *Un procedimiento de decisión: la formal del juez*
4. *Una función de ejecución: ejecución del juez por los órganos administrativos*
5. *Una función de retroacción: la regulación social puesta en marcha por el funcionamiento el sistema jurídico y analizando en resolución de conflictos, reproducción de estructuras jerárquicas sociales e integración social, reproduce el sistema jurídico en sí mismo, dándole "estabilidad" y la duración necesaria para su existencia. A la larga esta retroalimentación conduce a la evolución del sistema jurídico."*

E) PANORAMA NACIONAL

México no ha sido exento de ser alcanzado por la era de la información, y para lo cual se ha de reconocer que cada año el número de usuarios que cuentan con computadora, así como, el servicio de Internet va en alza.

Según estadísticas del Instituto Nacional de Estadística y Geografía[30], quienes arrojaron datos acerca del uso de tecnologías en nuestro país, el 32.2% de hogares en la república tiene al menos una computadora en su hogar con un incremento del 8.9% desde el 2011; el 26% de hogares cuenta con un servicio de Internet; hay 44.7 millones usuarios mexicanos con edades predominantes entre los 12 y 34 años de edad; el 49% son mujeres y el 51% son hombres. Además, el 59.7% de los usuarios encuestados señalan que utilizan Internet como medio de comunicación, mientras que el 31.1% lo utiliza para asuntos relacionados con la

[30] INEGI. Usuarios de Internet en México.
http://www.inegi.gob.mx/est/contenidos/espanol/temas/Sociodem/notatinf212.asp

escuela. Y por último, que el 48% de estos usuarios accesa a Internet con mayor frecuencia fuera de su hogar.

Usuarios de Internet por lugar de acceso y disponibilidad de computadora en su hogar, 2000 a 2012

Año	Total nacional	Acceden a Internet en su hogar [a]	Acceden a Internet fuera de su hogar		
			Total	Su hogar tiene computadora	Su hogar no tiene computadora
2000 [b]	5 057 533	2 568 783	2 488 750	294 238	2 194 512
2001 [c]	7 097 172	3 227 788	3 869 384	908 453	2 960 931
2002 [c]	10 718 133	3 920 649	6 797 484	1 989 527	4 807 957
2003 [b]	11 883 041	4 504 767	7 378 274	2 225 947	5 152 327
2004 [d]	12 835 946	4 907 385	7 928 561	2 420 501	5 508 060
2004 [e]	13 983 492	5 126 131	8 857 361	2 811 945	6 045 416
2005 [d]	16 364 130	5 178 626	11 185 504	3 131 760	8 053 744
2005 [e]	17 966 001	6 014 500	11 951 501	3 697 656	8 253 845
2006 [f]	18 517 066	6 210 750	12 306 316	3 889 828	8 416 488
2006 [e]	20 564 256	6 917 151	13 647 105	4 781 619	8 865 486
2007 [g]	20 848 040	7 116 782	13 731 258	4 831 857	8 899 401
2007 [e]	22 104 096	8 312 883	13 791 213	4 877 952	8 913 261
2008 [g]	22 339 790	8 426 749	13 913 041	4 922 812	8 990 229
2008 [e r]	23 260 328	9 138 944	14 121 384	4 625 711	9 495 673
2009 [h]	27 206 174	12 508 010	14 698 164	4 392 896	10 305 268

2009 e	28 439 250	13 201 930	15 237 320	4 259 603	10 977 717
2010 i	32 807 240	15 800 846	17 006 394	4 135 569	12 870 825
2010 e	34 871 724	16 922 047	17 949 677	3 968 185	13 981 492
2011 j	37 619 377	18 499 790	19 119 587	3 877 967	15 241 620
2011 e r	40 605 959	21 133 179	19 472 780	3 729 583	15 743 197
2012 j	40 916 394	21 267 017	19 649 377	3 636 655	16 012 722
2012 e r	45 108 655	22 489 854	22 618 801	3 498 718	19 120 083

Tabla con datos estadísticos de INEGI www.inegi.gob.mx

La cantidad de usuarios que existen en la red permite darnos una visión de la presencia de un amplio catálogo de víctimas potenciales de cualquier delito de carácter cibernético, así como de ser espiados por organizaciones o gobiernos como se ha considerado en el territorio mexicano.

A raíz de los espionajes internacionales, una de las situaciones preocupantes para México, son las controversias que se desataron a raíz de la visita de Martin Muench, creador de la aplicación *FinFisher*, un software dedicado a la intrusión de equipos computacionales y telefónicos por el cual, mediante el espionaje son capaces de detectar cualquier clase de información a través de virus o troyanos informáticos que les permiten la entrada a los dispositivos. Según palabras de Miriam Saage-MaaB[31] lo que se pretende es monitorear comunicaciones de periodistas, manifestantes y blogueros para identificarlos y arrestarlos.

[31] La Jornada, *"Activistas Europeos piden al IFAI investigar sobre software espía",* publicado el 24-07-2013, consultado el 30-08-2013, http://www.tedf.org.mx/sala_prensa/sintesis/sm2013/jul/130724/130724_ifai_activistas_europeos.pdf

El 20 de Junio de 2013, los grupos Propuesta Cívica y ContingenteMX, así como el Centro Europeo por los Derechos Constitucionales y Humanos (ECCHR) pidieron al IFAI la investigación sobre la implementación de este software que la Universidad de Toronto detectó ya existía en territorio nacional.

El espionaje cibernético ha causado un auge impresionante y negativo tanto para los ciudadanos que son sujetos a ser interceptados en la privacidad de sus dispositivos propios, así como los Estados se han vuelto víctimas en la revelación de secretos. El presidente Enrique Peña Nieto se ha visto envuelto en la polémica de espionaje del cual fue víctima por parte del ex analista de la NSA (Agencia de Seguridad Nacional de Estados Unidos) Edward Snowden, quien interceptó mensaje privados entre Peña y nueve de sus aliados partidistas y cuya información fue entregada a la cadena nacional de televisión brasileña TV Globo.

F) PANORAMA INTERNACIONAL

Se extiende por el mundo una nueva forma de activismo social. Los Estados internacionales se dan por enterados de acontecimientos suscitados a nivel mundial como las revoluciones árabes, las filtraciones de secretos de Estados Unidos, o movimientos nacionales como el afamado “Yo soy 132 en México”.[32]

Vivimos en una sociedad en constante cambio, la tecnología nos supera cada día, y la necesidad de acceder a información en grandes bancos de datos, para diversos fines particulares, impera en la sociedad que se ve inmersa en la

[32] GARCÍA GALERA, María del Carmen, DEL HOYO HURTADO, Mercedes *"Redes Sociales, Un Medio Para La Movilización Juvenil "* Zer: Revista De Estudios De Comunicación 17.34 (2013): 111-125. consultado 8 Oct. 2013.

navegación en redes para adquirir nuevos conocimientos. Abrir un navegador como Google o Yahoo y teclear palabras claves es más natural actualmente que sentarte a leer el índice de un libro para iniciar una búsqueda. No obstante, estos avances han llevado a los gobiernos –unos más que otros- a tomar medidas restrictivas sobre la entrada y salida de información mediante las redes informáticas. Ejemplo de ello, China que es el país con la mayor cantidad de cibernautas en el mundo con 591 millones[33], pero también el que más aprehensivo se muestra con referencia a las redes sociales como Facebook, cuyo uso fue prohibido en este país debido a la sensibilidad política que atraviesan en su comunismo. "*La creciente aceptación e introducción de las tecnologías digitales en la planificación y el armamento militar da paso a la perspectiva de una ciberguerra en la cual, habida cuenta de la interdependencia global de las estructuras de red, podría inevitable y profundamente afectar a la economía y a esenciales activos de la sociedad".*[34]

Entre los países que se han sumado al bloqueo de esta red social están Malasia, China, Pakistán, Siria, Irán, Uzbekistán, Bangladesh y Vietnam.[35] Quienes comparten revoluciones árabes que se han suscitado con una gran convocatoria debido a estas redes.

Además, la prohibición de utilizar Youtube existe en países como Irán, Libia, China, Túnez, Turquía y Turkemeinstán. Mientras Emiratos Árabes Unidos, China y Pakistán rechazan la idea de hacerse pertenecientes al mundo de Twitter. Aunque

[33] El Econonomista publicado el 17-07-2013
http://eleconomista.com.mx/tecnociencia/2013/07/17/aumentan-10-usuarios-internet-china
[34] WEGENER, Henning, *"los riesgos económicos de la ciberguerra"* Cuadernos de estrategia, ISSN 1697-6924, Nº. 162, 2013 (Ejemplar dedicado a: La inteligencia económica de un mundo globalizado) , págs. 177-227
[35] La Jornada (10-02-2013) http://www.jornada.unam.mx/2013/02/10/mundo/021n3mun

cabe destacar, existen otros países que han bloqueado también algunas de estas comunidades informáticas por cortos periodos de tiempo como Brasil, quién durante una semana restringió el uso de Youtube en el año 2007 o Irán que prohibió el acceso a twitter durante la semana de elecciones en el 2009 y posteriormente bloqueó cualquier servicio de correo electrónico que no fuera iraní[36].

El riesgo que representan las redes sociales para los gobiernos se traduce en las oportunidades de concientizar y recibir apoyo extranjero no solo de otros gobiernos, sino de ciudadanos civiles. De este modo, se presentó en el año 1995, a partir del movimiento masivo de estos profesionales de la informática, una guerra llamada "War II", en donde se trataba de contratar hackers como una nueva forma de terrorismo por los países de baja economía mundial denominados *crackers*, que son hackers profesionales que incluso han sido entrenados por las oficinas especiales de los gobiernos para sus propósitos, pero con objetivos muy específicos que tienen la capacidad para quedarse dentro de un sistema por largos periodos de tiempo hasta lograr su meta.[37]

Por otra parte, el derecho a la obtención de información así como su intercambio se ve amenazado por los gobiernos temerosos de enfrentar su poder al de las masas informáticas. Otro ejemplo de estas revoluciones cibernéticas es el caso de los "Anonymous", quienes no se relacionan personalmente de ninguna manera, pero que realmente son personas físicas que existen detrás de los

[36] La vanguardia. Publicado el 14-05-2012 http://www.lavanguardia.com/internacional/20120514/54293901755/iran-prohibe-uso-yahoo-gmail-hotmail.html

[37] MAD, Macz, *"Internet clandestino",* Editorial Page Free Publishing inc, Estados Unidos, 2002.

monitores y pueden constituir amenazas al poder del Estado desde el punto de vista de éste. Son Hackers que navegan en busca de información de cualquier índole que les atraiga y se definen por sus convicciones personales, que para la mayoría de ellos se traduce en injusticias de los gobernantes hacia el pueblo, recolectan datos que exponen por medio de las redes sociales e incluso generan amenazas verbales por medio de videos que se colocan en Youtube. Hacen justicia colectiva por su propia mano mientras enardecen a la sociedad afectada hacia dichos funcionarios y cualquier ciudadano que consideren como amenaza a sus intereses y lo manifiestan bajo el lema “Somos Legión. No perdonamos. No olvidamos. Espérenos”.

Los hackers tienen por lo general ideales políticos y sociales que mueven sus acciones a través de una computadora. Al principio eran considerados como héroes anónimos, sin embargo, esta visión cambió y pasaron a convertirse a la vista de la sociedad, en personas apasionadas por la información que indagaban en busca y recopilación de información, pero motivados por su arrogancia y sus propios ideales filosóficos que ya no fungían como operadores de los recursos tecnológicos en aras de la información social.

Sin embargo, las motivaciones principales para delinquir también han cambiado, pues anteriormente la razón principal era adjudicada al deseo de mostrar superioridad en cuanto a su habilidad para irrumpir en sistemas computacionales, mientras actualmente la principal motivación es económica.

Estos delincuentes cibernéticos son personas cuyo conocimiento informático y técnico es tan avanzado que se han dado a la tarea de desarrollar programas con formas nuevas de procesamiento de información y comunicación electrónica para

así penetrar en *hardwares* y se dedican a hacer caer sistemas. El cracker a diferencia del hacker, se aprovecha de su conocimiento y lo produce con fines ilícitos de la información obtenida.

Es larga la lista de hackers que han dejado en claro su habilidad para penetrar en sistemas computacionales y causar revuelo en los noticieros mundiales. Uno de los más jóvenes resultó ser un chico de 15 años llamado Kim[38]. Alrededor de 152 personas se quejaron judicialmente por el contagio de 15 virus cibernéticos que Kim creó y envió por correo electrónico, pero la policía cree que al final el número subió a 2000. Kim le dijo a la policía que envió los virus para demostrar su talento y para averiguar si alguien podía desarrollar un antivirus para ellos. El vocero dijo que Kim era conocido por ser un genio en la computación desde el 7mo grado cuando aprendió a utilizar el lenguaje en código –assembly 3- el cuál 1 de cada 40 personas puede desarrollar este talento.

Por su parte, Yang Geunwon, el líder del departamento de crímenes computacionales de la Policía Nacional de Corea comentó que los creadores de virus y hackers como Kim pueden convertirse en tesoros nacionales en el futuro.

Otro hacker que se hizo famoso debido a sus habilidades en la informática es Kevin Mitnick, uno de los hackers más famosos, es un estadounidense que accedió ilegalmente a una red de sistemas digitales y fue sentenciado a prisión. Más tarde en Febrero de 1995 fue arrestado nuevamente, ésta vez el FBI lo acusó de

[38] CLARKE, Richard A.; KNAKE, Robert. *"Guerra cibernética: la próxima amenaza a la seguridad nacional y qué hacer sobre ella".* Ed. HarperCollins, 2010.

robar 20,000 números de tarjetas de crédito y fue condenado a un año de privación de libertad. [39]

Y por último, David Smith[40], un hacker que comenzó a trabajar para el FBI pocas semanas después de ser arrestado en el año de 1999 mediante el uso de una identidad falsa para localizar a hackers de diversos lugares del mundo y poder rastrearlos. Smith ayudó al gobierno de Estados Unidos y les brindó un avance en su forma de investigación y procesamiento a delincuentes cibernéticos. Ejemplo de ello, la captura de Simon Vallor[41], creador del virus *Gokar* que infectó a miles de computadoras con sistema operativo Microsoft de todo el mundo.

Muchos crackers pertenecen a la categoría de los llamados Script kiddies[42], quienes como su nombre en inglés presume, son bromistas de mal gusto que penetran sin autorización en sistemas o crean y difunden virus informáticos con la finalidad de sentirse poderosos o para jactarse con sus amigos de sus habilidades.

Además de los hackers, existen organizaciones comprometidas con la lucha de la liberación de la información de forma más pacífica como 'Reporteros sin límites', una asociación que lucha por la libertad de los medios de comunicación, quien publicó una lista de los principales países cuyo bloqueo de la información los ha hecho ser considerados como enemigos del Internet. En dicha lista figuran hasta

[39] MITNICK, Kevin D.; SIMON, William L. *"El arte de la intrusion: Las historias: Las historias reales detrás de los motivos de los hackers, intrusos y embaucadores"*. Wiley. com, 2009.
[40] Idem.
[41] The register UK nota publicada el 13-11-2002
http://www.theregister.co.uk/2002/11/13/welsh_web_designer_charged/
[42] DAVIS, Joshua. *"Los Hackers tumban el país más lleno de cables en Europa*". Revista *Wired*, 2007, vol. 15, no 9, p. 15-09.

2012, Bahrain, Bielorrusia, Burma, China, Cuba, Irán, Corea del Norte, Arabia Saudita, Siria, Turkmenistan, Uzbekistán y Vietnam.[43]

Siendo Turkmenistán[44] el principal Estado que ha prohibido y bloqueado la entrada de medios de información extranjeros que puedan conducir a la democratización de su gobierno. Su régimen proporciona a sus ciudadanos seis televisoras nacionales que pueden ser vistas, sin embargo está estrictamente prohibido el acceso de las televisoras comerciales o privadas. Así mismo, aunque existe Internet dentro de su territorio, el único proveedor del servicio es "Turkmentelcom" y del cual solo el 2.2% está conectado a este servicio que se encuentra limitado a ciertas sitios excluyendo cualquier red social como Facebook, Twitter, Youtube y recientemente en 2010 Gmail también fue bloqueado.

La aprehensión de los gobiernos y su temor de pérdida del poder ha suscitado guerras informáticas como la de Julio de 2011, el cual fue un acontecimiento importante para los ciudadanos de Turkmenistán[45]. El cielo se cubrió de bombas apuntadas a civiles dentro de sus hogares y muchas vidas fueron perdidas. Fue entonces que el sitio de Internet de RFE/RL Radio libertad, recibió comentarios de internautas comandados por Dovletmyrat Yazkuliyev. Los mensajes eran diversos y aunque el gobierno bloqueó una gran cantidad de ellos, muchos ya habían llegado a ojos extranjeros que pudieron darse cuenta de su actual situación política, lo que fue considerado como una victoria para los ciudadanos para el país de Asia Central. Sin embargo, días más tarde, el principal corresponsal fue

[43] Lista encontrada en el sitio oficial http://en.rsf.org/t
[44] Nota publicada (12-03-2013) http://en.rsf.org/turkmenistan-turkmenistan-12-03-2012,42069.html
[45] Nota publicada (16-07-2011)
http://www.rferl.org/content/citizen_journalism_scores_breakthrough_in_turkmenistan/24266428.html

sentenciado a cinco años de prisión y los otros cibernautas fueron encontrados y arrestados por un corto periodo de tiempo.[46]

Por su parte, en el mismo tenor de control gubernamental, Corea del Norte en su intento de continuar con su régimen político a raíz de la muerte de su líder, Kim Jong Un ha continuado con la denegación al acceso a Internet de los ciudadanos en territorio norcoreano. En el año 2012 éste país entró oficialmente a Internet para distribuir su propaganda acerca de una guerra entre Estados Unidos y Corea del Sur. El régimen se equipó con un ejército de hackers instruidos para destruir sitios online y practicar espionaje.

Además, países como Cuba, China y Vietnam también se han sumado a la lucha contra la conexión externa de información en sus regímenes e incluso han creado sus propios *Facebook* nacionales a los cuales solo pueden conectarse dentro de su territorio.

La lucha entre los gobiernos e Internet es implacable e impredecible. La información ha llegado a constituirse como el arma más preciada ya puede destruir y controlar a las personas. La informática ha permitido avances positivos y negativos, pero sin duda dichos avances deben de ser tratados con cautela.

[46] Ídem.

3. Delitos Informáticos

A) DEFINICIÓN

La falta de legislación específica en materia de delitos cibernéticos impide la su persecución. Los delitos informáticos son aquellos en los cuales el autor produce un daño o una intromisión no autorizada en aparatos electrónicos ajenos, y que a la fecha por regla general no se encuentren legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad física y lógica de los equipos electrónicos y la intimidad de sus propietarios.[47]

Los actores en el Derecho informático se reducen principalmente a el usuario, que es quien utiliza las redes de comunicación; el proveedor de acceso, la compañía que provee el servicio de contratación de éste servicio y el proveedor de *hosting*, que se refiere a la compañía que permite la colocación de sitios en Internet a través de su servidor.

"Internet aún está considerado como un territorio sin ley, ni límites, la digitalización es cada día mayor, y se incorporan nuevos sistemas con la realización de actividades operacionales y control en ramas tan diversas como el tráfico aéreo y el sistema bancario. El creciente mundo cibernético permite deducir que el delito informático tiende a aumentar y a diversificarse."[48]

Aunque el Derecho Informático se encuentra aún en construcción, las conductas delictivas no escapan de su comisión en un espacio abstracto que se

[47] CAMPOLI, G., *"Delitos informáticos en la legislación mexicana",* Instituto Nacional de las Ciencias Penales, México, 2005, p. 15

[48] SÁNCHEZ CURBELO, Benigno Víctor. *"Las Nuevas Tecnologías Y Los Delitos Informáticos"* Tono: Revista Técnica De La Empresa De Telecomunicaciones De Cuba, S.A 3 (2006): 14-19. Web. 6 Nov. 2013.

convierte en un daño directo ya sea moral, económico, físico, contra la propiedad, la seguridad personal e incluso que atenta contra la vida. Su integración y tipificación se encuentra incluida en los códigos penales del mundo de manera completa y escasa en otros. Sin embargo, debe aclararse primeramente la naturaleza de estos delitos cometidos a través de computadoras.

En el siguiente cuadro comparativo se sometió el análisis de tres países pioneros en regulación informática que han incorporado delitos distintos al acceso en sistemas computacionales.[49]

País	Delito	Legislación
España	Sabotaje Informático. Daño mediante la destrucción o alteración de documentos o programas.	Art. 263 Código Penal
España	Falsedad. Falsificación de tarjetas de crédito así como la fabricación o tenencia de programas que permitan cometer estos delitos.	Art. 386 Código Penal
España	Amenazas. Anuncio del mal futuro ilícito mediante cualquier medio de comunicación.	Art 169 Código Penal
España	Identidad. Castigará a quien con intención de descubrir los secretos de otro mediante cualquier medio de comunicación, así como a quien acceda por cualquier medio, utilice o modifique en perjuicio de terceros, datos reservados de carácter personal o familiar, registrados o almacenados en cualquier tipo de soporte.	Art. 197 Código Penal
Estados Unidos	Virus. Se contempla la regulación de virus y gusanos.	Acta Federal del Uso Computacional de 1994
Holanda	Phreaking. El acceso no autorizado a teléfonos o smartphones.	Ley del delito informático de 1993.

[49] Cuadro de elaboración propia.

Señala el Maestro Téllez Valdez en su obra de *Derecho informático*[50] que los delitos informáticos pueden dividirse en dos categorías. "*Primero aquellas conductas criminógenas de las que se vale la computadora.*[51]*Y en segundo lugar se encuentran aquellas conductas criminógenas cuyo fin es la computadora de forma física*[52]

Los ataques cibernéticos son invisibles, aunque a veces detectables, de bajo costo y difíciles de evaluar con respecto a sus efectos pero con resultados reales y tangibles. Su comisión representa peligro en distintas escalas desde hurtos de información variable, convocar a masas a revoluciones, hasta ataques a infraestructuras nacionales.

La delincuencia ha dado un gran salto junto con los avances tecnológicos, la seguridad cibernética no es sólida y representa pérdidas enormes a las empresas anualmente, así como para la nación y la seguridad de los usuarios comunes. Sin embargo, las organizaciones comerciales no reportan estos ilícitos debido a la imagen que representan ante potenciales consumidores. Así mismo, la Unión

[50] TELLEZ VALDEZ, Julio, "Derecho Informático", 4ta Edición, MCgraw-hill México 2009

[51] Falsificación de documentos vía computarizada; Variación de los activos y pasivos en la situación contable de las personas; Planeación o simulación de delitos convencionales; Robo de tiempo de computadora; Lectura, sustracción o copiado de información confidencial; Modificación de datos tanto en la entrada como en la salida; Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (caballo de troya); Variaciones en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la "técnica del salami"; Uso no autorizado de programas de cómputo; Introducción de instrucciones de provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios, tales como "consulta a un distribuidor"; Alteración en el funcionamiento de los sistemas a través de virus informático; Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos; Acceso a áreas informatizadas en forma no autorizada; Intervención en las líneas de comunicación de datos.

[52] Programación de instrumentos que producen un bloqueo total al sistema; Destrucción de programas por cualquier método; Daño a la memoria; Atentado físico contra la máquina o sus accesorios; Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados; Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje.

Internacional de Telecomunicaciones informa que los ataques cibernéticos a empresas aumentaron en un 30% dejando afectaciones de 110mil millones de dólares entre 2011 y 2012.[53]

La intrusión de virus en los sistemas informáticos además de ser ataques ilícitos que atentan contra la privacidad de las personas físicas o morales representa un campo amplio de pérdidas económicas. Entre los virus más dañinos de los últimos diez años se destacan: I Love You (2000) cuyo costo ascendió a los 15 billones de dólares; My Doom's (2004) del tipo gusano tuvo un costo para los usuarios en el mundo de 38 billones de dólares y; Conficker's stealthy destruction (2007) con un saldo de 9.1 billones de dólares.[54]

Las organizaciones delictivas funcionan desde dos ángulos, dependiendo del nivel informático y el seguro. Para lo cual debemos estar conscientes de la profundidad de Internet y sus niveles, por lo que la mayoría de las personas ingresamos a la red navegando únicamente en la *surface web*, es decir, el lado exterior de Internet en donde utilizamos servidores de búsqueda como Google, Yahoo, Youtube, redes sociales y cualquier página de contenido "visible" e indexado por algún motor de búsqueda. En cambio la Deep Web, es conocida como el escenario escalofriante e invisible que reúne a los grandes criminales, como pedófilos, hackers, scripters, sádicos, necrofílicos, asesinos, traficantes de personas y delincuentes de toda índole.

[53] Noticia publicada el 15 de Julio de 2013 y consultada el 18 de Octubre de 2013. http://www.eluniversal.com.mx/finanzas-cartera/2013/ciberataques-dejaron-perdidas-de-110-mil-mdd-en-2012-936111.html

[54] McAffe 2001.

La *Red Profunda o Deep Web*, es en donde se almacena aproximadamente el 96% de Internet y cuyo acceso se realiza por medios no convencionales.

Los niveles que componen Internet se dividen de la siguiente manera:

1. Primer nivel. La surface retiene todo aquello que se encuentra indexado a sitios de búsqueda tales como Google, Yahoo, Bing, entre otros. Aquellos que se encuentra de forma más visible en la web e indexable pertenece a esta categoría y representa el 4% de lo que realmente existe en la red.
2. Segundo nivel. Conocido como Bergie que almacena la información que se encuentra pérdida o abandonada y sitios como 4chan.com, pornografía y torrents.
3. Tercer nivel. Deep web propiamente, aquí comienzan a sumergirse los usuarios en territorio peligroso, en donde deben navegar utilizando un proxy por seguridad ante hackers y el mismo FBI, aquí puede encontrarse material de tipo Gore, Suicida y Hackers.
4. Cuarto Nivel. El nivel más profundo al que los usuarios pueden adentrarse y cuyo material es altamente perturbador, aquí se reúnen las mentes criminales más oscuras de la red. Comercio de armas, venta de animales exóticos, Necrofilia, Pornografía infantil, Mutilación genital, Zoofilia, Videos Snuff[55], Hackers, Armado de bombas, Hidden Wiki, Experimentos humanos, Venta de humanos, Prostitución, etc.

[55] Películas de asesinatos sin ediciones de ningún tipo.

5. Quinto nivel. Mejor conocido como Marianas web, denominada así por las fosas marianas, la más profunda del mundo y alberga aquellos sitios que no pertenecen propiamente al Internet, sino al gobierno estadounidense, trátese del Pentágono, NASA, SNA, por su contenido documental secreto y hasta el momento solo ha habido un Hacker, Gary McKinnon que logró entrar en este nivel y cuya detención fue altamente publicitada por los medios de todo el mundo[56].

Los comentarios que pueden obtenerse de personas que se han sumergido en la red profunda son diversos, generalmente usuarios jóvenes con pocos conocimientos de informática con el deseo de saber y cuyo ánimo se ve propiciado por los tutoriales que abundan en la red que muestran como accesar, así como las precauciones que deben de tomar antes de sumergirse en lo desconocido. Lo cierto es que una vez dentro, las experiencias que cuentan coinciden en lo mismo: miedo, furia, repulsión y nerviosismo.

Parte del misterio de la Deep web recae en que para llegar a ella no es posible acceder por navegadores convencionales, sino mediante un navegador llamado "TOR"[57], además de asegurarse de que su IP ha sido cambiada, cubrir sus Webcams en caso de contar con ellas y desactivar imágenes para navegar en el anonimato, pues los Hackers se encuentran al asecho de encontrar presas vulnerables.

[56] Noticia publicada el 10 de Mayo de 2006 y consultada el 27 de Septiembre de 2013 http://tecnologia.elpais.com/tecnologia/2006/05/10/actualidad/1147249681_850215.html

[57] "The onion road", es un navegador que permite el acceso a sitios en Internet que no se encuentran indexados por navegadores convencionales o populares.

Entidades de seguridad como Interpol o FBI se han encargado de patrullar y desmantelar en lo posible páginas delictivas que residen allá “abajo”, sin embargo, la barrera del anonimato es la principal causa que hace difícil la detección de los criminales.

Se anuncian como empresas en la Sección amarilla, ofreciendo servicios ilícitos con descripciones llamativas a cambio de *bitcoins*, una moneda electrónica y descentralizada que se utiliza para realizar pagos y cuyo valor equivale aproximadamente a 15USD. *El bitcoin fue introducido en el 2009, basado en una publicación de Satoshi Nakamoto y cuyo pago funciona de manera similar al efectivo en donde un vendedor a quien le entregan dinero inspecciona la moneda y con un buen grado de confianza decide si el pago es válido o inválido. La diferencia más notable es que el la validación del bitcoin puede ser comprobado*.[58]

Se estima que en México para el año 2012, la delincuencia cibernética había presentado un alza del 40% principalmente debido a los *Hacktivistas* quienes se manifestaron por medio de ataques DDoS[59], XSS[60] e inyecciones SLQ[61] dirigidos a estructuras gubernamentales creadas y empleadas específicamente para apoyar las elecciones presidenciales de julio de 2012.[62]

---

[58] MARTINS, Sergio; YANG, Yang. *“Introducción a los bitcoins: un sistema de moneda pseudo-anónimo”,* En Congreso de 2011, Conferencia del Centro de Estudios avanzados en investigación por colaboración. IBM Corp., 2011. p. 349-350. (En inglés)

[59] Ataque de denegación de servicios que hace que un sitio sea inaccesible.

[60] Cross Site Scripting se utiliza para robar información delicada.

[61] Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos. Wikipedia http://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL

[62] “*Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos”* http://www.oas.org/es/ssm/cyber/documents/OASTrendMicroLAC_SPA.pdf

"Los delincuentes cibernéticos clandestinos en América Latina recurren mucho a troyanos bancarios, en comparación con otras regiones en donde de usan otros tipos de programas maliciosos como Ransomware y ATS"[63]

B) CLASIFICACIÓN

El catálogo es amplio y se actualiza constantemente, sin embargo resaltaré en este espacio los delitos más recurrentes que son cometidos mediante los sistemas informáticos.

I. Sexting

Es una práctica común entre jóvenes, y cada vez más entre adolescentes que se refiere a la contracción de los términos *sex* y *texting*, un anglicismo de nuevo cuño para referirse al envío de contenidos eróticos o pornográficos por medio de teléfonos móviles. Comenzó haciendo referencia al envío de SMS de naturaleza sexual. No se sostiene ninguna relación y no se debe confundir el envío de vídeos de índole pornográfico con el término "Sexting". En donde el protagonista posa de forma erótica y cuyo material es difundido por el actor mismo.

Las causas negativas resultantes de estas prácticas para estas personas son las amenazas de privacidad, es decir, que otras personas vean sus fotos, las humillaciones o exclusiones sociales, extorsiones o amenazas de reproducción del

[63] *"Tendencias en la Seguridad Cibernética de los Gobiernos".* Trendmicro.com, ISBN 978-0-8270-6061-6.

material en otros medios y el principal riesgo que es la localización mediante satélites a tu lugar de ubicación.[64]

La Cámara de Diputados aprobó la reforma al Artículo 200 del Código Penal Federal, que sanciona de uno a cinco años de prisión, y de 300 a 500 días de multa a quien distribuya, comercie, exponga, haga circular o venda a menores de 18 años imágenes u objetos de carácter pornográfico reales o simulados. Esto como forma de detener la actividad de Sexting que ha seguido creciendo en nuestro país.[65]

II. Child Grooming y Pornografía infantil

Aunque este delito no tuvo sus inicios en la red (pornografía infantil), cabe destacar que es uno de los delitos más cometidos y más rechazados por la sociedad, por lo cual los pedófilos son perseguidos con especial atención por la policía. Sus actividades consisten en la distribución del material, verlo, poseerlo o producirlo.

Las operaciones destinadas a atacar la pornografía infantil mediante Internet resultan de gran interés social. En Octubre de 2011, el grupo de Anonymous lanzó una amenaza pública mediante las redes sociales con el mensaje de "borrar los videos, imágenes y links que apoyaran la distribución de pornografía infantil en sus sitios, principalmente a Hidden Wiki, Freedom Hosting y Lolita City y de no hacerlo, revelarían información personal de los usuarios"[66], lo que provocó miedo en al menos un millón de usuarios que se alojaban en dichos sitios por temor a que

[64] LENHART, Amanda. "*Adolescentes y sexting. Internet y Reporte del Proyecto sobre la vida Americana"*, Julio, 2009, vol. 4, p. 2010.
[65] Decreto de reforma consultado el 26 de Septiembre de 2013. www.hsph.harvard.edu/population/trafficking/mexico.traf.07.doc
[66] Nota del portal de noticias Huffposting http://www.huffingtonpost.com/2011/10/22/anonymous-hacks-lolita-city_n_1026327.html

revelaran su paradero al FBI. Aún así, se negaron a eliminar su material pornográfico de la Deep Web y Anonymous efectuó su amenaza al tumbar sus servidores y reveló el nombre de 1,589 usuarios pedófilos encargados de distribuir material pornográfico mediante su sitio oficial[67].

Más recientemente, en Noviembre de 2013 surgió una operación internacional con sede en Holanda a través de una organización de derechos humanos la cual creó un anzuelo tras la identidad de "Sweetie", una niña filipina de 10 años de edad fabricada virtualmente con la finalidad de identificar a más de mil pedófilos de 70 países que respondieron a la oferta de interactuar con ella a cambio de dinero.[68]

Cientos de sitios en Internet promueven la comercialización de pornografía infantil, así como son cientos las organizaciones que localizan de redes de pedófilos y los entregan a autoridades para su detención.

En conjunto con la preocupación de fortalecer la protección infantil, el childgrooming se refiere al proceso de socialización que ocurre en los casos de abusos sexuales en contra de menores, en los que el victimario interactúa y se gana su afecto para la obtención de material pornográfico mediante la amenaza, como por ejemplo, contarles a sus amigos y a sus padres de sus actividades.[69]

"El acoso sexual a menores, no es diferente del real; son individuos de mente perversa disfrazados de usuarios decentes y anónimos. Son difíciles de identificar,

[67] Noticia consultada el 15 de Agosto de 2013 http://www.huffingtonpost.com/2011/10/22/anonymous-hacks-lolita-city_n_1026327.html

[68] Noticia. El Universal. "Atrapan a más de mil pedófilos con niña virtual" martes 5 de noviembre de 2013. http://www.eluniversal.com.mx/sociedad/2013/nina-virtual-pedofilia-963336.html

[69] FERNÁNDEZ TERUELO, Javier G. *"Derecho Penal e Internet",* Ed, Lex Nova, Primera edición, España 2011. Pág 153

de rastrear y de capturar a esos individuos. Desafortunadamente las leyes en contra de los acosadores se encuentran en escenario joven. Las agencias de seguridad no se encuentran completamente capacitadas para esto. Los ciber-acosadores obtienen a sus víctimas potenciales a través de Facebook, biografías y sitios familiares. Es responsabilidad de los padres y maestros educar a los niños acerca de los peligros de los acosadores cibernéticos".[70]

III. Ciberbullying

Este ocurre cuando una persona utiliza un medio electrónico para avergonzar, amenazar, acosar, intimidar, amenazar o causar algún daño directo a una persona. [71] Es un tipo delictivo que nace principalmente en las redes sociales, ya sea tras el anonimato o no y frecuentemente resalta entre jóvenes o adolescentes quienes se burlan de sus compañeros. Ésta práctica puede quedar en las burlas e incluso puede ser tan traumatizante para quien lo recibe que puede conducirlo al suicidio.

IV. Phishing

Se trata de la suplantación de sitios en Internet, que alude a la acción de "pescar", es la forma en que estos sitios falsos son colgados como anzuelos que aparentan ser instituciones de confianza como bancos o entidades financieras que son diseñadas para embaucar a los usuarios para obtener su información

[70] Hussain, Rashid. *"Fuerzas especiales del Ciberespacio para la protección infantil"* Revista Internacional de la Academia de investigación 3.2 (2011): 1001-1007. Consulta académica Web. 6 Nov. 2013. (Inglés)
[71] MC QUADE, Samuel C. *"Cyberbullying",* Librería del Congresos, Primera edición, Estados Unidos, 2009, Pág. 2

confidencial. El sitio intenta recoger estos datos al mostrar mensajes como “Por motivos de seguridad…” indicándole al usuario que teclee sus datos personales.[72]

Otra forma de caer en el Phishing, se realiza cuando recibimos correos electrónicos en nuestro buzón de invitaciones que hacen nuestros amigos para que nos unamos a un sitio web o que hemos recibido una postal falsa, y es aquí cuando se vuelve peligroso pues en el momento en que demos *click* se ejecutará un archivo que se instalará en nuestro equipo que puede ser un virus o un *keylogger*.

Recientemente un estudio realizado por una empresa de Estados Unidos arrojó que, durante el 2012 y principios de 2013, 37.3 millones de usuarios alrededor del mundo fueron sujetos a ataques de Phishing notando un aumento del 87% desde el 2011.[73]

V. Scam

Mejor conocido como fraudes, son todas aquellas actividades en las que se engañe a una persona mediante el uso de una computadora[74]. Tales fraudes representan diferentes gravedades según el caso concreto siempre y cuando el fin sea el de obtener un lucro.

El fraude cibernético, es otro de los delitos que ha evolucionado a la par de la informática como canal mediante el cual su comisión es posible.

---

[72] Recovery Labs, *“Fraude en internet: del phishing al pharming”* consultado el 16 de Octubre de 2013 http://www.recoverylabs.com/informes/Recovery_Labs_pharming.pdf

[73] Ver el estudio de Kapersky Lab http://media.kaspersky.com/pdf/Kaspersky_Lab_KSN_report_The_Evolution_of_Phishing_Attacks_2011-2013.pdf

[74] STAJANO, Frank; WILSON, Paul. *“Entendimiento a las víctimas del Scam: siete principios para los sitemas de seguridad”*. Communications of the ACM, 2011, vol. 54, no 3, p. 70-75.

La forma más común de este delito, es la venta de acciones o de objetos, en los que los defraudadores se encuentran al asecho en sitios de Internet o en salas de chats para hacer su mejor actuación e intentar por sus medios de convencimiento la realización de una "venta" fantasma[75].

VI. Robo de identidad

Es uno de los ilícitos más cometidos gracias a la cantidad de información que arrojamos a la red. Los hackers utilizan esta información para lucrar con ella de la forma en que les sea más conveniente, es así que pueden sustraer información de redes sociales mediante el hackeo de sus cuentas personales, el robo de bases de datos de empresas bancarias, de instituciones gubernamentales y todas aquellas de donde el contenido pueda aprovecharse, así como la entrada de intrusos en los ordenadores personales en busca de contraseñas, números bancarios o documentos importantes.

Es una actividad difícil de definir debido a su amplitud se presenta cuando alguien posee o adquiere información de una persona física o jurídica de forma no autorizada con la intención de cometer fraude u otros delitos a través de Internet.[76]

La forma más común de identificar el robo de identidad es cuando otra persona obtiene su número se seguridad social, el número de su licencia de conducir, fecha de nacimiento y los utiliza para abrir una cuenta de banco

[75] CHARNEY, Scott; ALEXANDER, Kent. *"Crimenes de computadora*". Emory LJ, 1996, vol. 45, p. 931.
[76]JIMENEZ, Enríquez, *"El robo de identidad, nuevo reto para el derecho del siglo XXI",* Revista Abogacía consultada el 11 de Octubre de 2013. http://www.abogacia.es/wp-content/abogados/ficheros/1331025558756.pdf

fraudulenta , una tarjeta de crédito, un número celular o cualquier cuenta para obtener falsos beneficios.

El robo de identidad más común de tipo no financiero ocurre cuando alguien le da a otra persona información personal como un policía cuando le han arrestado. Además, como daño resultado de este delito, la persona cuya información fue robada tendrá una historia crediticia errónea que cuesta horas dedicadas a hacer trámites para corregirla.[77]

VII. Spam

La Comisión Europea emitió un reporte titulado Comunicaciones Comerciales No Solicitadas y Protección de Datos[78], en el cual define el Spam como el envío masivo y repetitivo de mensajes comerciales no solicitadas por un remitente que oculta o disfraza su identidad.

Los resultados más perjudiciales del Spam son[79]:

a) Daño a la productividad
b) Daño de la competitividad de las empresas
c) Daño a la infraestructura informática
d) Pérdida de recursos por lo que se paga
e) Pagar publicidad que no se solicitó
f) Pérdida de información por combate

---

[77] *"Robo de identidad"* 2013, Enciclopedia Electrónica de Columbia, 6ta Edición, p. 1, EBSCOhost, consultada 16 Octubre 2013.
[78] GAUTHRONET, Serge; DROUARD, Etienne. *"Comerciales no solicitados y protección de datos"* Comisión de la Comunicación Europea, 2001. (Inglés)
[79] FONSECA MARTINEZ, Claudia, *¿Qué es el Spam y por qué existe?* "El SPAM y su impacto" Foro Cofetel 3 de Marzo de 2005 www.cofetel.gob.mx/foro_spam.shtml

g) Traslado de costos de combate por ISPs

h) Costos por ancho de banda

i) Costos en inversión para herramientas para su combate

j) Costos en imagen

k) Servicios de telecomunicación menos afines

l) Costos de servicios de telecomunicaciones más efectivos

m) Mayor incidentes de Spim

C) PERFIL DE LOS HACKERS

El punto de vista social que prevalece sobre los hackers cotidianamente es que son personas antisociales y marginadas que pasan todo su tiempo desarrollando programas que les permiten causar daños o beneficios sociales. Generalmente su motivación se basa en la sola capacidad de demostración de sus habilidades informáticas frente a otros hackers. Otro tipo de motivación es la económica y finalmente la activista.

Bill Gates, es un claro ejemplo de un hacker cuya motivación fue económica, se convirtió uno de los empresarios más ricos del mundo cuando fundó Microsoft siendo un hacker debido a la pasión que sentía por la programación computacional, la cual hasta la fecha se considera como la compañía líder en el mercado mundial de la computación.

Los Hacktivistas, (conformado por los términos *hackers* y *activistas)* son personas que se dedican a hacer hacking, phreaking[80] o crear tecnología para conseguir un objetivo político o social por el que luchan en un mundo virtual esperando resultados en un mundo material.[81]

La World Wide Web, es tanto benéfica como perjudicial y el resultado depende su utilización, el anonimato es un arma de doble filo, pues si bien nos permite proteger nuestra identidad para evitar ser víctimas, también los criminales lo utilizan para ganar la confianza o atacar sin ser detectados.

El anonimato también les permite a las personas emitir opiniones sin ser juzgados. Representa una máscara que los usuarios se coloquen en Internet para hablar o compartir sin censura.

En el año de 2006 surge WikiLeaks, fundada por Julian Assange, quien identifica a su organización como un sitio encargado de publicar documentos de interés público que mantiene las fuentes de información de manera anónima. Este sitio ha sido foco de controversia internacional debido al contenido de la información que se publica ahí, especialmente en el ámbito político y que ha desatado la furia de las naciones a las que se refieren los documentos y que han acusado a su fundador legalmente por revelar secretos de Estado, que ponen en peligro la integridad y seguridad de los Estados y sus ciudadanos.[82]

[80] Personas con amplios conocimientos en telefonía.
[81] VICENTE, Loreto, "¿Movimientos sociales en la red? Los hacktivistas" Revista El cotidiano, México, consultada el 16 de Octubre de 2013 http://www.elcotidianoenlinea.com.mx/pdf/12615.pdf
[82] Sitio oficial de WikiLeaks http://wikileaks.org/

Estados Unidos, se ha convertido el principal enemigo de Wikileaks e incluso en el pentágono se dispuso un equipo de 120 personas para vigilar y frenar los efectos de las filtraciones de Wikileaks[83] al sentirse amenazados por la importancia de la información, especialmente debido a los efectos que pueden sufrir directamente gracias a los 250,000 documentos que dijeron tener en su poder acerca de la guerra en Afganistán y que las oficinas del Pentágono advirtieron en su momento se detuvieran de mostrar tal información. Así mismo, otras figuras importantes de la política se pronunciaron en contra del movimiento Assange y compararon su detención con la de grupos terroristas como Al Qaeda. De esta forma, solicitaron su ejecución inmediata junto con la de los demás miembros encargados de filtrar la información en Wikileaks. Debido a la cantidad de amenazas de muerte hacia su persona, Assange ha señalado que en caso de ocurrirle algo, los Estados debían prepararse para "tirar de la manta", esto debido a que ha colgado en una conocida web de intercambio P2P un archivo cifrado de 1.38 GB, cargado de documentos secretos mucho más incendiarios y comprometedores que los ya filtrados y del cual él solo conoce la contraseña.[84]

Anonymous como principal grupo de hacktivistas tuvo su origen en los dominios de 4chan en 2008[85], un sito que aloja el intercambio de imágenes ya sea de manera anónima o mediante una cuenta privada. En él surgieron hackers que

[83] Noticia publicada el 12 de Septiembre de 2010 y consultada el 21 de Octubre de 2013 http://www.thedailybeast.com/articles/2010/09/12/pentagons-wikileaks-war-room-readies-for-new-document-dump.html

[84] ABC (5 de Diciembre de 2010) "Assange hace circular por la red un archivo de seguridad cifrado" Consultado el 14 de Octubre de 2013 http://www.abc.es/20101205/internacional/rc-assange-hace-circular-internet-201012051150.html

[85] Película "We are Legion" dirigida por Brian Knnapenberger Sitio oficial en inglés http://wearelegionthedocumentary.com/about-the-film/

encontraron fascinante la idea de operar mediante el anonimato para defender sus posturas ante las situaciones que en ese momento se estaban suscitando como la polémica reacción ante un video que fue sustraído de la iglesia de la Cienciología en donde aparece el actor estadounidense Tom Cruise hablando en una entrevista para los seguidores de la iglesia cuyos comentarios fueron mal vistos por muchos internautas e incluso noticieros locales. Posteriormente, surgió el proyecto Chanology[86] en el cual se hizo una convocatoria mediante un video en donde por primera vez surgieron con el nombre de Anonymous, para que aquellos que vieran el video se unieran a sus ideas de acabar con la iglesia de la cienciología, de forma en que levantarían una protesta afuera de las instalaciones religiosas en cada ciudad en donde tuvieran residencia y les pidieron que se cubrieran el rostro –de aquí sale la idea usar la máscara de la película V de venganza- para que no fueran identificados con facilidad. Y así lo hicieron el día 10 de Febrero de 2008 en ciudades como Londres, Los Ángeles, Sídney, Australia, Toronto, Dublín, Texas, Dallas, Florida, Boston, Seattle, Washington, entre otras, reuniendo a más de 7,000 personas enmascaradas.[87]

Cabe destacar, que a través de sus actividades como grupo anónimo, la policía ha hecho arrestos de algunos de sus miembros en las que destacan las de Deric Loustutter, Bradley Menning y Barret Brown. El primero, un joven de 26 años que vivía en una granja, con un trabajo normal y su hobby de músico de rap era lo

[86] LANDERS, Chris (25 de Enero de 2008). "El Internet está yendo a la guerra". Periódico de la Ciudad de Baltimore Publicado 2008-01-25. Consultado el 15 de Octubre de 2013. http://blogs.citypaper.com/?s=The+Internets+Are+Going+to+War

[87] Examiner (23-08-2013) consultad 28 de Agosto de 2013 http://www.examiner.com/article/anonymous-trolls-fbi-releases-contact-data-for-all-fed-employees

que se conocía de él. Dicho arresto surge debido a un caso de violación en el que dos jóvenes de un equipo de fútbol secundariano aprovechan el estado de embriaguez de una joven para abusar sexualmente de ella. Loustutter en aquel momento siente que no hay justicia para la chica y que al no contar con evidencias suficientes y que la fiscalía desecharía el caso, lanza un video amenazando a estos dos chicos de que de no disculparse con la chica haría públicas unas fotografías de ellos, así como imágenes de Twitter de sus conversaciones en donde estos jóvenes se burlan de la víctima por los eventos ocurridos.[88] Deric cumplió sus amenazas y el caso se resuelve ante la Corte de Justicia, sin embargo, al mismo tiempo, la policía rastrea a Loustutter e irrumpen en su casa para preceder a detenerlo alegando su participación en el grupo Anonymous y descubren su identidad.[89]

Barret Brown es otro ejemplo de los arrestos a miembros de este grupo, fue reportero de Vanity Fair y cuyo adentramiento en el mundo de los hackers fue de aproximadamente dos años. Admitió haber participado de forma activa y central en movimientos como el de Túnez, aunque también afirmó que no estaba de acuerdo con ciertas cuestiones como las revelaciones de números de tarjetas de crédito. A él se atribuyó su participación como portavoz oficial de Anonymous lo cuál negó y señaló que no es así como ellos desarrollan sus funciones. Su arresto se llevó a cabo en el interior de su residencia mientras realizaba un chat de video online, en el cual puede escucharse como es que él es detenido y sometido por el FBI. Un mes después de su arresto, Brown publica un video, esta vez desenmascarado, en

[88] El diario NY (3-01-2013) consultado 21 de Octubre de 2013)
[89] The daily beast (19-10-2013) consultado 21 de Octubre de 2013
http://www.thedailybeast.com/articles/2013/10/19/anonymous-maryville-and-the-new-vigilantism.html

donde amenaza públicamente al FBI y a sus familiares. Además, el grupo que lo respalda revela una lista de los nombres de los trece agentes del FBI que participaron en su detención junto con sus respectivas direcciones y números de tarjetas de crédito con lo cual se mofan diciendo que van a gastar mucho dinero de sus cuentas bancarias e incluso "comprarían flores para mandárselas a Brown". Su caso aún sigue sin ser resuelto, puesto que la competencia recae en una Juez cuyo marido ha sido afectado por las revelaciones que alguna vez hizo Barret de diversos documentos confidenciales.[90]

Otra de las grandes atribuciones de éste importante grupo son, el ataque DDoS a los sitios de Paypal, Visa y Mastercard, cuando éstos se negaron a recibir pagos para hacer donaciones a WikiLeaks. Además resalta su participación cibernética en contra de un Estado como Túnez. Esta nación durante el año 2011 prohibió el acceso a WikiLeaks para sus ciudadanos lo que hizo enfurecer a Anonymous, ya que esta acción se contraponía a su idea de la libre información y lanzaron un ataque *DDoS* a ocho sitios del gobierno.

Y la más importante revolución cibernética que enfrentaron en contra de un Estado, sucedió en el mismo año cuando Mubarack[91] se encontraba en plena revolución política en Egipto y cuyos ciudadanos se negaban a reconocerlo como presidente mediante manifestaciones y enfrentamientos ante la autoridad. Los egipcios hicieron uso de las redes sociales para informar a los Estados extranjeros lo que estaba pasando en tiempo real mayormente por medio de Twitter, así fue

[90] El diario español (05-10-2013) http://www.eldiario.es/turing/Hackers-tubo_0_174982681.html
[91] OLSON, PARMY. "Anonymous, Las armas falsas virtuales y militares. 2011.

como fotografías y videos eran vistos alrededor del mundo que mostraban el régimen de opresión que se encontraban viviendo y fueron apoyados por Anonymous, de forma que hicieron caer los sitios gubernamentales, a lo cual el gobierno contra atacó con la caída completa de Internet en todo Egipto, sin embargo, los *hacktivistas* ayudaron a restablecer la comunicación de los ciudadanos mediante el envío de faxes en los que les enseñaban a utilizar módems y radios austeros para restablecer su comunicación, además de enviarles imágenes descriptivas y traducidas al árabe sobre cómo protegerse de proyectiles de gas.

En nuestro país también existe una sede para los Hacktivistas cuyos ataques han sido dirigidos al IFE por el supuesto fraude electoral de 2012, mensajes de amenaza a Peña Nieto, Tv Azteca y Televisa. Además se enfrentaron al Cartel de los Zetas en 2011 luego de que miembros de esta organización delictiva secuestraran a un miembro de Anonymous mientras se encontraba en medio de una protesta en las calles de Veracruz. El grupo hacktivista lanzó un video amenazando con la revelación de miembros del cártel entre los que figuraban policías, taxistas y políticos en caso de seguir privando de la libertad al joven. Los zetas liberaron a su víctima el 4 de noviembre de 2011 junto con la amenaza de que por cada nombre que saliera a la luz, ellos matarían a diez ciudadanos civiles, lo cual ató de manos y pies a Anonymous y desistieron de su proyecto “OpCartel”.

No solo los Hackers son los delincuentes informáticos que se alojan en la inmensidad de la red. Las personas que aún sin tener conocimientos informáticos son capaces de ser persuadidos para realizar actos violentos mediante el contacto a través de sitios web como el caso que se presentó en Ucrania en el año 2007 cuando dos varones de 19 años fueron acusados de cometer 21 asesinatos

registrados en video y colgados en Internet convirtiéndose rápidamente en el video más impresionante de la red. El motivo que los incitó a realizar estos asesinatos según la novia de uno de ellos, fue que un sujeto dueño de una página web les dijo que les pagaría una gran cantidad de dinero una vez que tuvieran grabados 40 asesinatos snuff. [92]

La delincuencia cibernética se encuentra inmersa en un caos informático que puede ser observada desde cualquier punto del mundo. Las ciberguerras están ocurriendo, los delitos derivados de Internet se disparan y la información se encuentra vulnerable de ser alcanzada por manos equivocadas.

D) Legislación Mexicana sobre delitos informáticos

Es innegable la existencia de legislación en México sobre derecho informático, no obstante, aquella que recoge las tipificaciones delictuosas de carácter informático es escaza.

Comercio Electrónico

- Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público - 04/01/2000
- Ley de Obras Públicas -04/01/2000
- Reformas al Código de Comercio - 29/05/2000
- Reformas al Código Civil - 29/05/2000
- Reformas a la Ley Federal de Protección al Consumidor - 29/05/2000

[92] UNIAN(24-07-10) consultado el 18 de Septiembre de 2013 (inglés) http://www.unian.info/news/204617-three-19-year-old-youths-committed-19-murders-in-dnipropetrovsk-during-a-month.html

- Reformas al Código Federal de Procedimientos Civiles - 29/05/2000
- Ley Federal de Procedimiento Administrativo -30/05/2000
- Acuerdo que establece los lineamientos para la operación del Registro Público de Comercio - Sistema Integral de Gestión Registral - 08/09/2000
- Ley de Sociedades de Inversión -04/06/2001
- Norma Oficial NOM 151-SCFI 2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de los mensajes de datos - 04/06/2002
- Protocolo de Comunicación de la IES -08/2003
- Código Fiscal de la Federación -05/01/2004
- Ley Federal de Protección al Consumidor -04/02/2004
- Acuerdo 43/2004 del Instituto Mexicano del Seguro Social -03/03/2004
- Reglamento del Código de Comercio sobre Prestadores de Servicios de Certificación -19/07/2004
- Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación - 10/08/2004
- Reglamento de la Ley Federal de Protección al Consumidor- 03/08/2006
- Reforma de la Ley Federal de Protección al Consumidor -29/01/2009
- Acuerdo de 27 de febrero de 2012, por el que se dan a conocer las Reglas Generales para la gestión de trámites a través de medios de comunicación electrónica presentados ante la Secretaría de Gobernación. (DFO 9 de marzo de 2012)

Firma electrónica

- Infraestructura Extendida de Seguridad (IES) (Banco de México)
- Circular Telefax 1/2002, de 2 de enero de 2002
- Circular Telefax 19/2002, de 5 de julio de 2002
- Circular Telefax 19/2002 bis, de 11 de julio de 2003
- Protocolo de Comunicación de la IES -08/2003
- Reformas al Código de Comercio -28/08/2003
- Código Fiscal de la Federación -05/01/2004
- Resolución Modificaciones a la Resolución Miscelánea Fiscal -31/05/2004
- Leyes sobre el uso de medios electrónicos y firma electrónica de los diversos Estados
- Autorización otorgada al Servicio de Administración Tributaria para actuar como prestador de Servicios de Certificación -21/09/2004
- Circular Telefax 6/2005, de 15 de marzo de 2005
- Circular Telefax 6/2005 bis, de 15 de marzo de 2005
- Decreto por el que se expide la Ley de Firma Electrónica del Distrito Federal de 30 de octubre de 2009
- Proyecto de ley de firma digital de 27 de enero de 2010
- Decreto por el que se expide la Ley de Firma Electrónica Avanzada de 24 noviembre 2011 (D.O.F. 11/01/2012)
- Acuerdo de 27 de febrero de 2012, por el que se dan a conocer las Reglas Generales para la gestión de trámites a través de medios de comunicación electrónica presentados ante la Secretaría de Gobernación. (DFO 09/03/2012)

Protección de Datos Personales

- Ley para regular las Sociedades de Información Crediticia - 27/12/2001 (Diario Oficial de la Federación, 17 de enero 2002)
- Propuesta de iniciativa de Ley Federal de Protección de Datos Personales - 14/02/2001
- Propuesta de reformas al Art. 16 constitucional en materia de protección de datos personales - 21/02/2001
- Ley de Protección de Datos Distrito Federal, -26/08/2008 (Gaceta Oficial del Distrito Federal nº 434, 3 octubre 2008)
- Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo de la Ley Federal de Transparencia y Acceso a la información Pública Gubernamental - 27/04/2010 (Diario Oficial de la Federación, 5 de julio 2010).
- Leyes de Protección de Datos de los Estados Mexicanos
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares -19/12/2011 (Diario Oficial de la Federación, 21 diciembre 2011)

Derecho a la Información

- Art. 6 Constitucional
- Leyes de Acceso a la Información Pública de los Estados Mexicanos

- Reglamentos de las Leyes de Acceso a la Información Pública de los Estados Mexicanos
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental - 30/04/2002
- Decreto de 20 de diciembre de 2012, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Diario Oficial de la Federación de 24 de diciembre de 2002)
- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental - 10/06/2003
- Ley de Transparencia y Acceso a la Información Pública del Distrito Federal de México - 26/02/2008 (Gaceta Oficial del Distrito Federal nº 302 de 28 marzo 2008)
- Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos (Instituto Federal de Acceso a la Información y Protección de Datos) (Diario Oficial, Lunes 29 de Octubre de 2012).

Violación de la correspondencia

- Art. 173 al 177 del Código Penal

Revelación de Secretos

- Art. 210 al 211 bis del Código Penal

  Acceso ilícito a sistemas y equipos de informática
- Art. 211 bis 1 al 211 bis 7 del Código Penal

Proyecto en Decreto que reforma y adiciona diversas disposiciones al Código Penal Federal en materia de Delitos en contra de medios o sistemas informáticos, de 15 de febrero de 2012

Derechos de Autor

- Del Derecho de autor
- De la protección al derecho de autor
- De los programas de computación y las bases de datos
- Infracciones en materia de derecho de autor
- Art. 424 al 429 del Código Penal
- Reglamento de la Ley Federal de Derecho de Autor -15/05/1998.

Ley de Propiedad Industrial

- De los secretos industriales
- De las marcas
- De los esquemas de trazado de circuitos integrados
- De las sanciones y delitos

Ley del Mercado de Valores

- Registro de Valores
- Contratación y Contabilidad Bursátil

Telecomunicaciones

- Ley Federal de Telecomunicaciones -07/06/1995

En cuanto a la legislación acerca de la persecución de delitos informáticos encontramos su tipificación en el Código Penal Federal, con reformas publicadas el 17 de Mayo de 1999 en el Diario Oficial de la Federación dentro del Título Noveno del Código Penal Federal, al que se denominó "Revelación de secretos y Acceso Ilícito a Sistemas y Equipos de Informática".[93]

[93] ***Artículo 211 bis 1.-*** *Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.
Artículo 211 bis 2.- *Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.
Artículo 211 bis 3.- *Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.*
Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.
A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público. En una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.
Artículo 211 bis 4.- *Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.*

En los supuestos formulados, encuentro que aunque el capítulo del Código Penal Federal como bien describe, únicamente hace referencia a intrusiones en sistemas computacionales, cabe resaltar dos situaciones. La primera, que las penas se aumentan triplemente al tratarse de intrusiones en sistemas del Estado y seguridad pública comparado con los sistemas informáticos de los ciudadanos. Y la segunda, la inexistencia de las nuevas figuras delictivas que se consideran como una amenaza social, que no pueden ser adecuadas a ningún tipo penal positivo como el *Child grooming* o el *Phishing,* y aquellas que sí pueden adecuarse mediante la actualización de los supuestos ya existentes como el *Scam* o fraude informático, *Phreaking*, Robo de identidad en la red, Amenazas en redes sociales, Homicidios, Secuestros, etc, sino que son propias de Internet o de sistemas informáticos.

Por su parte, el Estado de Veracruz con ánimo de proteger su seguridad informática introduce en el año 2004 dentro de su Código Penal el supuesto sobre delitos informáticos justificado por el avance de las tecnologías (Artículo 181). Sin embargo su probanza aún está lejos de ser efectiva, pues hasta el año 2010 sólo

---

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

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

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

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

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

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

se había comprobado la existencia en juicio de un solo delito informático en sus seis años de vigencia[94].

Así mismo, cabe señalar que es el Estado del país que se encuentra en mayor avance en el rubro informático, de tal forma que el 10 de Octubre de 2013 se aprobó en el Pleno del Congreso de Veracruz[95] la reforma legal para crear la figura de la Policía Científica Preventiva encargada de combatir los delitos en la web. Y más transcendental aún, la reforma que dio lugar a tipificar un nuevo delito informático conocido como *Child Grooming*:

"Se sancionará de 10 a 20 años de cárcel y multa de hasta 700 días de salario a quien mediante el uso de internet, telefonía o cualquier otra tecnología de la información y la comunicación hubiese contactado y propuesto un encuentro a un menor de edad."

[94] ***Artículo 181.-*** *Comete delito informático quien sin derecho y con perjuicio de terceros:*
¡.Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar o alterar o reproducir la información en ellas contenida.
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.
Al responsable de este delito se le impondrán de seis meses a dos años de prisión y multa hasta de trescientos días de salario. Si se cometiere con fines de lucro las penas se incrementarán en una mitad.
[95]Nota de El Universal Veracruz publicada el 09-10-2013 http://www.eluniversalveracruz.com.mx/seguridad-veracruz/2013/aprueban-policia-cibernetica-contra-pornografia-infantil--19290.html

4. Evidencia Digital

A) RECOPILACIÓN DE EVIDENCIA DIGITAL

La carencia de guías de entrenamiento policiaco para recabar evidencia digital dificulta su aceptación en juicio como medio probatorio confiable. De acuerdo con la problemática tecnológica de carácter delictuosa, la forma de probanza de la misma debe concordar con el que le dio origen a la conducta antisocial.

La evidencia de tipo digital requiere de una comprensión desde el punto de vista jurídico como la manera de probar que se ha cometido un delito mediante el uso de un sistema informático. Se incluyen computadoras, audios digitales, videos digitales, celulares o smartphones, máquinas de fax digitales, discos duros, documentos creados en computadoras, etc. los cuales deben ser examinados con detalle y cuidado de no perder o distorsionar la información contenida en ellos.

Existen tres formas de clasificar la evidencia digital que puede ser analizada por especialistas y creada por usuarios o por los sistemas mismos.

I. Documentos almacenados (correos electrónicos, documentos Word, PDF).

II. Documentos generados por computadoras. Aquellos que no contienen datos creados por humanos, sino que son generados a partir de un procesamiento computacional seguidos de un algoritmo definido. (Server log in records).

III. Documentos mixtos. Son la combinación de los dos anteriores, es decir, con datos introducidos por humanos junto con un procesamiento del sistema. (Hoja de cálculo).

Para realizar un análisis de datos confiables, la provincia de Nequén, desarrolló una metodología de investigación que consta de cuatro pasos que me parecen pertinentes: Identificación, Preservación, Análisis y Presentación.

La *identificación* es esencial para describir al delito informático, es decir, poder decir y saber si ha habido una intrusión al sistema informático; en segundo lugar, la preservación de la evidencia digital es una pieza clave para respaldar su *fiabilidad*, debido a que quienes transportan el material informático no tienen cuidados reales, como los deberían tener en el caso de armas, documentos físicos, etc., hay que tener claro, que su información probatoria puede perderse o modificarse con el mínimo toque físico, es por esto que la Cadena de Custodia es Primordial para su resguardo que debe ser debidamente documentado. En tercer lugar, el *análisis* debe realizarse con pericia experta, se trata de la parte medular del proceso, en donde hay que emplear los conocimientos informático-jurídicos en la información que resulte relevante para el caso concreto. Por ejemplo, documentos en Word, hojas de cálculo, palabras claves, fotografías o videos dentro del sistema, así como las búsquedas realizadas en la web que puedan dar indicios de delito, incluso las *Cookies,* que permiten saber lo que piensa la persona mediante su historial de navegación por Internet, etc., Y por último, la *presentación* de un informe pericial sobre lo que se logró extraer del sistema que sea pertinente a presentarse en un juicio.

De acuerdo con Cano[96], los investigadores forenses deben cumplir con ciertos requisitos básicos que garantizarán el manejo efectivo de la ED:

[96] CANO, J. Informática forense, liderando las investigaciones. Portal de Seguridad viruspot: www.viruspot.com/Col8.html, 2001.

1. Usar medios forenses estériles para copias de información.
2. Mantenimiento y control de la integridad original.
3. Etiquetar, controlar y transmitir de forma adecuada las copias de los datos, imprecisiones y resultado de la investigación.

Debido a que cualquier objeto digital sin protección es objeto de un ataque informático, su protección debe estar actualizándose de manera constante.

Alrededor del mundo, existen diversas guías que desarrollan los pasos para llevar a cabo investigaciones exitosas en el manejo de información digital.

- RFC 3227 (Guidelines for evidence collection and archiving, 2002)
- Guía de la IOCE (Guidelines for the best practices in the forensic examination)
- ISFS (Information security and Forensic Society, Hong Kong)
- Investigación de la escena del crimen electrónico. Una guía para la respuesta inmediata, Departamento de Justicia de Estados Unidos.
- ACPO, Asociación de Oficiales de Policía. Guía de buenas prácticas para evidencia basada en computadoras.
- Guía para el manejo de evidencia en IT, 2003, Reino Unido.

En México, existen manuales que sirven como guías para controlar las acciones que deberían desarrollar los miembros oficiales de los cuerpos policiacos como el "Manual básico del policía preventivo"[97] de la Secretaría de Seguridad Pública, en cuyo índice se desglosan las facultades entre las que destacan: Patrullaje, Revisión, Detención, Uso de la fuerza, Preservación del lugar de los

[97] Manual básico del policía preventivo de la Seguridad de Seguridad Pública, México, 2009. http://media1.webgarden.es/files/media1:4c9bfe11eaf2c.pdf.upl/Manual%20Basico%20del%20Policia%20Preventivo.pdf

hechos, Violencia Familiar, Violencia en la Comunidad, Protección Civil, Parte informativo, Primeros Auxilios y Armamento. Sin embrago, se omite los pasos que deben seguir para recopilar evidencia a excepción de armas.

En el Protocolo de cadena de custodia publicado por Setec en su apartado 8 "Levantamiento de evidencia e indicio"[98], cuyo contenido se basa en los Manuales de procedimientos de fiscalía del Sistema Penal Acusatorio de Colombia, se enumeran algunos pasos a seguir en el momento de investigar una escena de crimen y cómo habrá de procederse con respecto a la recopilación de evidencia. Si bien, dichas reglas se pueden aplicar a casos de homicidio, robos y delitos comunes, pues se basa en el manejo de evidencia de tipo biológica principalmente, huellas de herramientas, armas, polvos metálicos o indicios orgánicos en frascos.

B) LA EVIDENCIA DIGITAL COMO MEDIO DE PRUEBA EN JUICIO

El tratamiento de este tipo de evidencia ha sido duramente criticado por sus opositores quienes afirman que no puede ser confiable su utilización en juicio debido a su naturaleza volátil y fácil de modificar. Sin embargo, el término evidencia sugiere que la colección de la misma es reconocida por los juzgados o tribunales y su presentación es esencial en juicio.

Pero, ¿Cuáles son las causas que hacen que la evidencia digital no sea considerada como fuente confiable? Principalmente el recurso humano y su desconocimiento en informática de primera fuente para recolectar la evidencia sin seguir una rigurosa metodología para el tratamiento del sistema.

[98] Mecanismo de Protección y Preservación de Evidencia, Cadena de Custodia, Secretaría de Gobernación, 2012. http://www.setec.gob.mx/work/models/SETEC/PDF/CadenaCustodia3.pdf

Señala Téllez[99] que *por lo que respecta a la valoración de las pruebas de los sistemas de cómputo, a las cuales se han hecho referencia, el juzgador deberá cumplir con la hermenéutica jurídica y con un análisis profundo, (…)en caso de que el juzgador no se encuentre convencido de darle valor a la prueba de cómputo que le es presentada y desahogada, deberá establecerlo sin temor alguno, ya que el perfeccionamiento de la computación como medio de prueba dependerá de su aplicación diaria en las relaciones procesales de las partes y el juzgador, al presentarse como medios de convicción diaria en las relaciones procesales de las partes y el juzgador al presentarse como medio de prueba.*

En el derecho comparado, hay que resaltar el nivel de importancia que toma la evidencia digital en países como el de Estados Unidos en donde se presentó un caso en la ciudad de Nueva York, en donde un ex empleado de la compañía *USB Paine Webber* inconforme por el pago de un bono menor a lo que esperaba, se armó de valor para lanzar una "bomba lógica" en el sistema de red de la compañía lo que resultó en pérdidas millonarias para la misma. Lo importante de este caso, es que las pruebas que recabaron entre los testimoniales de los empleados junto con la denuncia de los apoderados legales de la empresa, las más importantes fueron constituidas por los Agentes del Servicio Secreto de los Estados Unidos de Norteamérica especializados en materia de crímenes electrónicos[100]

Mientras en México, los medios de prueba digitales se introdujeron en los códigos de manera sutil, más no como una necesidad imperante en la que había de

[99] Op. Cit.
[100] Delitos informáticos en el Estado de Veracruz

estudiarse el Derecho Informático, sino como la evolución de los medios probatorios ajustados a la nueva época que encontraron su pertinencia en juicio.

El 29 de Mayo de 2000, se reformaron y adicionaron artículos a los Códigos Procesal Civil del Distrito Federal y de la Federación, en los que señalan su admisibilidad en materia de contratos y comercio electrónico.[101]

La Suprema Corte de Justicia de la Nación, por su parte ha emitido interpretaciones mediante jurisprudencia acerca de la valoración de pruebas digitales. Es así, que la tesis aislada número 11.1º.A.21 K página 1205, XXI, Marzo, 2005, Novena Época, Tribunal Colegiado de Circuito publicada en el Semanario Judicial de la Federación bajo el rubro "PRUEBAS EN EL AMPARO. PARA EL DESAHOGO DE LAS RELACIONADAS CON MEDIOS ELÉCTRICOS O ELECTRÓNICOS NO ES ADMISIBLE LA IMPOSICIÓN DE CARGA ESPECÍFICA A SU OFERENTE PARA VALORAR SU ADMISIBILIDAD", en la que señala, que es posible la admisión de la evidencia digital en material civil, más sin embargo, el

[101] Código de Procedimientos Administrativos. **Artículo 210-A.-** Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que se haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.
Cuando la ley requiera que un documento sea conservado y presentado en forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología, se ha mantenida íntegra o inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta puede ser accesible para su ulterior consulta.
Artículo 1803.- El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:
I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y
Artículo 1805.- Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.

juzgador no está facultado para obligar a las partes a presentarlas. Así mismo, que su valoración será basada en los conocimientos del juzgador.

En el Código Penal Federal de Procedimientos, en su articulado, señala en el capítulo de pruebas que es admisible como prueba todo lo que sirva para probar un hecho, es decir, incluye las pruebas digitales. Sin embargo, en el capítulo de la valoración de pruebas, describe que todo aquel medio de prueba distinto a la confesión, tendrá valor indiciario, lo cual parece lógico especialmente si recordamos que la evidencia digital se puede modificar fácilmente.

Primeramente, se admiten como pruebas todos aquellos medios que sean conducentes y no vayan en contra del derecho. Así mismo, salvo la confesión, cualquier otro medio de prueba tiene valor indiciario. [102]

En el auge de los juicios en línea en materia mercantil, fiscal y administrativa, podemos darnos cuenta de que los medios probatorios han cambiado su percepción calificativa debido a su naturaleza procedimental, en el cual existe un cambio de paradigma respecto a su valoración probatoria y cuyas reglas se señalan en el articulado de la Ley Federal de Procedimiento Contencioso Administrativo.

En el articulado de éste código podemos encontrar que los documentos deben subirse a la plataforma del Sistema de Justicia en Línea, cotejándose con los documentos originales. Si se descubre que una persona ha alterado, modificado o destruido la información contenida en el sistema en línea se tomarán las medidas necesarias.[103]

[102] Artículo 206, Artículo 279, Artículo 285 del Código Penal Federal de Procedimientos.
[103] Ley Federal del Procedimiento Contencioso Administrativo ARTÍCULO 58-K, ARTÍCULO 58-L, ARTÍCULO 58-R.

Sin embargo, en México, el auge de las pruebas digitales no ha alcanzado su valor adecuado dentro de los juicios. Tomando como ejemplo al Estado de Veracruz, en donde existe una tipificación en el Código Penal Estatal, se destaca que solo existe una denuncia radicada desde su entrada en vigor y en la cual no se tuvo por acreditada la existencia del delito dado que las pruebas presentadas en la *investigación ministerial* no eran aptas para probar que los presuntos indiciados habían entrado a una base de datos[104].

5. La Policía Cibernética

A) ORIGEN DE LA POLICÍA COMO INSTITUCIÓN DE SEGURIDAD PÚBLICA

[104] HERNANDEZ GARCÍA, Helena, VEGA LEBRÚN, Carlos, Efectos de los delitos informáticos en el Estado de Veracruz http://www.letrasjuridicas.com/Volumenes/23/01a.pdf

La inoperancia efectiva de las instituciones de ciber-policía en México contribuye a la impunidad de delitos cibernéticos que se cometen en la actualidad. Es así que referirse a la creación de policía supone hablar de los fenómenos delictivos cuya aparición demandó en los ciudadanos la necesidad de sentirse protegidos no solo por leyes y reglamentos, sino que existiera una institución cuya acción tangible debía manifestarse en la protección a la esfera ciudadana, pero que ha sido utilizada históricamente como correa de transmisión del orden constituido por los gobiernos a favor de sus intereses.[105]

Durante la Edad media existieron instituciones que actuaban para preservar el orden social operando de acuerdo a sus intereses; de este modo, los poseedores de las tierras eran responsables de hacer efectivo el derecho, y de la misma forma, si existía la posibilidad de capturar a un sospechoso era responsabilidad civil entregarlo al señor feudal para que recibiera un castigo.[106]

Se estableció propiamente la figura de la policía en París bajo el régimen de Luis XIV en 1667 con diversas funciones, desde la responsabilidad de alumbrar las calles hasta organizar los espectáculos públicos, y por supuesto la manutención de la ley y el orden público. Hacia la época de la revolución francesa, el gobierno parisino tenía a su disposición a más de 3mil hombres uniformados para una población de 500mil habitantes. [107]

---

[105] COUSELO, Gonzalo Jar. "El papel de la policía en una sociedad democrática" *Reís*, 1999, p. 199-220.
[106] FRUHLING, Hugo. Modernización de la Policía. En documento presentado en la conferencia del BID: Convivencia y Seguridad Ciudadana en el Istmo Centroamericano, Haití y República Dominicana. San Salvador: Junio de 1998.
[107] EMSLEY, Clive, *"Los Orígenes de la policía moderna."* Historia hoy 49, no. 4, 1999, Búsqueda Académica completa EBSCO*host*, consultado el 21 de Octubre de 2013.

En el caso de México, fue hasta el Estatuto Orgánico Provisional de la República Mexicana que se incorporó el derecho a la seguridad a un texto de la Carta Magna en su Artículo 30 cuya adición se convirtió en letra muerta. Sin embrago, "*la prioridad no era la sujeción de la ley, sino la capacidad de colaborar a garantizar la centralización del control político del gobierno de la República a cualquier costo*".[108]

La insatisfacción hacia los cuerpos policiales ha impulsado un esfuerzo por reformar sus actuaciones, lo que se encuentra lejos de ser fácil e inmediato. Lo cierto es que el Estado debe preocuparse por combatir la comisión de delitos así como la protección de sus gobernados. De esta forma, la participación activa y diaria de la policía en la sociedad asume un papel fundamental para el Estado de manera que es a través de esta institución que existe la facultad de mantener el orden público y dar cumplimiento a sus leyes.

En la Ley de Seguridad Pública Preventiva se enlistan las funciones que la policía realiza, es así que el cuerpo policiaco deberá primordialmente conducirse con apego al orden jurídico y respeto a los derechos humanos. También prestará auxilio a las víctimas de cualquier delito; no infligir violencia, discriminación; abstenerse de actos arbitrarios; desempeñar su misión sin actos de corrupción; realizar detenciones legales; velar por la vida e integridad física de las personas

[108]LÓPEZ PORTILLO V, Ernesto, *"La policía en México: función, política y reforma"* Inseguridad pública y gobernabilidad democrática, Retos para México y Estados Unidos, Smith Richardson Foundation, Febrero, 2000, México. http://torresllamas.com/insyde/wp-content/uploads/2013/08/Policia_y_democracia.pdf

detenidas; participar en operativos; y velar por la seguridad física de los ciudadanos.[109]

B) CREACIÓN DE LA POLICÍA CIBERNÉTICA

Las tecnologías de la información y comunicación también han revolucionado los asuntos militares, incluyendo la información de los campos de batalla, sus comunicaciones y los sistemas armamentísticos, al tiempo que han incrementado su vulnerabilidad a este tipo de invasiones.

El desarrollo de la tecnología ha propiciado la gran cantidad de información que puede ser obtenida y analizada sea compartida a mayor escala. La revolución de la información, el crecimiento de la documentación digital y el desarrollo de la identificación pública, búsqueda y sistemas de rastreo han jugado un rol central en la sociedad.[110]

Para hacer frente a esta problemática de delincuencia y principalmente a las organizaciones delictivas, la Policía Federal Preventiva cuenta con un cuerpo policiaco cibernético encargado de investigar y detectar sitios de Internet dedicados a la comisión de delitos informáticos.[111] Esta policía especializada forma parte del Grupo de Coordinación Interinstitucional de combate a Delitos Cibernéticos en México (DC México).

"…para la detección de nuevos modus operandis…la Policía Cibernética de la PFP, integró a finales de 2002 un equipo especializado en delitos cibernéticos y

[109] Artículo 105 de la Ley de la Policía Federal Preventiva.
[110] DONOHUE, L. "Derecho penal, Privacidad Anglo Americana y supervisión," El diario de Derecho Penal y Criminología, 2006, Estados Unidos.
[111] Estado y Seguridad Pública, Colección editorial del gobierno del cambio, México, 2005.

asumió la responsabilidad de la Secretaria Técnica del grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos en México (DC México), a través de la cual ha venido trabajando con diversas instituciones para hacer frente a estas organizaciones criminales. Cabe destacar, que México es uno de los tres países latinoamericanos, además de Brasil, y Chile, que cuenta con una policía que supervisa el Internet, y mantiene el intercambio de información y apoyos técnicos con los gobiernos de Estados Unidos, España y Brasil."[112]

Aunque no existe un decreto o documento en donde se establezca la creación de la policía cibernética en México, hay información en el sitio oficial de la Policía Federal Preventiva acerca de una unidad denominada "policía cibernética" que se encuentra adscrita a la misma.

De acuerdo con un informe del IFAI[113] en respuesta a un usuario que solicita estadísticas acerca del índice de delitos informáticos en México, éste, como órgano especializado en acceso a la información describe que dicha unidad de Policía Cibernética depende de la Coordinación de Inteligencia para la Prevención de la Policía Federal Preventiva. Así mismo, que ésta unidad tampoco se encuentra señalada en la Ley de la PFP o en su reglamento, ni en el organigrama.

C) PRINCIPALES IMPLICACIONES Y RETOS

[112] Cuarto informe de labores de la Secretaría de Seguridad Pública. http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/94829//archivo
[113] AHV-GIMM-DGEI-015-06 Estudio-2433-SSP

La OEA realizó una encuesta a los países Latinoamericanos y del Caribe por la consternación de la falta de seguridad informática en sus países y fueron éstos mismos quienes hablaron de la necesidad de contar con profesionales altamente capacitados que puedan asegurar redes, detectar intrusiones, y manejar eficazmente los incidentes cibernéticos cuando estos ocurren. Conjuntamente, su vulnerabilidad se asocia con la falta de legislación, la falta de experiencia de los investigadores de delincuencia cibernética y la escasez de fiscales especializados en delitos relacionados con la tecnología.[114]

Otro de los principales retos para la implementación efectiva de la policía cibernética en México, es la de invertir en capacitaciones, infraestructura, recurso humano, y especialmente en la adquisición de sistemas informáticos adecuados para realizar investigaciones policiales y patrullaje en el ciberespacio.

La falta de legislación principalmente deja un espacio latente en la detección de delitos cibernéticos, pues algunos de los crímenes informáticos existen propiamente derivados de Internet y cuya conducta no puede ser adecuada a los tipos existentes en los Códigos Estatales. El reto para los legisladores es crear normas jurídicas que permitan la sanción de conductas delictuosas que derivan de la tecnología. Los demás Estados deben comenzar a preocuparse por la inclusión de tipos penales pertinentes siguiendo el ejemplo del Congreso Veracruzano, el cual se pronunció a favor de la protección de menores en la red y aprobó de manera unánime la creación de la figura de la policía cibernética el 08 de Octubre de 2011

[114] Tendencias en la Seguridad Cibernética en América Latina y el Caribe y Respuesta de los Gobiernos http://www.oas.org/es/ssm/cyber/documents/OASTrendMicroLAC_SPA.pdf

reformando así su Código Penal, la Ley Orgánica del Poder Ejecutivo y la Ley del Sistema Estatal de Seguridad Pública.

Son apenas ocho los Estados de la República (Coahuila, Colima, Durango, Morelos, Nuevo León, Sinaloa, Tabasco y Veracruz) que incluyen en sus Códigos Penales la tipificación de "Delito Informático", sin embargo, se quedan en la intrusión a equipos con una pena de 3 meses a 3 años en promedio. Destaca el Estado de Morelos[115], en cuya descripción del tipo, además agrega que también comete delito informático quien haga uso de la red de Internet utilizando cualquier medio para realizar actos en contra de las personas o en un grupo o sector de ella, para perturbar la paz pública o que atente contra el orden constitucional. Lo anterior se refiere a *ciberterrorismo.*

Entidad	Fecha de creación	Número de Agentes	Estado	Comentario
Baja California				Persiguen delitos de pornografía infantil, terrorismo virtual, instigación al suicidio, cyberbullying, spam.
Guerrero	2008	No especifica	Activa	
Jalisco	30 de Septiembre de 2002[116]	No especifica	Activa	Es el primer cuerpo policiaco que se crea de su tipo a nivel Estatal.
Chihuahua		Se mantiene en anonimato por protección.		
Coahuila	Marzo de 2007	7 agentes ministeriales	Inactiva	De acuerdo con un reporte ciudadano, esta unidad dejó sus

[115] Artículo 148 quarter del Código Penal para el Estado de Morelos.
[116] Gaceta Parlamentaria, Número 3248-I, Martes 26 de Abril de 2011 http://gaceta.diputados.gob.mx/Black/Gaceta/Anteriores/61/2011/abr/20110426-I/ComunicacionOficial-6.html

				funciones desde Junio de 2013.[117]
Distrito Federal	Abril de 2013	35 agentes: 20 dedicados a patrullaje y 15 para prevenir e informar sobre delitos informáticos.	Activa	Han recibido 764 reportes desde su creación relacionados con delitos informáticos. Especialmente aquellos que fueron víctimas del ransomware[118].
Querétaro	Febrero de 2011	No especifica	Activa	Hasta 2012 se han registrado 52 ataques cibernéticos de tipo fraude, extorsión, pederastia, suplantación de identidad, homicidio, etc.[119] Sin embargo, no existe un sitio oficial de contacto en donde se pueda accesar a su información. Su Código Penal ha reformado sus tipos delictivos en Fraude, Falsificación e uso indebido de documentos, Extorsión y Pornografía infantil que señalan su comisión por medio electrónicos.[120]

[117] Nota publicada el 11-08-2013 consultada el 26-11-2013 http://www.eldiariodecoahuila.com.mx/notas/2013/9/11/desaparece-policia-cibernetica-386214.asp

[118] Ransomware. Es conocido como el "virus de la policía" el cual resulta en un bloqueo del sistema que ataca generalmente en sitios de descarga de música o videos, disfrazado en imágenes comerciales. El usuario es fotografiado por medio de su cámara web y luego aparece una imagen de la Policía Federal señalando que ha sido acusado de varios delitos por lo que debe realizar un pago para que poder desbloquear su equipo de cómputo.

[119] Noticia publicada el 25-04-2012 http://www.oem.com.mx/elheraldodechihuahua/notas/n2518420.htm

[120] Artículos 194 Fracción XVIII; 198 Fracción V; 232 Fracciones II, IV y V y; 239 bis del Código Penal del Estado de Querétaro.

Veracruz	19 de Noviembre de 2012		Activa	

La implementación de una Unidad de Delitos Cibernéticos en los Estados de la República Mexicana serviría como refuerzo para los esfuerzos de los Gobiernos por brindar seguridad a sus gobernados.

Como se denota en el recuadro comparativo, nos queda claro, que aunque existen cuerpos policiacos cuyas funciones son encaminadas a la detección de los delitos informáticos, no existe aún una cultura informática social que permita la denuncia de tales delitos por desconocimiento acerca del tópico. Así mismo, los agentes informáticos son pocos, así como sus oficinas son desconocidas por los usuarios en la mayoría de los Estados.

Por otra parte, constan éxitos de investigaciones cibernéticas de estas escazas unidades como la detección y detención de pedófilos como Arthur Leland Sayler y Robert Decker en nuestro país gracias a la tecnología y la cooperación con organismos internacionales.

D) FUNCIONES DE LA POLICÍA CIBERNÉTICA

Las funciones de la policía cibernética son diversas y recogen acciones en materia de seguridad y prevención:

- Punto de contacto nacional e internacional para atender las amenazas cibernéticas.
- Impartir a alumnos, padres de familia y ciudadanía en general consejos y medidas preventivas al navegar en la Internet y explicar los riesgos que corren los menores.
- Prevenir y combatir los delitos como: pornografía infantil, fraudes, trata, prostitución y cualquiera que se derive del uso de medios informáticos y electrónicos.
- Informar y asesorar a la ciudadanía como denunciar si ha sido víctima de un delito relacionado con un sistema informático.
- Monitoreo y patrullaje de la web para detectar y prevenir delitos.
- Lanzar comunicados informativos de carácter informático.
- Dar seguimiento a las denuncias recibidas por medio del Ministerio Público de carácter informático.
- Proporcionar respuesta y defensa contra incidentes de seguridad de la información a instituciones del Estado.
- Coadyuvar con el Ministerio Público en investigaciones donde se requieran de sus conocimientos.
- Encargarse de recopilar la información digital en la comisión de delitos.

En entrevista con el comandante Raúl Peralta Alvarado, Jefe General de la Policía de Investigación en el DF[121], señala que los requisitos para ser parte de la policía cibernética son:

- Tener una carrera universitaria terminada.
- Edad mínima de 21 años y máxima de 30.
- Pasar el proceso de capacitación en el instituto para agentes de investigación, que incluye las materias de marco jurídico, leyes y reglamentos, acondicionamiento físico, sometimiento de personas, traslado de detenidos, prácticas de tiro, entre otras.
- Se realizan grupos de acuerdo a su perfil académico.
- Para la policía cibernética, se seleccionan agentes que tengan conocimiento en temas de cómputo y manejo del software utilizado en esa área.
- Al grupo seleccionado se le da una capacitación para desarrollar sus habilidades. Este curso puede durar hasta 1 año.

Para obtener un mejor desempeño en la investigación de conductas tendientes a la comisión de un delito electrónico, o bien para actuar en coadyuvancia de la Autoridad competente en la indagatoria de un delito electrónico, la Unidad de Delitos Cibernéticos cuenta con la siguiente estructura:

1. Área de monitoreo en Internet. Esta área es en específico la que de mayor manera refleja la función contenida en el artículo 8 fracción XLII de la Ley de la Policía Federal, ya que en la misma se realizan las

[121] El ABC de ser ciberpolicía, Entrevista en video www.vertigopolitico.com, publicado el 17 de Abril de 2013

labores de monitoreo constante en la red de Internet, a fin de encontrar en los contenidos de las páginas y blogs conductas que en algún momento pudieran consolidarse en delitos, o en su caso, si los contenidos por la descripción legal que corresponde ya estuvieran consumados, y éstos se persiguieren de oficio, de manera inmediata se dará vista al Ministerio Público de la Federación o a la autoridad que por razón de competencia deba conocer. Ésta área conoce todo tipo de conductas que puedan ser consideradas como delitos con excepción de aquellas que atenten contra los menores o contra quienes no tengan la capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo.

2. Área de delitos contra menores. Al ser la red de Internet un medio que permite la realización de delitos en agravio de los menores de edad o contra quienes no tienen capacidad para resistirlo, toda vez que permite el escudo del anonimato que otorga la gran comunidad virtual, resulta inminente el monitoreo de Internet en específico a efecto de descubrir conductas que van en agravio de la niñez y de personas vulnerables y que resulta de gran interés por tratarse de un bien jurídico supremo, en ese orden de ideas, esta área se encarga de la atención de asuntos de pornografía infantil, trata de menores para fines de explotación sexual y laboral y la elaboración de investigaciones de índole preventivo y en coadyuvancia con la Procuraduría General de la República o la autoridad competente que así lo solicite en las cuales medie un equipo o sistema de cómputo.

3. Área Forense. Esta área es una de las más importantes de la Unidad, en virtud de que acorde con las facultades otorgadas por la fracción XVII del artículo 8 de la Ley de la Policía Federal, en coadyuvancia con autoridades competentes, con respeto irrestricto a los Derechos Humanos y Garantías individuales, se obtienen elementos indiciarios para la investigación de un delito, materializados por el análisis de evidencia digital".

E) SITUACIÓN NACIONAL

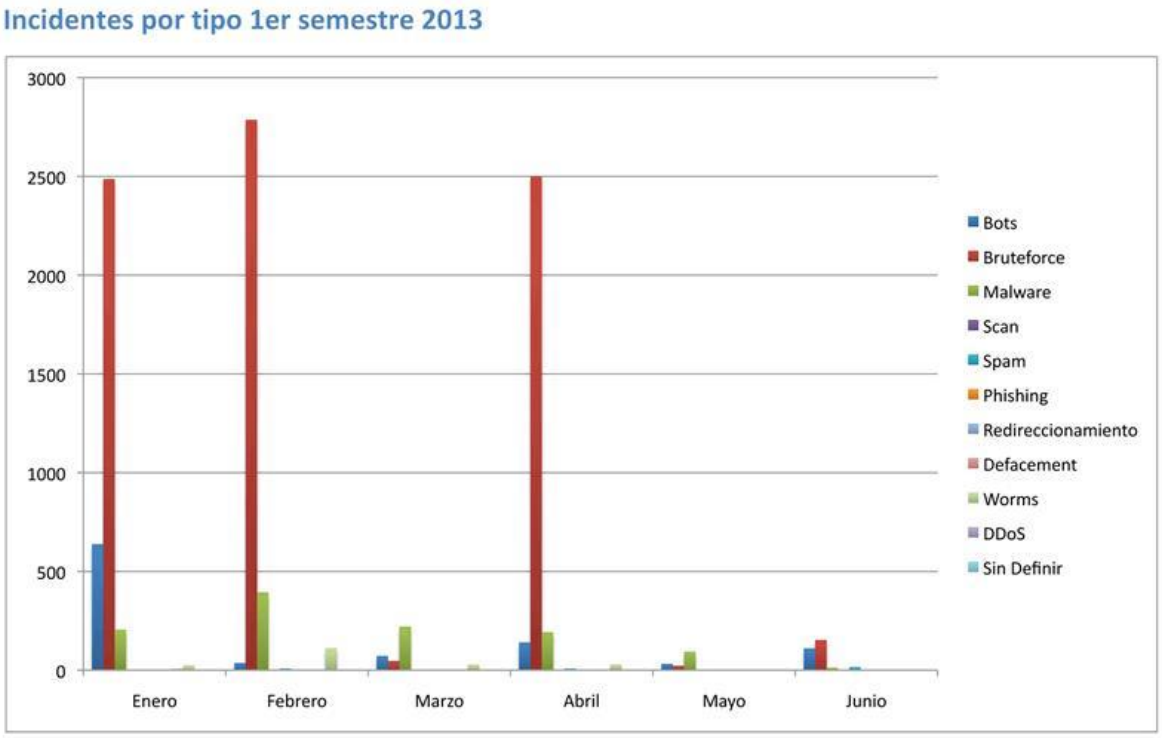
Existen organismos descentralizados que han atendido las llamadas de auxilio de quienes han sido víctimas de delitos cibernéticos en México, dichos grupos se han conformado por expertos en sistemas informáticos que coadyuvan con el Ministerio Público entregando reportes de los ilícitos.

- CERT-MX[122] (Equipo de Respuesta a Incidentes de Seguridad en Cómputo) Es un equipo de profesionales de seguridad en cómputo que se encuentra localizado en la subdirección de la Información de la Dirección General de Cómputo y Tecnologías de Información y Comunicación de la UNAM. Su función es la de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún ataque, así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar

[122] Sitio oficial del CERT en México http://www.cert.org.mx/index.html

investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios.

De acuerdo con su naturaleza de carácter institucional y académico, aclarar, que el CERT no es un cuerpo policiaco, ni procurador de justicia, ni abogados, ni solucionador de conflictos internos de empresas o corporaciones. [123]



Estadística que muestra el índice de delitos cibernéticos cometidos por mes y detectados por el equipo del CERT http://www.cert.org.mx/estadisticas.dsc

- DC México (Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos)

[123] GUEL LÓPEZ, Juan Carlos. Miembros operativo del CERT-MX http://lacnic.net/.../juan_carlos_guel_UNAM-CERT.ppt

Inicia sus actividades el 9 de Diciembre de 2002 con la misión de implementar políticas y acciones tendientes a combatir los delitos cibernéticos en México. Este grupo se encuentra encabezado por la Policía Federal Preventiva como Secretaria Técnica. Así mismo cuenta con el respaldo de miembros de la Secretaría de Gobernación, la Defensa Nacional, la de Marina, Relaciones Exteriores, la Procuraduría General de la República, Universidades Mexicanas, E-México y Empresas de telecomunicaciones.

DC México tiene como tareas fundamentales la identificación de monitoreo, y el rastreo de cualquier manifestación delictiva que se cometa mediante computadoras conectadas en territorio mexicano o fuera de él y que tenga afectaciones en nuestro país.[124]

La situación nacional se ha visto afectada por la desorganización de los cuerpos de seguridad pública en sus áreas informáticas. Es notable que la existencia de los grupos externos enfocados a la seguridad cibernética se han ocupado de combatir en la medida de sus posibilidades aquellos conflictos que surgen en las redes.

[124] CAMPOLI, Gabriel Andrés, "Pasos hacia la reforma penal en materia de delitos informáticos en México", AR: Revista de Derecho Informático, núm. 079, febrero de 2005, http://www.alfa-redi.org/rdi-artículo.shtml?x=974

6. Consideraciones Finales

I. El avance tecnológico que permea en la sociedad, ha causado una dependencia social que no puede ser esquivada. La población avanza a ritmo rápido y continuo, así como las conductas criminales que no escapan de subirse al tren de la era digital.

II. Los abogados y funcionarios deben tener presente que para que sus funciones sean realizadas con eficacia, éstas deben adaptarse a las necesidades jurídicas que surgen a partir de la evolución tecnológica.

III. Debe ser imperante que los legisladores propongan la creación de nuevas figuras delictivas propias de cometerse mediante Internet o un sistema informático.

IV. La figura de la Policía Cibernética, ha sido desde su creación, un ente que ha significado éxitos en los Estados que han atendido las denuncias de acuerdo con la importancia que merecen. Y sus logros dependerán del seguimiento y capacitación que les permita contar con personal calificado para emplear sus conocimientos aplicados a la persecución de los delitos en un espacio virtual.

V. Los agentes cibernéticos, deben además, no solo estar capacitados en el marco legal e informático, sino que deben ser especialistas en el campo de la investigación para poder recopilar evidencia digital que logré ser pertinente como medio probatorio en juicio.

Bibliografía

ATIENZA, Manuel. *"Constitucionalismo, globalización y derecho. El Canon",* 2009.

BADIA, Félix. *"Internet, situación actual y perspectivas",* Ed. La Caixa, Barcelona, 2002, Pág. 22

CÁCERES NIETO, Enrique. *"El sistema UNAM-JURE, un banco de información legislativa"*, México 1991.

CAMPUZANO, A.J, Racionalidad jurídica y globalización. Paradojas y perplejidad en torno al ordenamiento jurídico, Revista Cien. Jur. e Soc. da Unipar, Umaurama, v.11, n.1, p. 223-245, En/Jun, 2008.

CERVANTES CABALLERO, Eva Leticia. *"Problemática documental de la información jurisprudencial en México"* México, 1991.

CLARKE, Richard A.; KNAKE, Robert. *"Guerra cibernética: la próxima amenaza a la seguridad nacional y qué hacer sobre ella".* Ed. HarperCollins, 2010.

COUSELO, Gonzalo Jar. "El papel de la policía en una sociedad democrática" *Reís*, 1999, p. 199-220.

FERNÁNDEZ TERUELO, Javier G. *"Derecho Penal e Internet",* Ed, Lex Nova, Primera edición, España 2011. Pág 153

FIX FIERRO, Héctor, MUÑOZ DE ALBA, Marcia, "*El sistema unam-jure hoy, Diálogo sobre informática jurídica",* Editorial UNAM, 1989. Págs, 31 y 32.

FLINT, David, *"Ley modelando la tecnología: la tecnología modelando la ley",* Revista Internacional de Derecho, Computadoras y tecnología, Vol.23, Marzo-Julio de 2009.

FRUHLING, Hugo. Modernización de la Policía. En *Documento presentado en la conferencia del BID: Convivencia y Seguridad Ciudadana en el Istmo Centroamericano, Haití y República Dominicana. San Salvador: junio*. 1998.

G. RROBERTS, MIT: *"Hacia una red Cooperativa de Computadoras de Tiempo Compartido",* Estado Unidos, 1966 (Inglés)

GRÜN, Ernesto, *"El derecho en el mundo globalizado del siglo XXI desde una perspectiva sistémico cibernética",* Revista Telemática de Filosofía del Derecho n°4 2000/2001, .43-124.

HUSSAIN, Rashid. *"Fuerzas especiales del Ciberespacio para la protección infantil"* Revista Internacional de la Academia de investigación 3.2 (2011): 1001-1007. Consulta académica Web. 6 Nov. 2013.

INTZESSILOGLOU, Nikolaos G., *"L'approche systémique au système ouvercomme stratégie d' élaboration' d'un project d'étude interdisciplinaire de phénomène juridique* » Congreso jurídico de sistémica, Lausanne, 1989 p. 168

LENHART, Amanda. "*Adolescentes y sexting. Internet y Reporte del Proyecto sobre la vida Americana"*, Julio, 2009, vol. 4, p. 2010.

MARTINS, Sergio; YANG, Yang. *"Introducción a los bitcoins: un sistema de moneda pseudo-anónimo",* En Congreso de 2011, Conferencia del Centro de Estudios avanzados en investigación por colaboración. IBM Corp., 2011. p. 349-350.

MC QUADE, Samuel C. *"Cyberbullying",* Librería del Congresos, Primera edición, Estados Unidos, 2009, Pág. 2

MITNICK, Kevin D.; SIMON, William L. *"El arte de la intrusion: Las historias: Las historias reales detrás de los motives de los hackers, intrusos y embaucadores"*. Wiley. com, 2009.

PÉREZ CRUCI, Juan Ignacio, *"La globalización y sus consecuencias en el nuevo orden jurídico internacional".*

ROJAS AMANDI, Víctor M. *"El uso del Internet en el Derecho"* Ed. Oxford, México, 2000, P.11

ROMEO CASABONA, Carlos Ma. , *"Poder informático y seguridad jurídica",* Fundesco, 1988.

Secretaría de Programación y Presupuesto, "*La Informática y el Derecho"*, INEGI, México, 1983, p. 23.

TELLEZ Valdés, Julio, *"Derecho Informático",* Editorial UNAM, México, 1991, Pág. 7.

TELLEZ VALDEZ, Julio, "Derecho Informático", 4ta Edición, MCgraw-hill México 2009

VIEIRA POSADA, Edgar. "Interpretaciones Y Transformaciones Tecnológicas En Los Procesos De Globalización."Papel Político 16.2 (2011): 667-699.

VON BERTALANFFY, Ludwig "Teoría General de los Sistemas" Fondo de Cultura Económica, México, 1984.

WEGENER, Henning, *"los riesgos económicos de la ciberguerra"* Cuadernos de estrategia, ISSN 1697-6924, Nº. 162, 2013 (Ejemplar dedicado a: La inteligencia económica de un mundo globalizado), págs. 177-227

WIENER, Norbert, *"Cibernética y Sociedad",* INEGI, México, 1981, p.97.

Páginas Web

"Robo de identidad" 2013, Enciclopedia Electrónica de Columbia, 6ta Edición, p. 1, EBSCOhost, consultada 16 Octubre 2013.

ABC (5 de Diciembre de 2010) "Assange hace circular por la red un archivo de seguridad cifrado" Consultado el 14 de Octubre de 2013 http://www.abc.es/20101205/internacional/rc-assange-hace-circular-internet-201012051150.html

CANO, J. Informática forense, liderando las investigaciones. Portal de Seguridad viruspot: www.viruspot.com/Col8.html, 2001.

CARRANZA TORRES, Luis "Las nuevas tecnologías de la información y el contralor ciudadano de la administración" Revista Informática Jurídica http://www.informatica-juridica.com/trabajos/Las_nuevas_tecnollogias.asp

CARRANZA TORRES, Luis." El derecho frente a la sociedad de la información" http://www.informatica-juridica.com/trabajos/El_derecho_frente_a_la_sociedad.asp

CHARNEY, Scott; ALEXANDER, Kent. *"Crimenes de computadora*". Emory LJ, 1996, vol. 45, p. 931.

Cuarto informe de labores de la Secretaría de Seguridad Pública. http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/94829//archivo

DAVIS, Joshua. *"Los Hackers tumban el país más lleno de cables en Europa*". Revista *Wired*, 2007, vol. 15, no 9, p. 15-09. http://en.rsf.org/t

DONOHUE, L. "Derecho penal, Privacidad Anglo Americana y supervisión," El diario de Derecho Penal y Criminología, 2006, Estados Unidos.

El diario español (05-10-2013) http://www.eldiario.es/turing/Hackers-tubo_0_174982681.html

El diario NY (3-01-2013) consultado 21 de Octubre de 2013)

El Econonomista publicado el 17-07-2013 http://eleconomista.com.mx/tecnociencia/2013/07/17/aumentan-10-usuarios-internet-china

EMSLEY, Clive. 1999. "Los Orígenes de la policía moderna." Historia hoy 49, no. 4: 8.Búsqueda Académica completa EBSCO*host*, consultado el 21 de Octubre de 2013.

FONSECA MARTINEZ, Claudia, *¿Qué es el Spam y por qué existe?* "El SPAM y su impacto" Foro Cofetel 3 de Marzo de 2005 www.cofetel.gob.mx/foro_spam.shtml

GARCÍA GALERA, María del Carmen, DEL HOYO HURTADO, Mercedes *"Redes Sociales, Un Medio Para La Movilización Juvenil "* Zer: Revista De Estudios De Comunicacion 17.34 (2013): 111-125. consultado 8 Oct. 2013.

GAUTHRONET, Serge; DROUARD, Etienne. *"Comerciales no solicitados y protección de datos"* Comisión de la Comunicación Europea, 2001. (Inglés)

GUEL LÓPEZ, Juan Carlos. Miembros operativo del CERT-MX http://lacnic.net/.../juan_carlos_guel_UNAM-CERT.ppt

HENNING Wegener, Los riesgos económicos de la ciberguerra dialnet.unirioja.es/descarga/articulo/4276097.pdf

HERNANDEZ GARCÍA, Helena, VEGA LEBRÚN, Carlos, Efectos de los delitos informáticos en el Estado de Veracruz http://www.letrasjuridicas.com/Volumenes/23/01a.pdf

JIMENEZ, Enríquez, *"El robo de identidad, nuevo reto para el derecho del siglo XXI",* Revista Abogacía consultada el 11 de Octubre de 2013. http://www.abogacia.es/wp-content/abogados/ficheros/1331025558756.pdf

La Jornada (10-02-2013) http://www.jornada.unam.mx/2013/02/10/mundo/021n3mun

La Jornada, *"Activistas Europeos piden al IFAI investigar sobre software espía",* publicado el 24-07-2013, consultado el 30-08-2013, http://www.tedf.org.mx/sala_prensa/sintesis/sm2013/jul/130724/130724_ifai_activistas_europeos.pdf

La vanguardia. Publicado el 14-05-2012 http://www.lavanguardia.com/internacional/20120514/54293901755/iran-prohibe-uso-yahoo-gmail-hotmail.html

LANDERS, Chris (25 de Enero de 2008). "El Internet está yendo a la guerra". Periódico de la Ciudad de Baltimore Publicado 2008-01-25. Consultado el 15 de Octubre de 2013.

http://blogs.citypaper.com/?s=The+Internets+Are+Going+to+WarExaminer (23-08-2013)

LÓPEZ PORTILLO V, Ernesto, *"La policía en México: función, política y reforma"* Inseguridad pública y gobernabilidad democrática, Retos para México y Estados Unidos, Smith Richardson Foundation, Febrero, 2000, México. http://torresllamas.com/insyde/wp-content/uploads/2013/08/Policia_y_democracia.pdf

MAD, Macz, *"Internet clandestino",* Editorial Page Free Publishing inc, Estados Unidos, 2002.

Nota de El Universal Veracruz publicada el 09-10-2013 http://www.eluniversalveracruz.com.mx/seguridad-veracruz/2013/aprueban-policia-cibernetica-contra-pornografia-infantil--19290.html

OLSON, PARMY. "Anonymous, Las armas falsas virtuales y militares. 2011.

Película "We are Legion" dirigida por Brian Knnapenberger Sitio oficial en inglés http://wearelegionthedocumentary.com/about-the-film/

PEÑA, Carlos A. *"Informática Jurídica y Derecho Informático"* , Universidad de Palermo, www.palermo.edu/ingenieria/downloads/pdfwebc&T8/8CyT05.pdf

PRADO, Pedro Antonio. *"La informática y el abogado"* Ed. Abelardo Perrot, Buenos Aires, 1988.

Recovery Labs, *"Fraude en internet: del phishing al pharming"* consultado el 16 de Octubre de 2013 http://www.recoverylabs.com/informes/Recovery_Labs_pharming.pdf

Sánchez Curbelo, Benigno Víctor. *"Las Nuevas Tecnologías Y Los Delitos Informáticos"* Tono: Revista Técnica De La Empresa De Telecomunicaciones De Cuba, S.A 3 (2006): 14-19. Web. 6 Nov. 2013.

Sitio oficial del CERT en México http://www.cert.org.mx/index.html

STAJANO, Frank; WILSON, Paul. *"Entendimiento a las víctimas del Scam: siete principios para los sitemas de seguridad"*. Communications of the ACM, 2011, vol. 54, no 3, p. 70-75.

SUNDARAM, Ravi, "*Temas sobre informática teórica: problemas de la investigación del Internet",* publicado el 13-02-2002 y consultado el 10 de Octubre de 2013 http://mit.ocw.universia.net/18.996/s02/lecture-notes/lecture2_mit.pdf

Tendencias en la Seguridad Cibernética en América Latina y el Caribe y Respuesta de los Gobiernos http://www.oas.org/es/ssm/cyber/documents/OASTrendMicroLAC_SPA.pdf

The daily beast (19-10-2013) consultado 21 de Octubre de 2013 http://www.thedailybeast.com/articles/2013/10/19/anonymous-maryville-and-the-new-vigilantism.html

The register UK nota publicada el 13-11-2002 http://www.theregister.co.uk/2002/11/13/welsh_web_designer_charged/

UNIAN(24-07-10) consultado el 18 de Septiembre de 2013 (inglés) http://www.unian.info/news/204617-three-19-year-old-youths-committed-19-murders-in-dnipropetrovsk-during-a-month.html

VICENTE, Loreto, "¿Movimientos sociales en la red? Los hacktivistas" Revista El cotidiano, México, consultada el 16 de Octubre de 2013 http://www.elcotidianoenlinea.com.mx/pdf/12615.pdf